Apple Technical White Paper

Security for Mac Computers in the Enterprise

October, 2012

Mountain Lion 10.8

Contents

Introduction

OS X is designed from the ground up with an eye toward providing and maintaining system security in an automatic and easy-to-use way. Apple strives to ensure that OS X provides protection to systems, software, and data without the need for advanced configuration or specialized tools. As your organization considers security strategy, it's important to find the mix of technologies that best protects against unauthorized use or access and that also meets the needs of your business.

The Mac is designed to provide a resilient defense against security threats through a series of protective systems and approaches to identify potential threats and proactively protect against them. These defenses:

- Manage access to system resources at a granular level
- Mitigate advanced runtime attacks
- Protect against network-borne threats
- Validate the integrity and authenticity of software
- Quarantine unknown files

Apple also implements many security features designed to protect the confidentiality of both user and corporate data. Some of these features protect data stored on a local or removable volume (data at rest), while others protect data shared on a local network or traveling across the Internet (data in transit). Many of these technologies are inherent in the design of the operating system and are active without requiring configuration. Others, such as FileVault 2, can be easily enabled and configured by both users and IT departments.

OS X is built on a foundation of open source components that have been through decades of intense scrutiny by Apple, third-party developers, and security experts. Apple participates in the open source community by sharing the development process of many OS X components with third-party developers. This ongoing effort leads to the incorporation of recommended improvements and provides the transparency necessary to validate that many critical components of OS X are as secure as possible.

Apple also collaborates with the broader information security community, including CERT, FIRST, the FreeBSD security team, and government security experts. These efforts have led to a joint review and validation of technology implementations and have also resulted in ongoing security guidance. A thorough and granular discussion of methods to refine the security configuration of OS X systems is publicly available in the form of Apple Security Configuration Guides (www.apple.com/support/security). You can also find them on the NSA Information Assurance website (www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml).

Service and App Protection

OS X provides a range of technologies that work to ensure the security of Mac systems. One of the most critical is the use of digital signatures to certify applications are safe and haven't been tampered with by an individual, malware, or file damage. Sandboxing of applications and services ensures that a compromised app or process can have only limited impact. Mandatory access controls work with other security technologies to help ensure system, application, and data security.

Gatekeeper

Gatekeeper allows users and organizations to set a required security level for installing applications. For maximum security, users can install only apps from the Mac App Store. Users can also choose to install apps from the Mac App Store and apps that have a Developer ID. In addition, employees and organizations can install apps from any source—just as they can today. Finally, users can temporarily override their setting and install any app at any time. Organizations wishing to enforce the use of Gatekeeper can use their Mobile Device Management (MDM) of choice to manage this setting.

Digital Signatures and Developer IDs

OS X uses digital signatures for each application on a system to greatly enhance system and application security. The Apple Developer Program allows each company creating Mac software to sign its applications using a Developer ID. This digital certificate, which can be verified by Apple, offers two levels of protection.

First, OS X ensures that an application installed on a Mac system is the genuine article from the developer. When a user launches an application, a Mac system verifies the authenticity of the application with Apple. Because the signature is embedded in the application, OS X can determine that an item with a name, icon, and other content matching a legitimate app isn't genuine. This feature can alert users to the presence of malware or spyware.

Second, OS X uses digital signatures to validate the data integrity of the application to ensure that it hasn't been tampered with, damaged, or infected by malware. If it has, the system will alert the user trying to launch the compromised application. Even if a developer chooses not to sign an application, OS X will sign the application using a local signature the first time it's run and use the signature to validate the app.

Client management options for OS X—including configuration profiles and even parental controls—all rely on application signatures when restricting access to applications. Even if users rename a restricted application, they won't be able to run it.

App Sandboxing

Sandboxing places controls on apps, such as restricting what data can be accessed, preventing communication on a network, and preventing the launch of other applications. This ensures that software does only what it's intended to do and prevents compromised code from hijacking applications or system services. Apps downloaded from the Mac App Store run only in a sandboxed state. Sandboxing, combined with digital signatures, ensures that any software purchased through the Apple Mac App Store is secure. By standardizing around such apps, an organization can feel secure about the apps it deploys to Mac systems.

Sandboxing also goes beyond individual applications. Many OS X system services are sandboxed to ensure system security. Services that can access arbitrary files or communicate on the network, such as Bonjour and Spotlight, are examples of high levels of sandboxing. With such services and applications, Apple strives to provide security at an integrated level without sacrificing functionality.

Mandatory Access Controls

OS X includes a fine-grained access control mechanism known as mandatory access controls. These controls enforce restrictions on access to system resources such as networks, files, and process execution. This restriction applies even to processes running as the superuser (that is, "root"), ensuring only explicitly granted system resources are available. Mandatory access controls underlie many OS X features, including Gatekeeper and app sandboxing.

Runtime Protection

OS X employs a number of hardware and software techniques to protect the operating system and applications. These runtime protections are designed to prevent the unauthorized execution of malicious code, mitigate the effectiveness of advanced exploits, and help prevent unauthorized access to data and system resources. Combined, all of these built-in technologies contribute to a layered defense against malware.

Execute Disable

One of the most common attacks used to gain unauthorized access to systems is known as a "buffer overflow," wherein an attacker attempts to inject and execute a malicious payload by overfilling memory reserved for input data. OS X provides protection against this attack by taking advantage of the eXecute Disable (XD) function available in Intel microprocessors. At compile time, Xcode developer tools mark the portions of an app that contain executable code and those that contain data. The Mac processor then honors these flags at runtime, mitigating the risk of buffer overflow attacks.

System Library Randomization

A "return-to-libc" attack attempts to trick a Mac into executing malicious code by manipulating memory addresses of the stack and system libraries. In OS X, system library memory addresses are randomly generated at installation. This process also occurs after system software updates and can be initiated manually through command-line tools. For any given Mac system, the memory address of a particular library function may be in one of thousands of random locations. Across an enterprise deployment, this randomization differs on every Mac, making "return to libc" exploits much more difficult.

Address Space Layout Randomization

Address Space Layout Randomization (ASLR) is designed to further obscure memory addresses from potential attackers. Taking advantage of the vast 64-bit memory space of the Mac, ASLR places executable code, system libraries, and related programming constructs in randomized locations for Position Independent Execution (PIE). This reduces the likelihood of many sophisticated attacks, such as "return to libc" and "shellcode" exploits.

Data Protection

OS X includes easy-to-use methods for ensuring that data stored on Mac systems is kept in a secure manner. As with other systems and devices, OS X uses file and data encryption to ensure privacy. Apple has worked to provide secure encryption tools that are easy to use and as transparent as possible to trusted users. In addition, OS X provides both local and remote methods for secure sanitization of data on a Mac system, preventing recovery if a computer is decommissioned, repurposed, lost, or stolen. The secure erase functionality in OS X meets the standards for sanitizing magnetic media set by the U.S. Department of Defense.

Note: The secure erase function of OS X Mountain Lion does not yet meet the standards for sanitizing the flash storage found in products such as MacBook Air.

FileVault

FileVault 2 provides full disk encryption for "data at rest." This protection can be applied to both internal and removable drives. FileVault 2 employs XTS-AES-128 data encryption to secure data on a Mac system should it be lost or stolen. Enterprise organizations should consider requiring the use of FileVault 2 to protect sensitive data stored on Mac systems, particularly on portable systems like the MacBook Air.

When FileVault 2 is enabled on Mac systems, a preboot authentication prompts the user for login credentials. Valid credentials must be entered before continuing the boot process. Valid credentials must also be entered to gain access to specialized startup modes, such as target disk mode. Without valid login credentials or a recovery key, the whole volume remains encrypted and is protected from unauthorized access even if the physical drive is removed and connected to another system.

When FileVault 2 is enabled, initial encryption is fast and performed unobtrusively in the background. Designed for balanced system performance, FileVault relinquishes processor cycles to higher-priority user tasks and applications. After initial encryption is complete all data is protected at rest. FileVault ensures that data actively being used is only encrypted or decrypted at runtime as needed.

During setup, FileVault 2 generates a personal recovery key (PRK) to allow access to the encrypted volume should a user's password be forgotten or otherwise unavailable. In an enterprise environment, this PRK could be recorded and securely stored by the IT organization (or the owner of the computer in a BYOD situation). IT departments should implement an institutional recovery key (IRK) to accommodate forensic and electronic discovery processes if needed.

Encrypted Disk Images

Using Disk Utility, and third-party tools, it's possible to create encrypted disk images. Unlike images used for system deployment, encrypted disk images serve as secure containers that can be used to store or transfer sensitive documents and other files. Disk images can be encrypted using either 128-bit or 256-bit AES encryption. Because a mounted disk image is treated as a local volume connected to a Mac system, users can copy, move, and open files and folders stored in it. As with FileVault 2, a disk image's contents are encrypted and decrypted in real time. Users can use encrypted disk images to safely exchange documents, files, and folders by saving the encrypted disk image to removable media, sending it via email, or storing it on a remote server.

Keychains

Using a unique password for each resource is a good security practice. This can be a daunting task given the number of file servers, websites, email accounts, encrypted volumes, and other password-protected resources encountered by today's users. OS X offers a secure store known as a keychains. Keychains provide a convenient and secure repository for credentials such as digital identities, user names and passwords, encryption keys, and secure notes. Using keychains eliminates a user's need to enter—or even remember—the credentials for each resource. An initial default keychain is created for each Mac user though users can also create additional keychains for specific purposes.

In addition to user keychains, OS X relies on a number of system-level keychains that maintain authentication assets that are not user-specific, such as network credentials and public key infrastructure (PKI) certificates. One of these keychains, the "System Roots" keychain, is an immutable store of Internet PKI root certificates to facilitate common tasks like online banking and e-commerce. IT administrators can similarly deploy internally provisioned certificate authority (CA) certificates to managed Macs to aid in the validation of internal sites and services.

Secure Erase

In standard computing models, including OS X, files and data are only removed from a storage device when another file is written over the storage used by the "deleted" data. Many commercial disk management, data recovery, and forensic tools offer the ability to recover deleted files from a device. Even if data is partially overwritten, the original files can often be reconstructed to some extent.

This creates a security challenge for enterprises as well as individual users. To help ensure data cannot be recovered, there are two options. The first is to securely encrypt data and ensure the security of user credentials and recovery keys for a system or external drive. Even if the physical media is

lost, stolen, or compromised, the data remains secure provided any credentials for decryption remain secure.

The second option is to use a sanitization feature named secure erase. As mentioned earlier, OS X provides tools to sanitize data by overwriting the original drive contents (or the portion of the drive marked as free space, which retains deleted files). There are varying levels of security offered depending on the number of passes and whether each path uses a specific data pattern or random data. Disk Utility in OS X offers multiple sanitization options for an entire volume or free space. A seven-pass erase option is available that meets U.S. Department of Defense standards (DOD 5220-22M).

Users can also initiate sanitization while deleting files using the Secure Empty Trash command in the Finder. This command overwrites files as they are deleted using a single-pass erase.

Remote Lock and Wipe

The OS X Server Profile Manager (as well as some third-party MDM solutions) offers a managed method for remotely locking and wiping a lost or stolen system. Many MDM solutions include a self-service portal where users can enroll Mac systems and download approved apps. Most MDM packages include the ability for users to remotely lock, wipe, and locate Mac systems and other devices using that self-service portal without assistance from IT.

Secure Networking

In today's mobile world, more and more devices are connecting to corporate resources from untrusted networks. OS X includes technologies that help the Mac connect to secure networks, authenticate users and systems, quarantine and validate incoming files, and protect data in transit. OS X also has features designed to prevent the accidental exposure of private information like contacts and location.

Strong Authentication

OS X integrates with many popular authentication systems, including Microsoft Active Directory, RADIUS, and 802.1x. These technologies give administrators control over user accounts and let users enjoy access to network services. OS X also offers support for digital certificates and multifactor authenticators, such as password token systems and smart cards.

Secure Transports

OS X includes standard enterprise virtual private networking (VPN) technologies. VPN protocols included with OS X include Cisco IPSec, L2TP, PPTP, and SSL-based VPN. OS X implements industry-standard SSL/TLS to aid in the secure transport of data at the application layer. Network credentials and configurations can be deployed through MDM, facilitating easy setup and deployment of VPN services to Mac systems.

Firewall

OS X has an application layer firewall allowing control over connections on a per-application basis in contrast to traditional port-based firewall systems (which are also available options using the built-in packet filter service). By default, Mac systems allow apps with a valid digital signature to receive incoming connections, which allows trusted apps from the Mac App Store access to the network and the Internet without configuration. Configurable firewall options provide a way to block all incoming connections, manage incoming connections for each app, and ignore Internet Control Message Protocol (ICMP) communications or pings. OS X also includes a traditional UNIX-based firewall to process traffic at the packet level: packet filter.

Quarantining

In OS X, downloaded files are tagged with special file system metadata. This process automatically marks files as potentially dangerous and quarantines them. The metadata propagates from ZIP archives, disk images, and similar digital containers to their contents, ensuring items remain quarantined. If the download contains executable code, its signature, code pattern, and other properties are examined against a list of known malware. If malware signatures are detected, OS X immediately

deletes the download and notifies the user. Apple maintains updated malware signatures and delivers them daily to Mac systems using Software Update.

OS X also tags executable files that aren't identified as known malware. The first time such a file is opened, OS X alerts the user and provides details about where the file originated and when. A user then has the choice to continue opening the item or delete it. If a user chooses to open an application not signed with a developer-provided digital signature, OS X dynamically signs the application. That signature is used to ensure application integrity—that it hasn't been tampered with or damaged each time it's opened.

App Privacy

Users often want to share their location, personal and professional details, and other information with a range of on-device and online services. Additionally, users may want to access data across a range of applications, Mac systems, and other devices. Revealing personal or confidential details as well as business data to unauthorized systems can create privacy and security breaches that may violate corporate policies, industry regulations, and local or national laws. OS X Security preferences contains a range of privacy options that can be managed across installed apps and services from a single central location.

Note: Diagnostic and usage data collected and sent to Apple will be protected and used in compliance with the Apple Privacy Policy, available at www.apple.com/privacy.

Conclusion

Security is an ever-present concern for IT teams in all organizations. OS X offers a solid set of security components built into every Mac. OS X also integrates with many industry-standard solutions and meets or exceeds stringent security guidelines from U.S. federal government agencies. In addition, Apple provides tools and guidance to IT departments wanting to further manage Macs in an enterprise setting.

For more information regarding OS X security, contact your Apple Authorized Reseller or Apple account team.

10/03/12