RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -24

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- iOS Security Framework
  - Introduction
  - iOS System Security
- Data Security in iOS
- App Security
- Network and Internet Services Security
- Issues with iOS security
  - iOS jailbreaking
- MCQ
- References

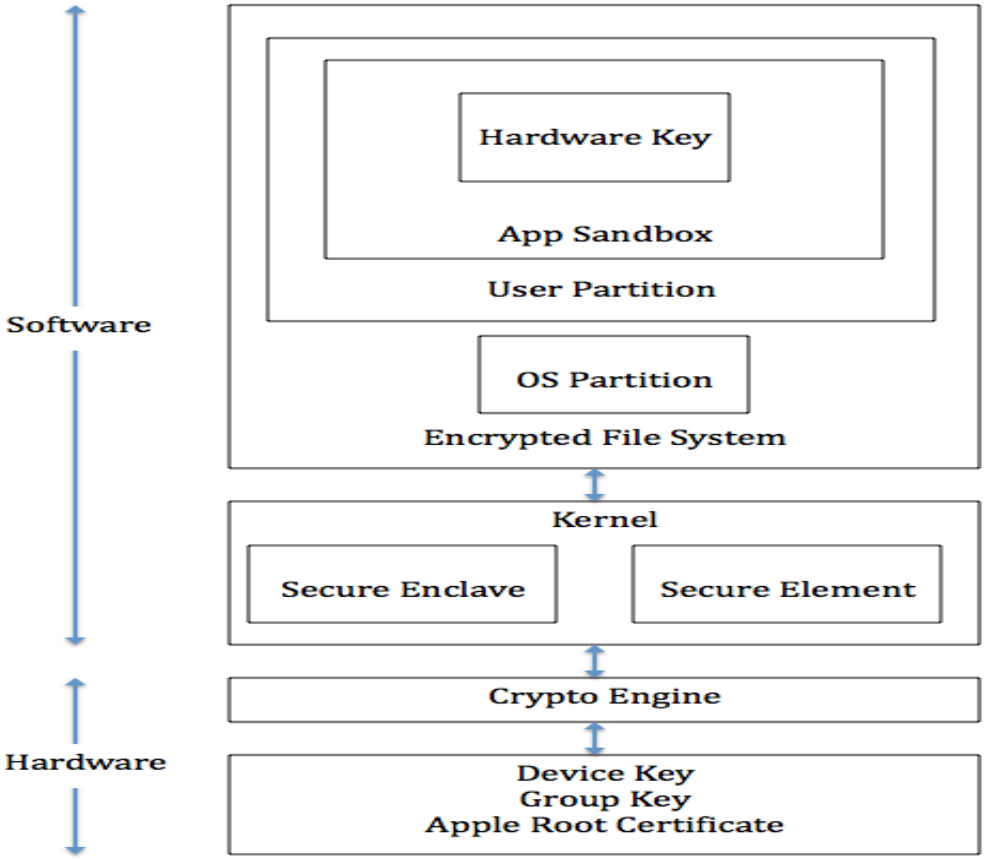
iOS SECURITY FRAMEWORK

Introduction

- iOS was designed and created by Apple Inc, it is distributed exclusively for Apple hardware.
- iOS protects not only the data stored in the iOS device, but also the data transmitted on networks when using internet
- services.
- iOS provides advanced and sophisticated security for iOS devices and itâ€™s also very easy to use.
- Users donâ€™t need to spend a lot of time on security configurations, as most of the security features have been
- automatically configured by iOS.
- iOS also supports biometric authentication (Touch ID), which has recently been incorporated into iOS devices, users can
- easily use their fingerprints to perform private and sensitive tasks such as unlocking the iPhone and making payments.

iOS System Security

System security is central to security in iOS. It makes the hardware and software securely integrated with each other such that every component in iOS is secure and trusted. Fig.1 is a high-level overview of iOS security architecture, the details are explained in the following sections.



1. Secure booting process

During the booting process, iOS uses a mechanism called "secure boot chain" to ensure that the low-level software is not compromised and iOS is running on a validated iOS device. Each step in secure boot chain verifies if the next step of chain is valid and signed by Apple. The booting process will only proceed to the next step of chain if the verification succeeds.

When you turn on an iOS device, the processor first executes the code from Boot ROM (read-only-memory). The code in Boot ROM is created during chip fabrication, hence it is trusted and immutable. The code in Boot ROM also contains the Apple Root CA public key, which will be used to verify if Low-Level Bootloader (LLB) is signed by Apple. If LLB is valid, the processor will run the next-stage bootloader, iBoot, which will in turn verify and run the iOS kernel.

2. Secure Enclave

The Secure Enclave is a coprocessor for Appleâ€™s A-series processor. It has its own secure boot separated from the application processor, communication between it and the application processor is highly encapsulated. Its tasks include key management, processing cryptographic operations and maintaining the data integrity.

Each Secure Enclave comes with a unique ID (UID) during the fabrication. Other parts of the system donâ€™t have access to UID, neither does Apple. UID is used to encrypt the Secure Enclaveâ€™s memory space and data of files stored in the file system.

The Secure Enclave is also responsible for decrypting and processing the fingerprints received from the Touch ID, verifying if the coming fingerprints match the registered fingerprints. The application processor forwards the fingerprints data to the Secure Enclave. Because the fingerprints data is encrypted with a session key between the Secure Enclave and the Touch ID, the application processor canâ€™t read it.

3. Touch ID Security

Touch ID is a fingerprints sensor that can read fingerprints from the user. A user who passes the fingerprints verification can have secure access to the device, such as unlocking the iOS device, making purchases from the App Store, and making secure payment through Apple Pay (More information in the Apple Pay section).

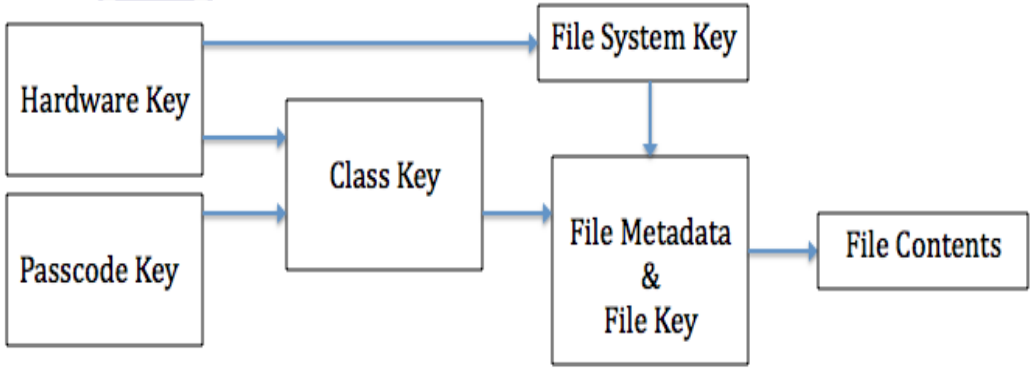
When the user touches the home button, the capacitive steel ring on the home button detects the finger and activates the Touch ID sensor. Then Touch ID scans the fingerprints and sends a 88-by-88-pixel, 500-ppi raster scan to the Secure Enclave for authentication. The scan is vectorized for analysis and temporarily stored in encrypted memory in the Secure Enclave. After authentication, it is discarded.

iOS SECURITY FRAMEWORK

Data Security in iOS

Besides making sure that only trusted code and apps can run on the devices, iOS also encrypts and protects userâ€™s data locally and remotely.

1. **Hardware security features**
2. **File Data Protection**
3. **Passcodes**
4. **Data Protection Class**
5. **Keychain Security**



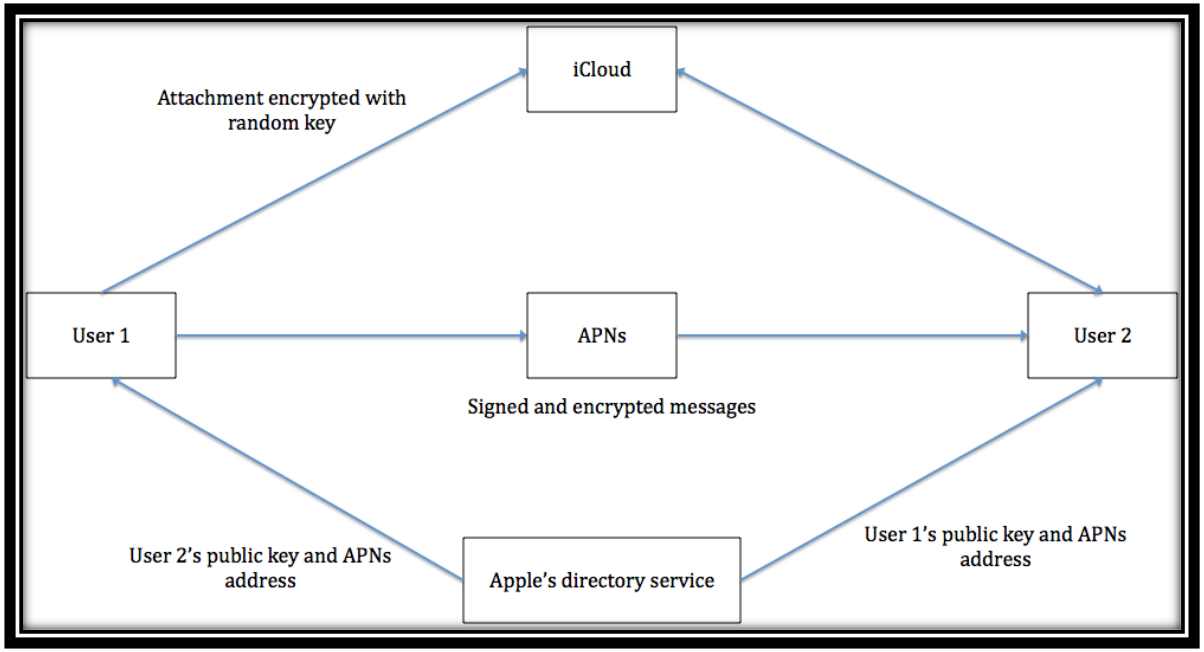
App Security

Applications are one of the most important elements in iOS. As of June 2014, Appleâ€™s App Store contained more than 1.2 million iOS applications, which have collectively been downloaded more than 60 billion times. While apps bring users incredible productivity and pleasing user experience, the existence of unauthorized malware is still a big threat to iOS security. To make sure all the apps running on iOS are not performing malicious tasks, Apple encores that all the apps must be reviewed and approved by Apple before being available on the App Store.

1. **App review and code signing**
2. **Runtime process security**
3. **Data Protection in Apps**

Network and Internet Services Security

1. SSL, TLS
2. Wifi
3. AirDrop security
4. iMessage Security
5. FaceTime Security
6. iCloud Security
7. Continuity and Handoff



iMessage Security

iOS SECURITY FRAMEWORK

Issues with iOS security

1. Benign apps could become evil
2. Unauthorized origin-crossing threats
3. Masque Attack
4. iOS jailbreaking
5. Privacy issues

After masque attack

iOS jailbreaking

iOS jailbreaking is the process of removing limitations on iOS, Apple's operating system on devices running it through the use of software and hardware exploits. The reason that many people want to jailbreak their iOS devices is because it gives users root access to iOS, making users have more privileges on customizing their iOS devices. Such privileges include installing applications or extensions that are not provided by Appleâ€™s App Store, and personalizing the user interface of iOS.

The biggest problem of jailbreaking is that it puts users into huge security risks since it disables the Sandbox feature of iOS. Sandbox is an important iOS security feature during runtime process, it separates the applications installed on the device such that apps are restricted from accessing files associated with other files during runtime. If a user installs a malicious app on the jailbroken iOS device, the malicious code will have access to address book, photos, location data and other private data without telling the user. Besides the security risks brought by jailbreaking, once a user jailbreaks his/her iOS devices, the warranty (AppleCare) provided by Apple will be void immediately. Meanwhile, as Apple has constantly been incorporating new features into the latest version of iOS, the benefits brought by jailbreaking are becoming less and less.

MCQ

Q 1 - How to get a response from an activity in Android?

A - startActivityToResult()

B - startActiivtyForResult()

C - Bundle()

D - None of the above

Q 2 -How to move services to foreground in android?

A - Services always work in Foreground only

B - No,We can't do this query

C - Using startService(Intent intent)

D - startFordgroud(int id, Notification notification).

Q 3 -What are the functionalities of Binder services in android?

A - Binder is responsible to manage the thread while using aidl in android

B - Binder is responsible for marshalling and un-marshalling of the data

C - A & B

D - Binder is a kind of interface

E - None of the above

Q 4 - What is the use of content provider in android?

A - To send the data from an application to another application

B - To store the data in a database

C - To share the data between applications

D - None of the above.

Q 5 -What is the 9 patch tool in android?

A - Using with tool, we can redraw images in 9 sections.

B - image extension tool

C - image editable tool

D - Device features

REFERENCES

- https://www.cse.wustl.edu/~jain/cse571-14/ftp/ios_security/index.html