Apple Platform Security

Introduction to Apple Platform Security

Lecture

Apple Platform Security

- Number of security features built-into Apple Platforms
  - Firewall & VPN
  - System Integrity Protection
  - Gatekeeper
  - XProtect
  - FileVault
  - Hardware Security (Secure Enclave, T2)

Developing a Security Strategy

Lecture

Secure By Design

- Apple's security mantra is 'Secure By Design'
  - A great user-first experience.
  - A deep integration between hardware, software, and services.
  - A commitment to providing a secure ecosystem.

Developing Your Strategy

- Device Enrollment
- Enforcing Security & Configuration Policy
- Monitoring Endpoints
- Managing Access
- Using an Identity Provider
- Using MFA or Passkeys

Microsoft Zero Trust

Lecture

Microsoft Zero Trust

- Microsoft's modern security model that focuses on explicit verification, least privilege access, and assumed breach.
- Zero Trust assumes that there was a security breach, or in other words it doesn't implicitly trust any authentication request regardless of where it originates.
- Uses micro-segmentation to ensure even if security is compromised in one area, it's limited and doesn't grant full access across the whole tenant.

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

Mac Firmware Security

Practical Exercise

Gatekeeper & XProtect

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.

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 with Intune

Practical Exercise

Digital Certificates

Lecture

Purpose

- Used to establish trust between two sources for the secure exchange of data.
- Encrypt network communications.
- Authenticate users to networks and services without the need for usernames/passwords.

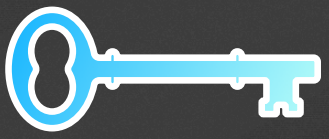
Structure

Anatomy of a Certificate

Certificate & Identity Formats

- A certificate and it's associated private key are known as an identity.
- Certificates can be freely distributed but private keys need to be kept secure. The public key must have a matching private key to decrypt.
- The private key is stored as a PKCS #12 - .p12 file.
- Apple supports .cer, .crt, .der, X.509 with RSA keys for certificate formats. They support .pfx and .p12 as identity formats.

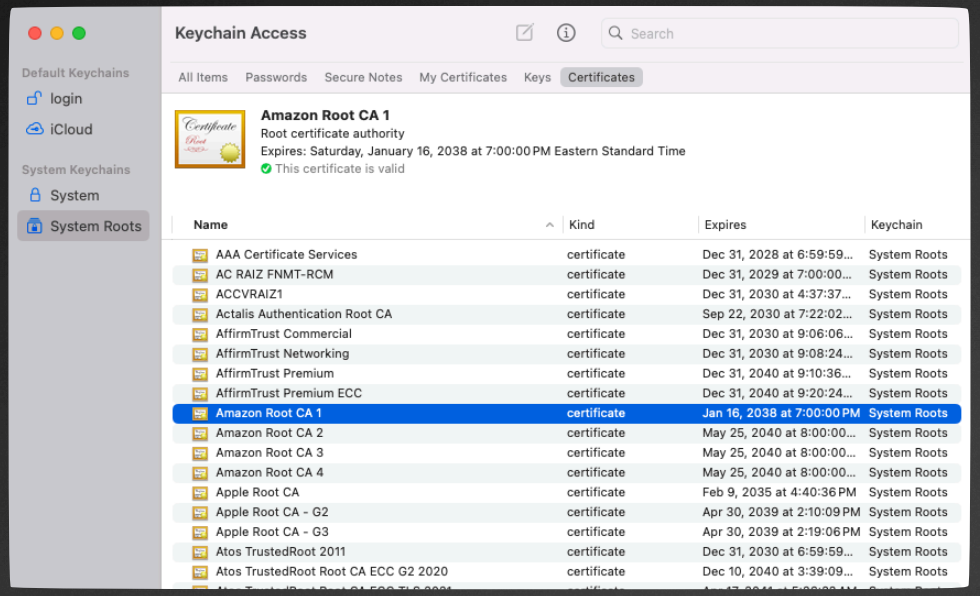
Public Key



Private Key

Trusting & Verifying Certificates

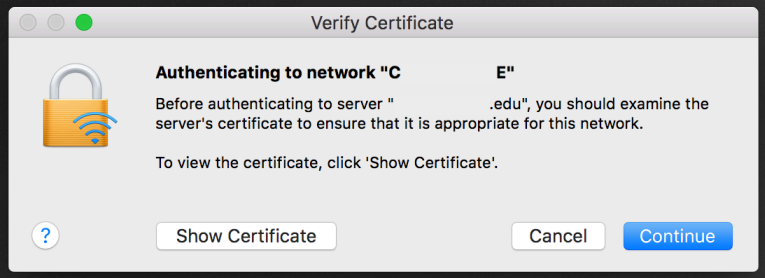
- A certificate is usually signed (verified) by a Certificate Authority.
- To evaluate a certificate's chain of trust, a device verifies the signature of the certificate and the root authority (anchor).
- Apple devices include a number of pre-installed root certificates called Trust Stores.



Built-in Trusted Root Certificates - via Keychain Access

Trust Stores

- Categories
  - Trusted certificates
  - Always Ask certificates
  - Blocked certificates
- MDMs provide the ability for organizations to distribute certificates and establish the cert as a root that it trusts.
- MDMs also allow for a payload to automatically not accept untrusted certificates.



Example of an Untrusted Certificate

Managing Digital Certificates

Practical Exercise

Apple Software Update

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.

Configuring Software Update

Practical Exercise