Monday, 27 September 2021

iOS/iPadOS security mechanisms - overview

- **On-device security**
  - Users cannot install potentially malicious unsigned apps.
  - Verification of memory pages load to ensure app has not been modified since it was installed.
  - Sandboxing: Apps are restricted from accessing other apps or make devices changes. Each has its own unique home directory.
  - Entitlements: Specific token permissions that an app requests for specific privileged operations that would otherwise require root access.
  - Address Space Layout Randomization[1]
  - Memory pages are marked as writable and executable for apps with Apple-only entitlements.
  - Packet filter(firewall)
- **Cloud-based security**
  - All apps must be signed with a certificate issued by Apple. The identity of an Apple developer is firstly checked before issuing a developer certificate with which apps can be signed.
  - Code signature validation of all dynamic libraries that processes of an app link at launch time.
  - Others:
    - End point protection: MRT*(Malware Removal Tool), eficheck(rootlet detection)*, Gatekeeper*(enforces code signing on apps to help ensure that only trusted software runs)*
    - Malware definitions: File quarantine, XProtect/YARA signatures, Plug-in unapproved list, Safari extension unapproved list

[1] Helps protect against the exploitation of memory corruption bugs.

References:

1. Security of runtime process in iOS and iPadOS: https://support.apple.com/guide/security/security-of-runtime-process-sec15bfe098e/1/web/1
2. App code signing process in iOS and iPadOS: https://support.apple.com/guide/security/app-code-signing-process-sec7c917bf14/1/web/1
3. App security overview: https://support.apple.com/guide/security/app-security-overview-sec35dd877d0/1/web/1