iOS Platform and Security

Overview

- Summarize the characteristics of the iOS platform
- Summarize the security design features of iOS
- Summarize significant security changes in recent iOS updates

iOS Basics

- Minor differences in OS between iPhone, iTouch and iPad
- Most restrictive platform
  - Apple controls device hardware and software
  - Apple does not allow Mobile Operator software
  - Closed source, proprietary platform
  - EULA prohibits attempting to derive source code
    - A significant issue in security testing

iOS Architecture

- Processors - ARM (Advanced RISC Machine) processors
  - iOS 7 and higher supports 64 bit processors
  - Only 64 bit apps permitted after 6/1/2015
- Kernel – XNU part of open sourced Darwin OS
- OS Platform – BSD UNIX, also used in OS X
  - Some UNIX command line tools use different parameters than Linux
- Executable Architecture – Mach-O also used in OS X
  - Executables, object code and shared libraries
- File System – Hierarchical File System – X with no removable storage

iOS Updates

- Apple distributes bundled updates with security updates and enhancements
- Occasional bug fixes distributed separately
- Can be installed immediately, or “tonight”

Model	Release(d)		Discontinued	Support			
	With OS	Date		Ended	Final OS[a]	Lifespan[b] Max[c]	Min[d]
iPhone 6s / 6s Plus	iOS 9.0	September 25, 2015	September 12, 2018	August 17, 2022	iOS 15.6.1 (15.8.1)	8 years, 3 months	5 years, 4 months
iPhone SE (1st)	iOS 9.3	March 31, 2016	September 12, 2018	still supported (last security update: January 22, 2024)		7 years, 9 months	5 years, 4 months
iPhone 7 / 7 Plus	iOS 10.0	September 16, 2016	September 10, 2019			7 years, 4 months	4 years, 4 months
iPhone 8 / 8 Plus	iOS 11.0	September 22, 2017	April 15, 2020	September 7, 2023	iOS 16.6.1 (16.7.5)	6 years, 4 months	3 years, 9 months
iPhone X	iOS 11.0.1	November 3, 2017	September 12, 2018	still supported (last security update: January 22, 2024)		6 years, 2 months	5 years, 4 months
iPhone XS/ XS Max	iOS 12.0	September 21, 2018	September 10, 2019	current	latest iOS	5 years, 4 months	4 years, 4 months
iPhone XR	iOS 12.0	October 26, 2018	September 14, 2021			5 years, 2 months	2 years, 4 months
iPhone 11	iOS 13.0	September 20, 2019	September 7, 2022			4 years, 4 months	1 year, 4 months
iPhone 11 Pro / 11 Pro Max	iOS 13.0	September 20, 2019	October 13, 2020			4 years, 4 months	3 years, 3 months
iPhone SE (2nd)	iOS 13.4	April 24, 2020	March 8, 2022			3 years, 8 months	1 year, 10 months
iPhone 12 / 12 Mini	iOS 14.1	October 23, 2020 (12) November 13, 2020 (12 Mini)	September 12, 2023 (12) September 7, 2022 (12 Mini)			3 years, 3 months	1 year, 4 months
iPhone 12 Pro /12 Pro Max	iOS 14.1 (12 Pro) iOS 14.2 (12 Pro Max)	October 23, 2020 (12 Pro) November 13, 2020 (12 Pro Max)	September 14, 2021			3 yeears, 3 months (12 Pro) 3 years, 2 months (12 Pro Max)	2 years, 4 months
iPhone 13 / 13 Mini	iOS 15.0	September 24, 2021	September 12, 2023 (13 Mini)	current	latest iOS	2 years, 3 months	4 months
iPhone 13 Pro /13 Pro Max	iOS 15.0	September 24, 2021	September 7, 2022	current	latest iOS	2 years, 3 months	1 year, 4 months
iPhone SE (3rd)	iOS 15.4	March 18, 2022		current	latest iOS	1 year, 10 months	
iPhone 14 / 14 Plus	iOS 16.0	September 16, 2022 (14) October 7, 2022 (14 Plus)				1 year, 4 months	
iPhone 14 Pro /14 Pro Max	iOS 16.0	September 16, 2022	September 12, 2023	current	latest iOS	1 year, 4 months	4 months
iPhone 15 / 15 Plus	iOS 17.0	September 22, 2023		current	latest iOS	4 months	
iPhone 15 Pro / 15 Pro Max	iOS 17.0	September 22, 2023				4 months	

Legend: Discontinued, bug fixes only | Discontinued, still supported | Current or still sold

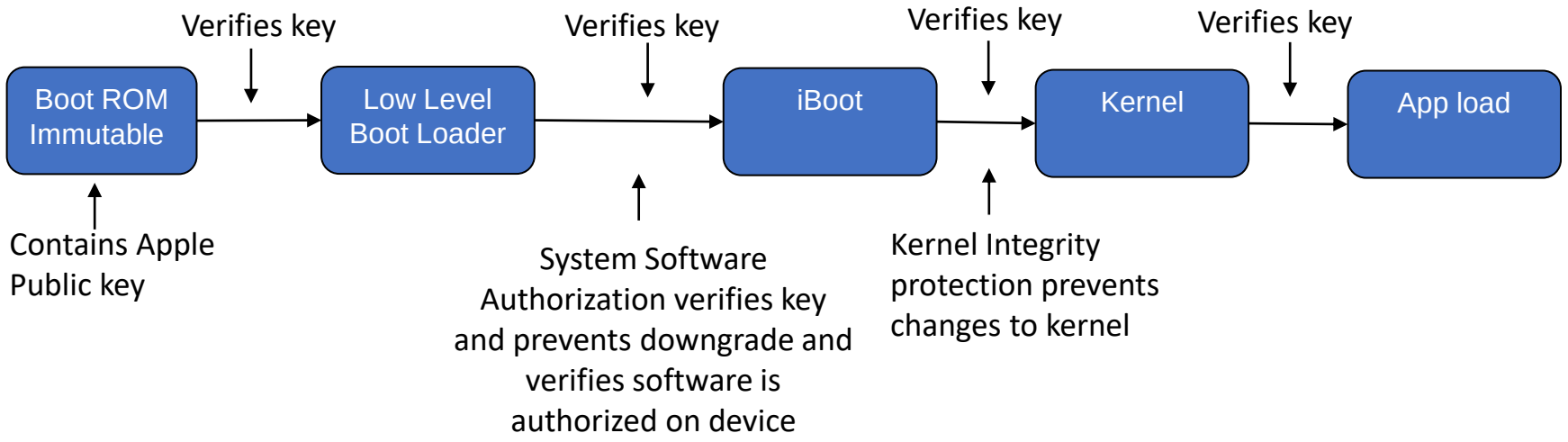
Little iOS Fragmentation

- Over 90% of devices sold in the last four years are on the current version
- No problems with integration with hardware OEMs or carriers because Apple controls the hardware.
- https://developer.apple.com/support/app-store/

iOS Security Design

Secure Boot Process

- Boot process starts with Boot ROM that has loader and Apple public key burned in.
- Public key is used to verify each piece of software that is loaded during boot and app load.



Legacy IPC before iOS 8

- Built-in API support for Facebook, Twitter sharing, not extensible
- Only alternative was custom URL handler data sharing
  - Current app opens custom URL with encoded data in parameters
  - Closes calling, switches to handler app
  - No user interaction required, access depends on what the developer exposes in the app
  - Example:
    - twitter:/ /post?message= hello%20world&in _reply_ to_ status _id= 12345
  - Pre-registered URLs documented here: https://iphonedevwiki.net/index.php/NSURL

URL Handler Inconsistencies

- URLs managed by Apple, including mailto, http, and sms, always invoke Apple applications
- Third-party URL handlers are not managed consistently
- Third-party apps can open *fb://post/user_message%2ohere* to post on another user's wall
- Other apps could register that same handler
  - If it belongs to Apple, their app will take precedence
  - Others will be linked to the last app to register the handle

Example URL Handler Vulnerability

- In 2014 a research analyst discovered that Chrome for iOS would prompt a user to accept a Facetime call before the Facetime app was launched
- This allowed an attacker to initiate Facetime from a malicious app and record audio and video until terminated by the user
- Could be done from any browser by redirecting to chrome for iOS

```
<html><head></head><body><Script>
if (navigator.userAgent.indexOf("CriOS") == -1) { // Not Chrome for iOS
location.href="googlechrome://www.example.com/urllove/"; } else {
location.href="facetime://user@example.com";
</script></body></html>
```

iOS Security Features

Apple Secure Enclave

- Secure coprocessor that includes a hardware-based key manager, which is isolated from the main processor
- Maintains the integrity of its cryptographic operations even if the device kernel has been compromised
  - https://support.apple.com/guide/security/secure-enclave-overview-sec59b0b31ff/web
- Researchers claim un-patchable vulnerability in Secure Enclave on older chips
  - https://9to5mac.com/2020/08/01/new-unpatchable-exploit-allegedly-found-on-apples-secure-enclave-chip-heres-what-it-could-mean/

Data Execution Protection (DEP)

- Marks memory locations as either writable or executable but not both (W^X)
- Enforced by the CPU
- Significantly reduces the opportunity for successful memory corruption attacks but does not completely prevent them
  - Attacker can use buffer overflow to write code to memory, but can't execute it
  - If attacker can anticipate memory locations, a technique known as return-oriented programming can use existing instruction in memory can be manipulated to execute code (ASLR makes this very difficult)

Address Space Layout Randomization (ASLR)

- Executables and libraries distributed with iOS are compiled to randomize their address locations at startup
- Randomizing the locations of system components makes it difficult for attackers to know exactly where to hook their code, in order to take over the system
- An incorrect guess crashes the system, so the potential impact is limited to DOS

iOS Walled Garden

- Primary control is the app store review
- The majority of iOS runs as the non-privileged user "mobile," as do all third-party apps
- Each app has a unique home directory for its files, which is randomly assigned when the app is installed
- File systems are isolated by:
  - Using a process similar to a chroot jail to restrict app to home directory
  - Preventing an app from gaining access to OS kernel
  - Preventing an app from obtaining root privileges through driver installation

iOS Walled Garden continued

- Apps can determine whether other applications are present on device by using the custom URL scheme provided by iOS (Inter-process communication)
- Must declare apps you will check in info.plist and they are supposed to be limited to your own

News

- 'Hot Garbage': Developers Are Not Pleased With Apple's Unlocked App Store (businessinsider.com)

Code Signing

- App developers must register and pay to become official iOS developers
- Are given a digital certificate with which to sign their applications
- Only digitally signed applications from authorized developers can be uploaded to App Store
  - Digital certificate ensures integrity of application, code cannot be tampered with after release

Code Signing continued

- App store signs downloaded apps with Apple private key
- App loading process uses public key from Boot ROM to verify private key
- Apps without correct private key are rejected by device

Code Signing continued

- Apple iOS Developer Program and iOS Developer Enterprise Program is used to ensure that users can trust authenticity and integrity of applications in App Store
  - Enterprise Program allows organizations to distribute their own internal apps
  - Recently changed to allow "unpublished" apps for enterprises
- Does not guarantee safety, but increases odds that application developers will be held accountable for their work
- Deters developers from publishing malicious code

Code Signing Exceptions

- Progressive web app
  - Not signed by App Store
  - Delivered from web, with offline access

File System Encryption

- Apple iOS devices always encrypt the flash (NAND) storage memory using the Unique ID (UID) key that is burned into the Apple processor when it is fabricated. The UID key is not accessible through any software functions or through any known hardware attacks.
- Every iOS device has a dedicated AES-256 crypto engine built into the DMA path between the flash storage and main system memory, making file encryption highly efficient.
- No software or firmware can read the UID or GID directly; they can see only the results of encryption or decryption operations performed by dedicated AES engines implemented in silicon using the UID or GID as a key.

File Data Protection

- Key system apps, such as Messages, Mail, Calendar, use Data Protection by default, and third-party apps installed on iOS 7 or later receive this protection automatically
- When a user applies a passcode to lock an iOS device, files on the filesystem can also be encrypted with a unique key that is only accessible to the applications that are granted an *entitlement* to access the file

File Data Protection - continued

- Levels of protection can vary based on developer preferences
  - **No protection**. The file is always accessible.
  - **Complete until first user authentication**. (Default) The file is inaccessible until the first time the user unlocks the device. After the first unlocking of the device, the file remains accessible until the device shuts down or reboots.
  - **Complete unless open.** You can open existing files only when the device is unlocked. If you have a file already open, you may continue to access that file even after the user locks the device. You can also create new files and access them while the device is locked or unlocked.
  - **Complete**. The file is accessible only when the device is unlocked.

iOS Permissions Model

- Apple's model is designed for user simplicity
- Many permissions are available and only controlled by the App Store review process or Apple approved APIs. They do not require user approval in install
- iOS requires developers to provide an informative screen requesting permissions for personal data and protected resources like Bluetooth and WiFi connections.

Source: https://developer.apple.com/design/human-interface-guidelines/privacy

Example Exploit of Permissions

- In 2008, the Aurora Feint application was pulled from the Apple App Store after it was reported that the application retrieved all the contacts from the address book and sent them to the Aurora Feint servers for storage and analysis. The application was later reinstated by Apple after the developer filed a grievance indicating that the data collection was part of a mechanism to support social network gameplay

iOS App Extensions

- App extensions give users access to app's functionality and content throughout iOS
- Users select extensions to place access to an app wherever they want
- Examples:
- **Share**
  - Enables apps to share photos, videos, websites, and other content with users on social networks and other sharing services
- **Photo Editing**
  - Embed filters and editing tools directly into the Photos or Camera app
- **File Provider**
  - Provide a document storage location that can be accessed by other apps
- **Document Provider**
  - create an app extension that lets users directly upload and download documents from remote storage in any compatible app

Source: https://developer.apple.com/app-extensions/

Potential App Extension Vulnerabilities

- Third party keyboards
  - Introduced in iOS 8 to compete with Android
  - These keyboards have access to the Internet and all keystrokes
  - User is warned of full access risk
  - Apple vets for legitimacy

Touch ID and Face ID

- Images are encrypted and sent to Secure Enclave for matching
- Reference:
  - https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf

Privacy - Emergency SOS

- Shortcut to place emergency call and disable biometric authentication
- Device will not unlock with Face ID or Touch ID
- Possibly directed against law enforcement as courts have ruled that biometric data is not protected by the 5th Amendment to the U.S. Constitution

iOS 17 Security and Privacy Enhancements

- Lockdown Mode
  - Targeted at people who might be targets of state sponsored attacks
  - Blocks “complex” web technologies
  - Blocks many incoming messages and Facetime unless you contacted them first