AUTOMATA

Technology Services

Privacy and Security - macOS

FileVault
Managing Privacy Settings
Managing Sharing Settings
Using Find My Mac

Introduction to FileVault

Lecture

FileVault

- Data encryption for Mac computers.
- Enforces the following…
- Encrypts data at rest.
- Requires a password to access encrypted data.
- Requires a password to login and unlock/wake a Mac.

Volume Ownership

- Introduced with Apple Silicon.
- Doesn’t have anything to do with physical ownership of the device.
- Refers to the user who first configured the Mac from initial setup.
- Organizations can also configure a bootstrap token to be an additional volume owner.
- The owner and the bootstrap token generate a secure token to use to create the recovery key for FileVault.

Recovery Keys

- A string of letters and numbers that the Mac creates to secure a FileVault Volume. Needed to turn off encryption.
- Enabling FileVault on Unmanaged Mac: Personal Recovery Key (PRK).
- Organizations can create and use an Institutional Recovery Key (IRK) - *Deprecated*.
- MDM solutions can escrow the Recovery Key and also rotate them.

FileVault Management

- MDM payload options include…
  - Recovery Key Management
  - When to turn-on FileVault and if it's required.
  - If a user can defer enabling encryption.
  - Token management.

Enabling FileVault

Practical Exercise

System Integrity Protection (SIP)

Lecture

System Integrity Protection (SIP)

- Ensures that specific Unix system folders cannot be modified by 3rd party software.
- Previous to Mac OS X 10.11 (El Capitan) the root user had full control to all folders.
- Folders protected using SIP include
  - /System
  - /usr
  - /bin
  - /sbin
  - /var

Enable / Disable SIP

Practical Exercise

macOS Malware Protection

Lecture

Gatekeeper & Notarization

- Determines if applications or processes can run.
- Requires code signing by an Apple Developer account.
- If malware is using a signing certificate, Apple can remotely update Gatekeeper to no longer trust that certificate and keep that malware from running.
- Users will get a trust warning and must override Gatekeeper to launch an unsigned application.

XProtect

- Built-in Anti-Virus and Anti-Malware software.
- Runs in the background and Apple updates definitions regularly.
- Has the ability to identify and then clean/remove/delete known viruses and malware.

Apple Security Response

- Associated Developer certificates are revoked.
- Notarization revocation tickets are issued (GateKeeper).
- XProtect signatures developed and released.
- Critical security update may be released.

Configuring Gatekeeper

Practical Exercise

Managing Software Updates

Lecture

Planning for Software Updates

- **Test**
  - Ideally, get involved with AppleSeed for IT.
  - Test beta releases thoroughly.
  - Defer software updates for up-to 90 days.
- **Deploy**
  - Deploy software updates via MDM when ready.
  - Manage App version updates accordingly.
- **Enforce**
  - Use MDM to specify if a Mac can defer updating.

Software Update Categories

- **Software Upgrades**
  - macOS 14 Sonoma to macOS 15 Sequoia
- **Software Updates**
  - macOS 15.0 to 15.1 or macOS 15.1 to 15.1.1
- **Security Responses and Security Updates**
  - Rapid Security Responses
  - Security Patches
- **Application Updates (App Store)**

Privacy Permissions and Settings for Mac

Practical Exercise

Configuring Sharing Settings for Mac

Practical Exercise

Using Find My Mac

Practical Exercise

Activation Lock on Mac

Lecture

Mac Activation

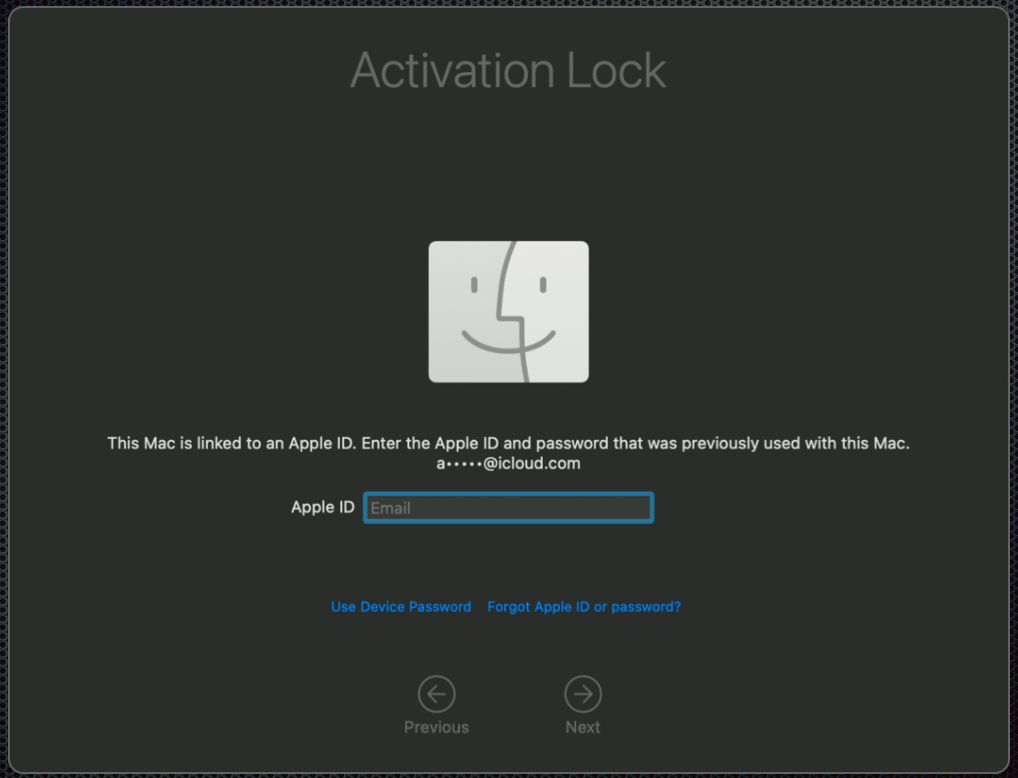

Image courtesy of Apple Inc

System Extensions & Kernel Extensions

Lecture

System Extensions

- Work in the background to extend your Mac's functionality.
  - Typically installed by third-party software applications.
  - Kernel extensions or 'kexts' are older style system extensions that are not as secure or reliable as newer system extensions.
  - Kernel extensions were deprecated with macOS X 10.15 - Catalina and starting with macOS 11 were no longer supported.
- System Extension Alerts
  - Will be prompted to install or allow a new System Extension when installed.
  - Warning that a system extension may be incompatible with a future version.
  - Could be prompted that the extension was not allowed to run.