Key Features of iPhone Device and Data Security for Forensics Analysis

Matt Danda
Webster, University
December 2017

Abstract

This paper provides a broad overview of the security mechanisms implemented on modern iPhones. It begins with a high-level description of the iOS operating system, and then it covers the main security features that protect the device and data. Whenever possible, this paper describes various weaknesses and strengths of these features and how they impact the role of a forensic investigator.

Introduction

According to NIST, "When a mobile device is encountered during an investigation, many questions arise…The key to answering these questions begins with a firm understanding of the hardware and software characteristics of mobile devices." (Ayers, R., Brothers, S., Jansen, W., 2014, ES-1) This paper provides a broad overview of the security mechanisms in place on modern iPhones using the most recent version of iOS. It begins with a high-level description of the operating system, and then it covers the main security features that protect the device and data. The paper covers security issues from a forensics perspective, and, whenever possible, describes vulnerabilities.

This paper does NOT cover the following:

- Application security. Security issues related to iOS apps and programming iOS apps.
- iPhone X security. This device has new, unique features such as FaceID. Its vulnerabilities are not widely known.

What is iOS?

iOS is the operating system used in Apple iPhones. Originally unveiled in 2007 for the first iPhone, iOS has been extended to support other Apple devices such as the iPod Touch (September 2007) and the iPad (January 2010). Major versions of iOS are released annually. The current version, iOS 11, was released on September 19, 2017.

Not to be confused with MacOS, iOS is designed specifically for mobile devices with touch screens, while MacOS is used in traditional (Apple-branded) laptop and desktop computers. The two operating systems are separate, but they share a core set of open-source Unix components.

iOS runs on a variety of Apple devices, but the most notable is the iPhone. iPhone hardware is also updated regularly. The diagram below summarize the specifications of some the latest iPhones:

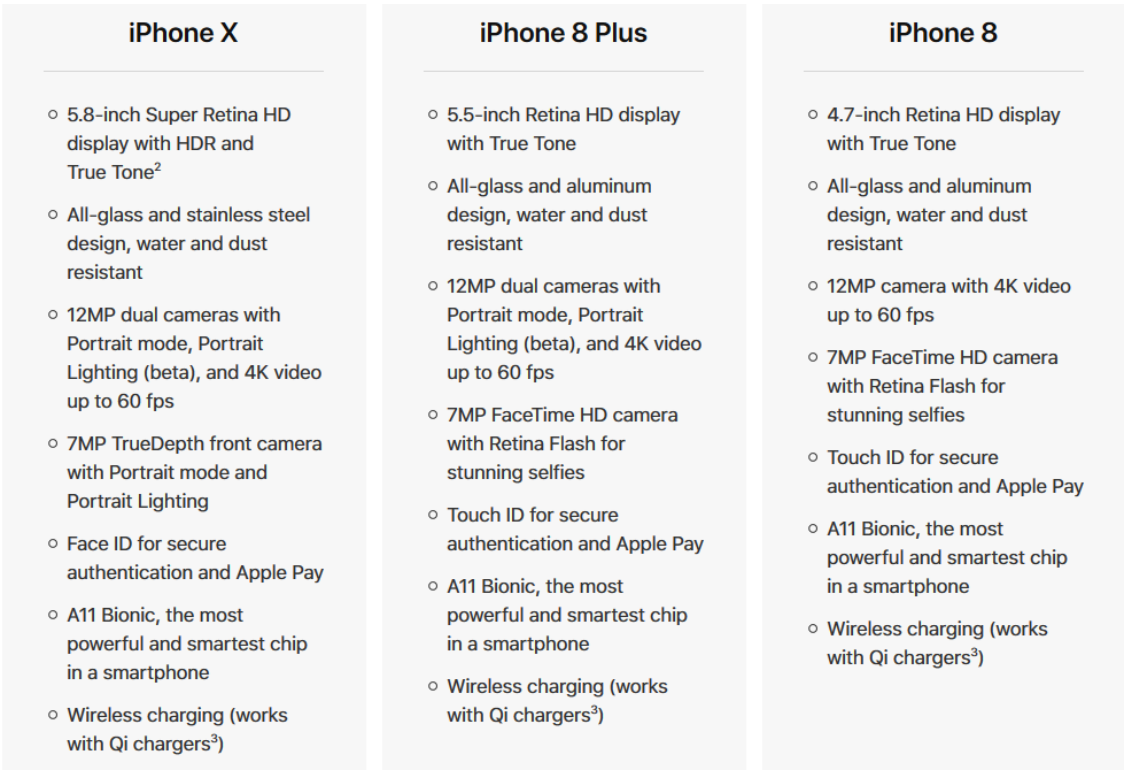

Figure 1: iPhone Specifications (Source: https://www.apple.com/iphone/compare/)

File System

This section describes how data is stored on the iPhone, which is of particular interest to a forensics investigator.

Apple File System (APFS)

Apple File System (APFS) is the latest file system developed by Apple. In the 1980s, Apple developed the Macintosh File System (MFS) to support floppy disk drives. When hard drives came on the scene in the mid-1980s, Apple introduced the Hierarchical File System (HFS) to overcome some of the performance problems of MFS. As hard drives got larger and larger, HFS was no longer sufficient, and, in 1998, Apple introduced HFS+ with MacOS 8.1. HFS+ added a variety of performance improvements. In 2017, to address the unique needs of solid state drives in particular, Apple announced APFS. According to the *Apple File System Guide* (2017):

> *Apple File System is a new, modern file system for iOS, macOS, tvOS, and watchOS. It is optimized for Flash/SSD storage and features strong encryption, copy-on-write metadata, space sharing, cloning for files and directories, snapshots, fast directory sizing, atomic safe-save primitives, and improved file system fundamentals.*

APFS Components

The major components of the APFS file system are:

- Container Superblock. The highest level in the file system that contains information about the entire APFS container.

- Checkpoint Superblock Descriptor. Information about meta-data structures in APFS.
- Bitmap Structures. Records used and unused blocks.
- Volume Superblock. The highest level in a volume.
- File and folder B-Tree. Records all files and folders in a volume.
- Extents B-Tree. A separate B-Tree of all extents (references to file content) per volume. A file with some content will have at least one extent. A fragmented file will have multiple extents.
- Snapshots. A user stored state of a volume at the time the snapshot was created.
- Checkpoints. A historical state of the container.

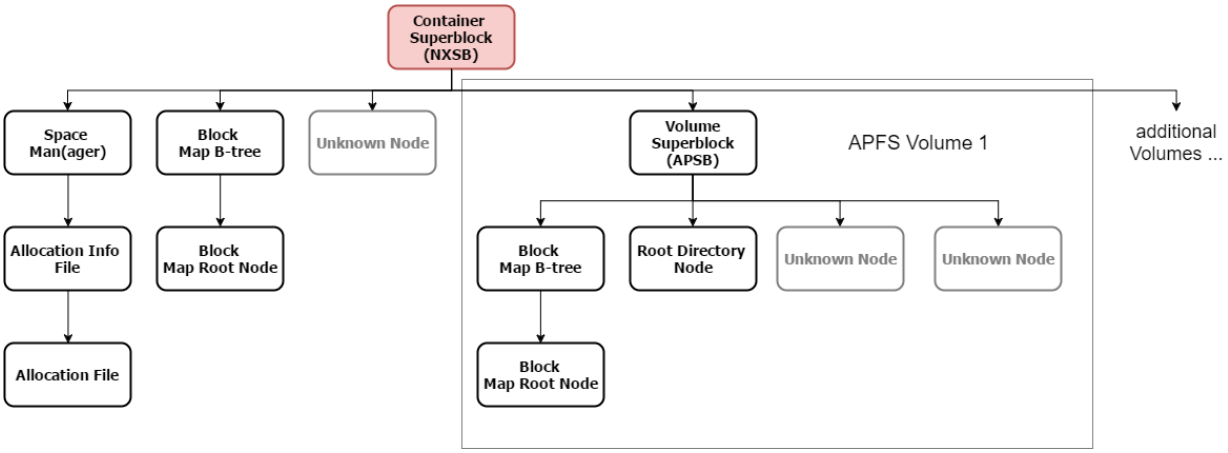

Figure 2: APFS Structure (Cogu's blog, 2017)

SQLite Databases

iOS uses SQLite to store user data. SQLite is an embedded database management system that is a popular choice for web browsers, operating systems, and devices such as mobile phones. SQLite stores the entire database (definitions, tables, indices, and the data itself) as a single cross-platform file on a host machine.

For forensics purposes, the most interesting SQLite databases on the iPhone are Call History, Address Book, SMS, and Maps. The file locations are:

- **Calls**: /private/var/mobile/Library/CallHistoryDB/CallHistory.storedata
- **Contacts**: /private/var/mobile/Library/AddressBook/AddressBook.sqlitedb
- **SMS**: /private/var/mobile/Library/sms.db
- **Maps**: /private/var/mobile/Applications/com.apple.Maps/Library/Maps/History.mapsdata

These databases can be extracted through applications available such as SQLite Database Browser (Mahalik, 2017).

iOS Operating modes

iOS can boot into one of three modes. A forensics investigator should be familiar with these modes:

- **Normal mode**. The mode used for regular activities. The Normal mode boot process consists of three steps: Low-Level Bootloader, iBook, and iOS kernel.

- **Recovery mode**. The device enters Recovery mode if any of the steps in the boot process fail to load or verify. This mode is also used to perform upgrades or to restore iPhone devices. To enter Recovery mode, follow these steps:
    - Turn off the device.
    - Use the USB cable to connect the device to a computer while holding the Home button.
    - Wait until the "Connect to the iPhone" screen disappears, then release the Home button.
- **Device Firmware Upgrade (DFU) mode**. DFU mode is a low-level mode for diagnostics. This mode is typically used to perform iOS upgrades. The forensic investigator also uses this mode for many data acquisition techniques. To enter DFU mode, follow these steps:
    - Use the USB cable to connect the device to a computer that has iTunes installed.
    - Hold the Home button and power button for 8 seconds.
    - Release the power button while still holding the Home button. The screen remains blank in DFU mode.

(Shaikh, H., 2017)

iOS Security Mechanisms

This section describes some of the security features that protect the iPhone device and data.

Passcode

The passcode is a numeric PIN used to unlock the device. The minimum length is six digits. iOS provides the option to configure an alphanumeric passcode if desired. If someone attempts to guess the passcode, the following delays are enforced after each failed attempt:

Attempts	Delay Enforced
1-4	none
5	1 minute
6	5 minutes
7-8	15 minutes
9	1 hour

Table 1: Delays between passcode attempts
(Apple, Inc., iOS Security Guide, p12)

If the Erase Data feature is turned on, the device will automatically wipe after 10 consecutive incorrect attempts to enter a passcode. As an added defense, Apple incorporated an iteration count that makes each attempt slower (iOS Security Guide, p.12). By their reckoning, it would take more than 5 ½ years to try all combinations of a six-character alphanumeric passcode with lowercase letters and numbers.

TouchID

TouchID is a fingerprint sensing system that enables users to unlock devices using fingerprint data. TouchID does not replace passcodes. However, with TouchID, users don't have to enter passcodes as frequently. As a result, TouchID makes it more practical to create longer, more complex passcodes (Apple, Inc., iOS Security White Paper, p7).

In the following situations, TouchID is intentionally disabled and passcodes are required to unlock the device:

- The device was just turned on or restarted.
- The device wasn't unlocked during the last 48 hours.
- The passcode hasn't been used in the last 6.5 days and TouchID hasn't been used in the last 4 hours.
- The device was locked remotely.
- There were five unsuccessful attempts to use TouchID.
- When setting up or configuring TouchID.

TouchID can be trained to recognize up to five different fingers. TouchID does not store any images of your fingerprint, and instead relies only on a mathematical representation. It isn't possible for someone to reverse engineer your actual fingerprint image from this stored data (Apple, Inc., 2017).

iOS Pairing

iOS enables you to connect the device to a computer and establish a trust relationship between the two. The computer can then gain access to the data on the iPhone, which is useful for features such as data synchronization. This feature is important to forensics investigators when performing logical acquisition of the iPhone data. However, various safeguards are in place to prevent an investigator (or an attacker) from simply plugging in a phone to a computer and acquiring the data.

In order to establish the trust relationship, the device must be unlocked. Prior to version 11 of iOS, a forensics investigator could use TouchID to unlock the phone and establish the relationship. Now, knowledge of the passcode is required.

This change is very important from the legal standpoint. In certain cases, the user may be legally required to unlock their device using their fingerprint. However, the passcode may have different legal protections that make obtaining it more challenging for investigators and, in many jurisdictions, not legally possible (Afonin, 2017).

The iPhone remembers indefinitely the computers or devices it has been configured to trust. In certain cases, a forensics investigator can use a trusted computer to gain access to the data on an otherwise locked iPhone. The investigator could also acquire the lockdown records, or pairing records, from the trusted computer, and use those records (along with forensics tools) to create a trusted relationship on an entirely different computer (ElcomSoft, 2016). However, in order to successfully unlock the device with a pairing record it is still essential that the iPhone in question remains powered on and is not allowed to shut down or reboot before the unlock is attempted (Afonin, 2017).

Users have the ability to cancel the trust relationship (Settings > General > Reset > Reset Location & Privacy). Once cancelled, the next time the device is connected to the formerly trusted computer, the Trust alert asks whether to trust that computer (Apple, Inc. 2017).

S.O.S Mode

S.O.S. mode is an emergency feature that gives users a new lockscreen with options to make an emergency call or display personal health information. Simply press the power button five times rapidly. This option temporarily disables TouchID, thereby preventing someone from unlocking your phone

while you're unconscious, for example. From a forensics perspective, this feature is interesting because a suspect could use the SOS mode to disable TouchID just prior to being arrested (Greenberg, 2017).

Keychain

The iOS Keychain protects short but sensitive pieces of data used by many apps, such as passwords, encryption keys, authentication tokens, and credit card numbers. The Keychain is a SQLite database, and Keychain items can only be shared between apps from the same developer (Apple, Inc., iOS Security Guide, p.13-15). iOS does not provide a user interface to view the Keychain contents. By design, each application can only access its own data in the keychain, and not system records or any other app's data (Katalov, 2017).

Remote Wipe

iOS devices can be erased remotely by an administrator or user. The mechanism works by discarding the block storage encryption key from Effaceable Storage, making all data on the device unreadable (Apple, Inc., iOS Security Guide, p.60). To help thwart a criminal from remotely wiping a confiscated phone, Nelson, Phillips, and Steuart (p462) recommend placing the device in a paint can that previously contained wave-blocking paint, or putting it into a specially designed bag that conforms to Faraday wire cage standards.

Secure Enclave

The Secure Enclave is a coprocessor within Apple A7 and later processors that provides all cryptographic operations for data protection (iOS Security Guide, p.7). On A9 or later processors, the chip generates the Unique ID (UID), which is unique to the device and not shared with Apple or any other devices. The UID changes every time the devices is rebooted and remains unknown to other parts of the system.

The Secure Enclave prevents the main processor from gaining direct access to sensitive data, and it supports a number of different services including TouchID and password verifications. The Secure Enclave runs its own operating system with its own kernel, drivers, services, and applications.

Very few technical details about the Secure Enclave have been released by Apple. However, in August of 2017, a hacker released what he claims to be a full decryption key for the Secure Enclave Processor firmware. While this key does not directly threaten the data on the iPhone, it could open the door for password harvesting, spoofing, and other security-compromising attacks (Viglilarolo, 2017).

According to Katalov (2017), "Secure Enclave has a severe effect on physical acquisition. Even with jailbreak and OpenSSH, the encryption keys required to decrypt the device image and keychain cannot be extracted from the device as they are well protected by Secure Enclave."

iOS Backup Security

iOS system backups are (and always were) the fastest and easiest way to obtain most data from the iPhone (Katalov, 2017). This section describes the methods that iOS uses to create backups and to secure the data on the backups. Apple provides backup options using both iTunes and iCloud.

iTunes System Backups

The iTunes backup option creates a backup file on a computer that can be used to restore that device's data to a new device. For obvious reasons, this backup file could be quite useful to a hacker or forensic analyst.

To create an iTunes system backup, connect the device to a computer with iTunes installed, establish the trust relationship (described previously in this paper), and use the Back Up Now feature in iTunes. In order to establish the trust relationship, the user must unlock the device using the passcode, not with TouchID. As discussed previously, the passcode provides a higher level of security than TouchID.

An iTunes backup includes nearly all of the device's data and settings, including call logs, internet history, saved credentials to most email accounts, social networks and instant messengers, and other information stored in apps (which may vary depending on how the apps were designed). iTunes provides the option to encrypt the backup, which also adds additional sensitive information to the backup file including Activity, Health, and Keychain data.

According to Apple, an iTunes backup does not include:

- Content from the iTunes and App Stores, or PDFs downloaded directly to iBooks (You can back up this content using Transfer Purchases in iTunes.)
- Content synced from iTunes, like imported MP3s or CDs, videos, books, and photos
- Photos already stored in the cloud, like My Photo Stream, and iCloud Photo Library
- Touch ID settings
- Apple Pay information and settings
- Activity, Health, and Keychain data (To back up this content, use Encrypted Backup in iTunes.)

As a result, if the backup file is not encrypted, it can only be restored to the same device. To restore the backup to a different device, the backup file must be the encrypted version that includes the additional data (Katalov, 2017).

iCloud Backups

The iCloud Backup feature automatically backs up devices over a Wi-Fi network connection and stores the information on the Apple iCloud. You don't need to plug your device into a computer or even be at home to back up with iCloud. iCloud backups are always encrypted.

According to Apple, iCloud backups include nearly all data and settings on the device except the following:

- Data that's already stored in iCloud, like Contacts, Calendars, Notes, My Photo Stream, and iCloud Photo Library
- Data stored in other cloud services, like Gmail and Exchange mail
- Apple Pay information and settings
- Touch ID settings
- iCloud Music Library and App Store content (If it's still available in the iTunes, App, or iBooks Store, you can tap to re-download your already purchased content.)

To use iCloud backup, connect the device to a Wi-Fi network and select to turn on the feature under Settings>iCloud. From a security perspective, note that anyone with the correct Apple ID credentials can obtain access to a device's iCloud backup files.

Conclusion

Introduced in 2007, the iPhone and the iOS operating system have been continually refined and improved over the years. Throughout this time, Apple has remained focused on improving security and privacy features. These features are of keen interest to hackers and forensics investigators alike. In this paper, we learned some of the basics of how the iPhone stores data using Apple's proprietary file system, APFS, and SQLite databases. We discussed the relationship between passcodes and TouchID, and how these features affect the security of pairing and SOS mode. This paper described how security is built into the processor itself using the Secure Enclave. Finally, we discussed how to create a backup of an iPhone's data using either iTunes or iCloud and some of the security issues that backups entail.

Sources

- Afonin, O. (September 7, 2017) “New Security Measures in iOS 11 and Their Forensic Implications” Retrieved from https://blog.elcomsoft.com/2017/09/new-security-measures-in-ios-11-and-their-forensic-implications/
- Apple, Inc. (2017) “About backups for iOS devices” Retrieved from https://support.apple.com/en-us/ht204136
- Apple, Inc. (2017) “About Touch ID advanced security technology” Retrieved from https://support.apple.com/en-us/HT204587
- Apple, Inc. (2017) “About the ‘Trust This Computer’ alert on your iPhone, iPad, or iPod touch” Retrieved from https://support.apple.com/en-us/HT202778
- Apple, Inc. (2017) *Apple File System Guide*. Retrieved from https://developer.apple.com/library/content/documentation/FileManagement/Conceptual/APFS_Guide/Introduction/Introduction.html#//apple_ref/doc/uid/TP40016999-CH1-DontLinkElementID_19
- Apple, Inc. (2017) *iOS Security*. Retrieved from https://developer.apple.com/security/
- Ayers, R., Brothers, S., Jansen, W. (May 2014) “Guidelines on Mobile Device Forensics.” National Institute of Standards and Technology.
- Cugu’s blog (2017, April 22) “APFS filesystem format.” Retrieved from https://blog.cugu.eu/post/apfs/
- ElcomSoft. (November 14, 2016) “Forensic Implications of iOS Lockdown (Pairing) Records.” Retrieved from https://articles.forensicfocus.com/2016/11/14/forensic-implications-of-ios-lockdown-pairing-records/
- Greenberg, A. (September 11, 2017) “APPLE’S IOS 11 WILL MAKE IT EVEN HARDER FOR COPS TO EXTRACT YOUR DATA.” Retrieved from https://www.wired.com/story/apples-ios-11-will-make-it-even-harder-for-cops-to-extract-your-data/
- Hansen, K.H., Toolan, F. (2017) “Decoding the APFS file system.” Digital Investigation. Retrieved from http://dx.doi.org/10.1016/j.diin.2017.07.003.
- Katalov, V. (November 2, 2017) “The art of iOS and iCloud forensics.” Retrieved from https://blog.elcomsoft.com/2017/11/the-art-of-ios-and-icloud-forensics/#more-4311
- Mahalik, H. (September 30, 2017) “TIME IS NOT ON OUR SIDE WHEN IT COMES TO MESSAGES IN IOS 11.” Retrieved from http://smarterforensics.com/2017/09/time-is-not-on-our-side-when-it-comes-to-messages-in-ios-11/.
- Nelson, B., Phillips, A., and Steuart, C. 2016. *Guide to Computer Forensics and Investigations*. Cengage Learning. Boston, MA.
- Shaikh, H. (July 25, 2017) “iOS Forensics.” Retrieved from http://resources.infosecinstitute.com/ios-forensics/#gref.
- Viglilarolo, B. (2017, August 17) “Hacker claims to have decrypted Apple's Secure Enclave, destroying key piece of iOS mobile security” Retrieved from https://www.techrepublic.com/article/hacker-claims-to-have-decrypted-apples-secure-enclave-destroying-key-piece-of-ios-mobile-security/