iOS Security

Teacher:

Dr Tran Ngoc Minh

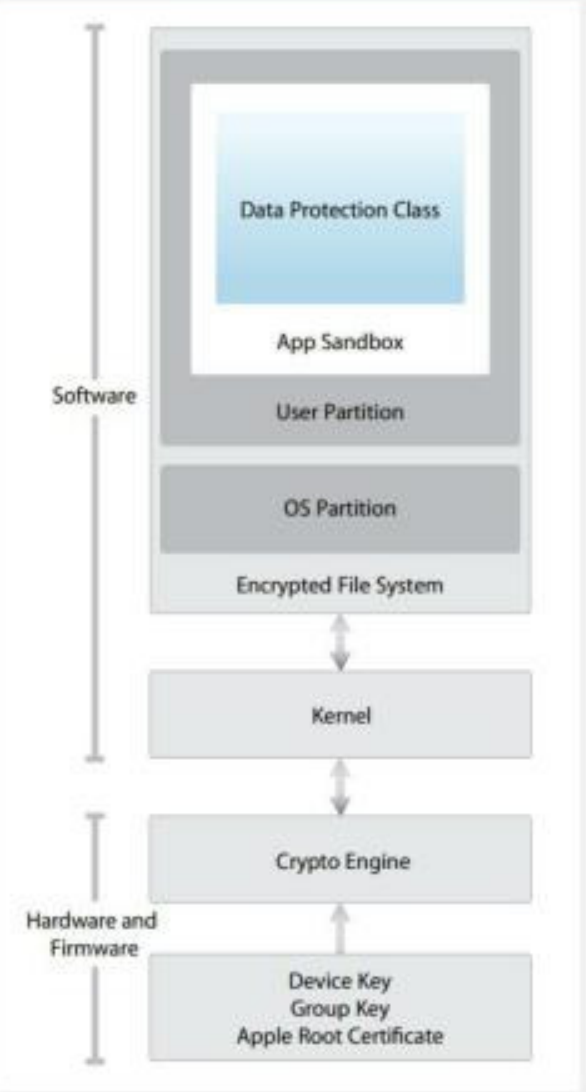
Group members:

Vo Tran Dang Khoa

Le Hoa

Introduction

- Every iOS device combines software, hardware, and services designed to work together for maximum security and a transparent user experience.
- iOS protects not only the device and its data at rest, but the entire ecosystem, including everything users do locally, on networks, and with key Internet services.
- iOS and iOS devices provide stringent security features, and they're easy to use.



iOS Security

- **System security**: The integrated and secure software and hardware that are the platform for iPhone, iPad, and iPod touch.
- **Encryption and data protection**: The architecture and design that protect user data if the device is lost or stolen, or if an unauthorized person attempts to use or modify it.
- **App security**: The systems that enable apps to run securely and without compromising platform integrity.
- **Network security**: Industry-standard networking protocols that provide secure authentication and encryption of data in transmission.
- **Internet services**: Apple's network-based infrastructure for messaging, syncing, and backup.
- **Device controls**: Methods that prevent unauthorized use of the device and enable it to be remotely wiped if lost or stolen.

System security

- Secure Boot Chain
- System Software Authorization
- Secure Enclave
- Touch ID

System security

- Secure Boot Chain
- System Software Authorization
- Secure Enclave
- **Touch ID**

Touch ID

- The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory to generate map of nodes.
- Touch ID can be trained to recognize up to five different fingers.
- With one finger enrolled, the chance of a random match with someone else is 1 in 50,000
- Touch ID can also be configured to approve purchases from Apple's stores.

Encryption and data protection

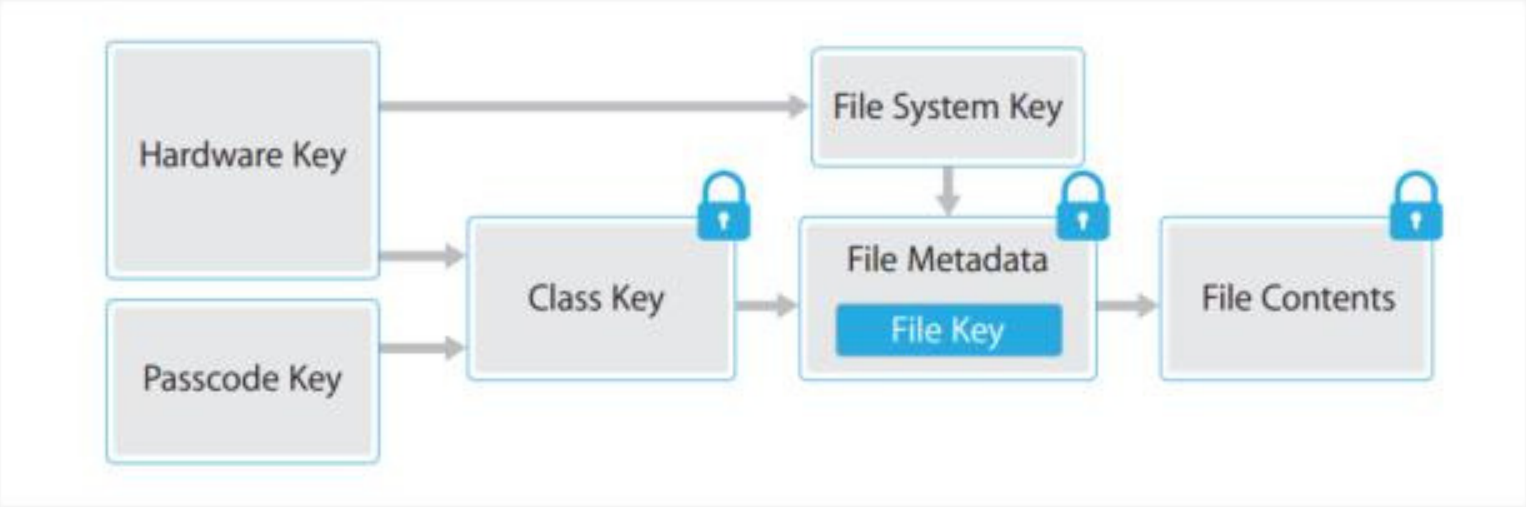
- Hardware Security Features
- File Data Protection
- Passcodes
- Data Protection Classes
- Keychain Data Protection

Encryption and data protection

- Hardware Security Features
- **File Data Protection**
- Passcodes
- Data Protection Classes
- Keychain Data Protection

File Data Protection

- Every time a file on the data partition is created, Data Protection creates a new 256-bit key (the "per-file" key).
- The per-file key is wrapped with one of several class keys, depending on the circumstances under which the file should be accessible.
- After that it is stored in a file's metadata, which is in turn encrypted with the file system key. The class key is protected with the hardware UID.



Internet Services

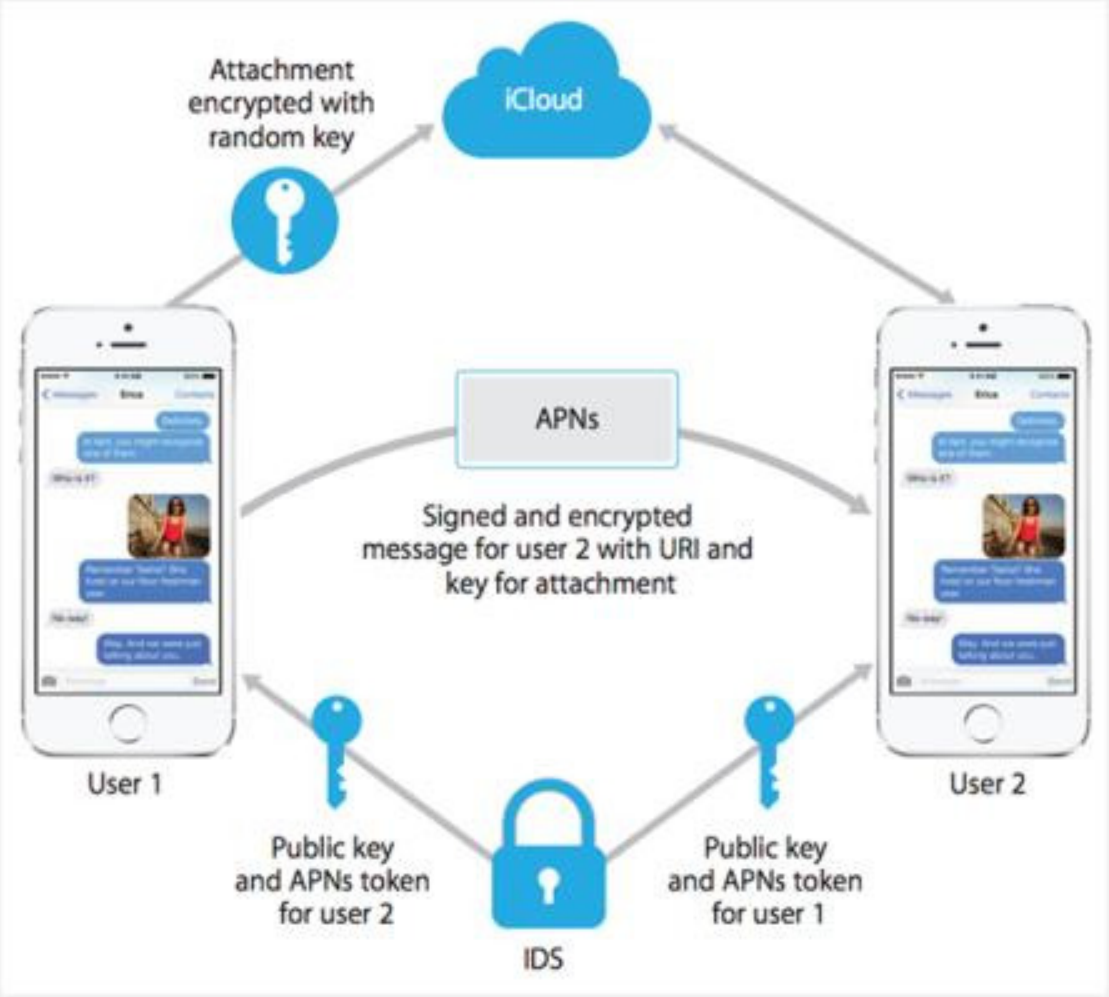
- iMessage
- FaceTime
- Siri
- iCloud
- iCloud Keychain

Internet Services

- **iMessage**
- FaceTime
- Siri
- iCloud
- iCloud Keychain

iMessage

- Two pairs of keys.
- The private keys are saved in the device's keychain and the public keys are sent to Apple's directory service (IDS).
- Public key to send and private key to receive messages.
- If the message text is too long, or if an attachment such as a photo is included, the attachment is encrypted using a random key and uploaded to iCloud.



Reference

- Apple (2/2014), *iOS Security document.*
- Greg Kumparak *(27/2/2014), Apple Explains Exactly How Secure iMessage Really Is,* <http://techcrunch.com/2014/02/27/apple-explains-exactly-how-secure-imessage-really-is/>.

Thank you for your attention !!