

Contents

- Terrorist attack in San Bernardino
- Investigations leading to terrorist's iPhone 5C
- Demands of FBI
- Reaction of Apple Inc.
- Introduction to iOS security
- Result of the court case
- Conclusion

Terrorist attack in San Bernardino

- On December 2, 2015, 14 killed and 22 injured at Inland Regional Center, SB, California.
- The perpetrators were **Syed Rizwan Farook and Tashfeen Malik** who targeted a public event.
- FBI was unable to unlock the recovered **iPhone 5C** with iOS 9 operating system issued to its employee, Syed, **due to its advanced security features.**

Investigations leading to terrorist's iPhone 5C

- Device's encryption technology was enabled, preventing the FBI from accessing its contents without knowing the device's 4 or 6 digit PIN.

NBC News reporting on it:

*“In a 40-page filing, the U.S. Attorney's Office in Los Angeles argued that it needed Apple to help it **find the password** and access **“relevant, critical data”** on the locked cellphone of Syed Farook, who with his wife Tashfeen Malik murdered 14 people in San Bernardino, California on December 2.”*

Demands of FBI

- Apple should create a unique version of iOS that would **bypass security protections** on the iPhone Lock screen.
- It would also add a completely new capability so that **passcode** tries could be **entered electronically**.
- Disabling the feature that **wipes the data** on the phone after **10** incorrect tries at entering a password.
- Thus making it easier to unlock an iPhone by “**brute force**,” trying millions of combinations without risking the deletion of the data.

Reaction of Apple Inc.

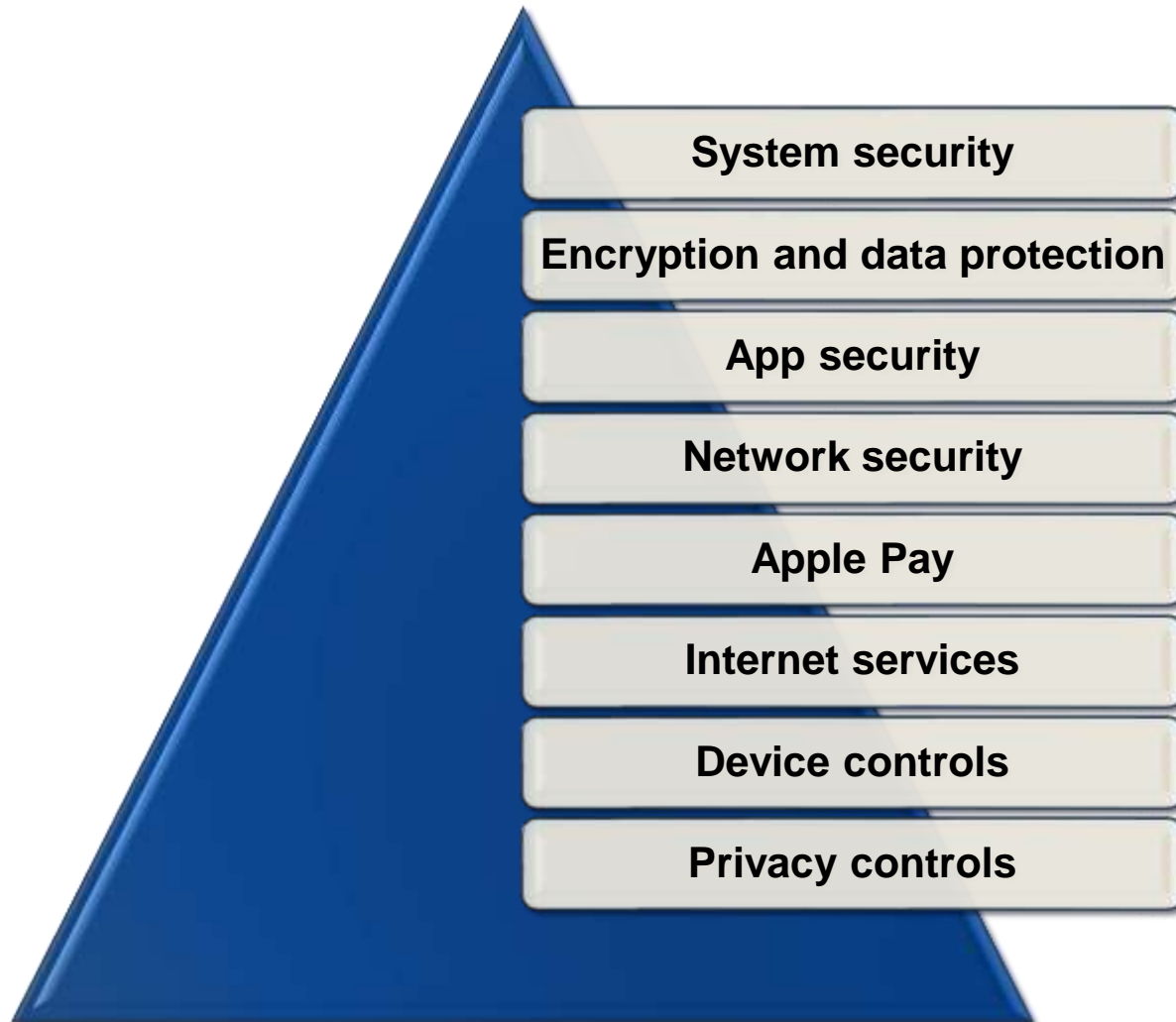
- Passcode lock & manual entry is the heart of the safeguards.
- Unlocking one iPhone would be the equivalent of a master key, capable of opening hundreds of millions of locks.
- Strongest suggestions offered was to pair the phone to a previously joined network, allowing FBI to back up the phone and get the data.
- The iPhone couldn't access iCloud services due to change in password by FBI.
- Handed over all the data it had, including a backup of the iPhone in question.

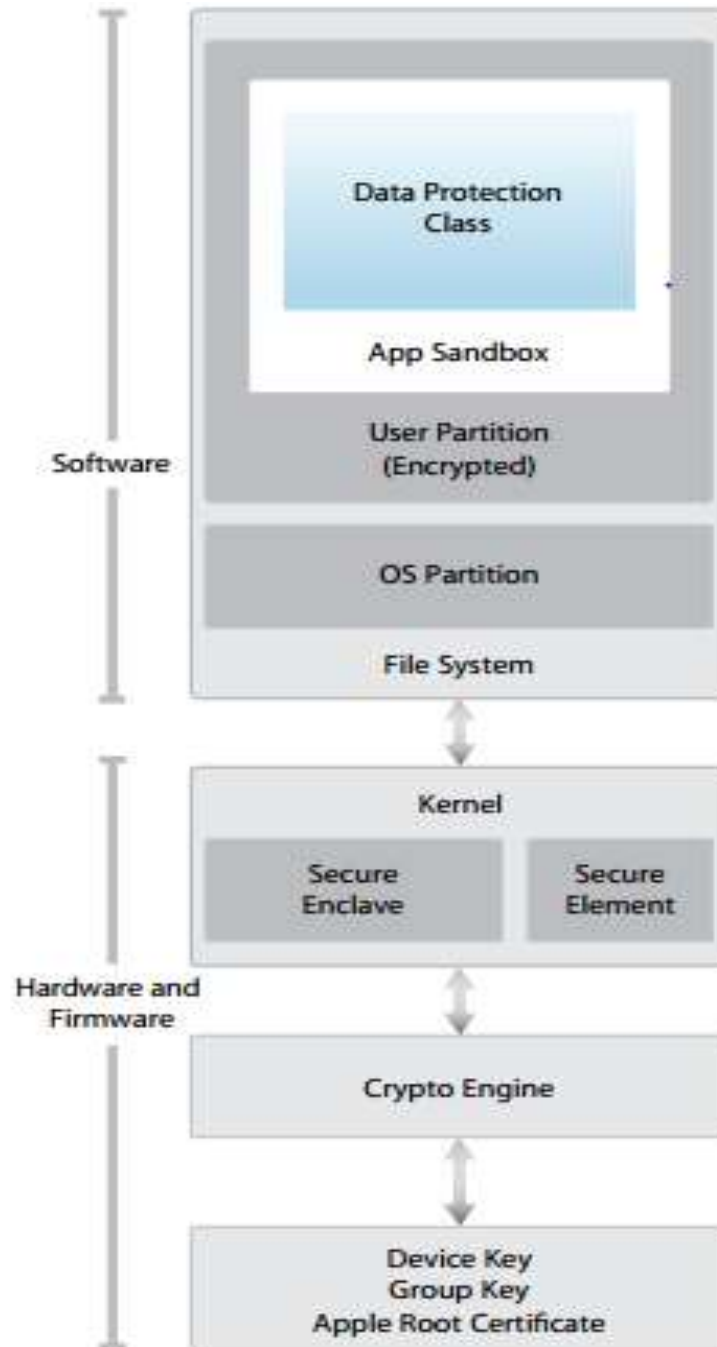
Introduction to iOS security

- Security kept at core, analyzing security hazards of the desktop environment.
- Every iOS device combines software, hardware, and services designed to work together for maximum security.
- After iOS 7, Apple decided to protect much more of the data **under the user's passcode**.
- Starting with iOS 8, all of the data on an iPhone is **encrypted on disk** with extremely strong encryption.



Security Classifications





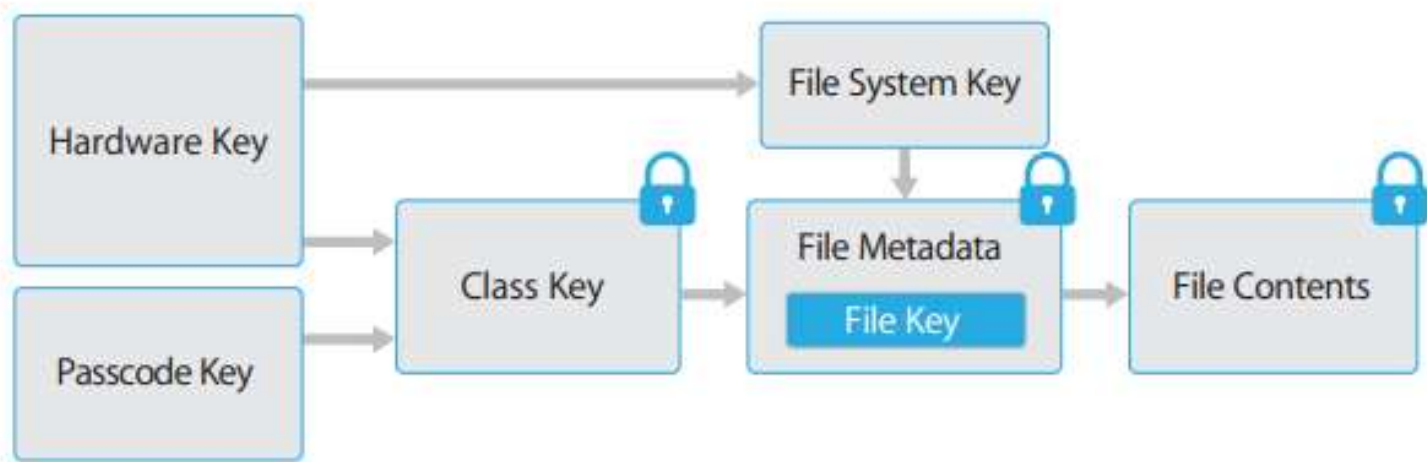
Security architecture diagram of iOS provides a visual overview of the different technologies

System security

- Boot-up process, software updates and Secure Enclave
- Secure boot chain
- System Software Authorization
- Secure Enclave

Encryption and data protection

- Hardware security features
- File Data Protection



- Passcodes

App security

- App code signing
- Runtime process security
- Extensions
- App Groups
- Data Protection in apps

Network security

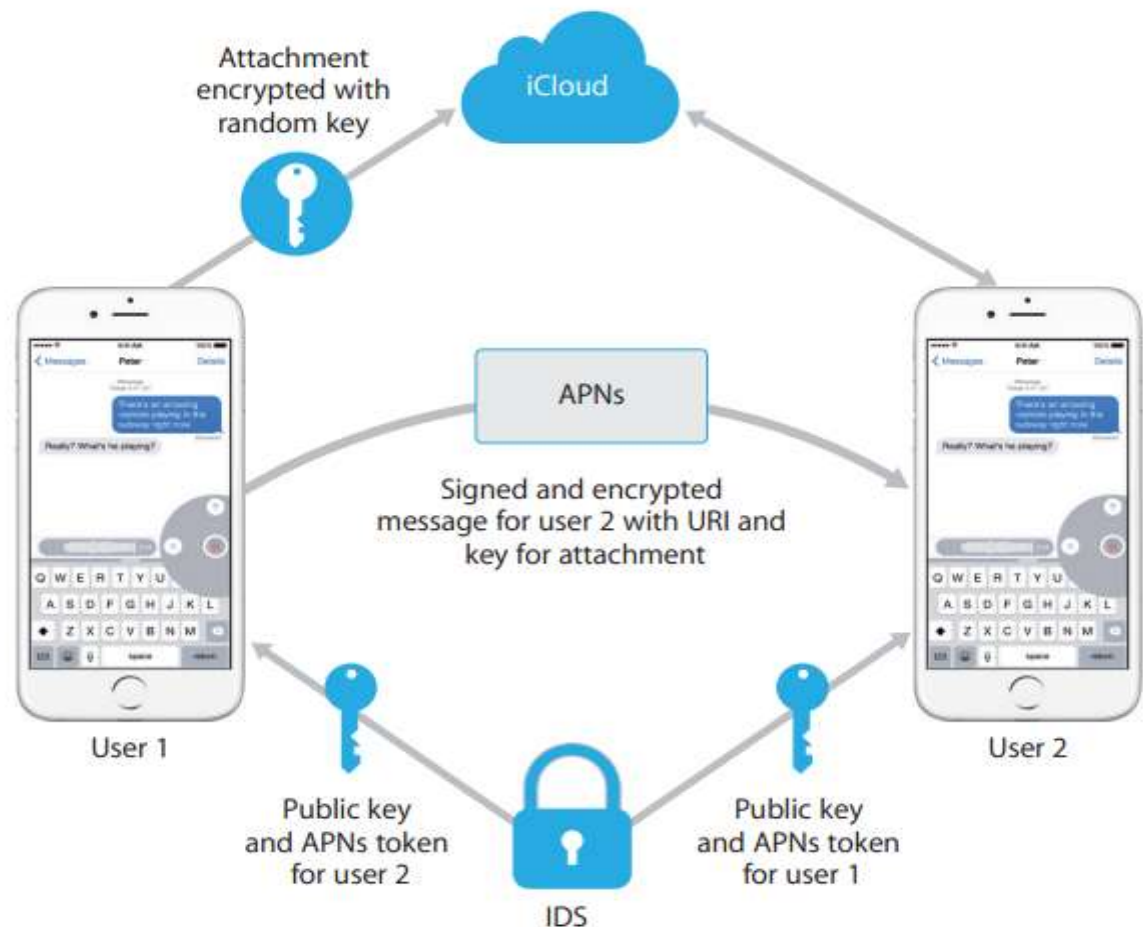
- TLS
- VPN
- WiFi
- Bluetooth

Apple Pay

- Apple Pay components
 - Secure Element
 - NFC controller
 - Wallet
 - Secure Enclave
 - Apple Pay Servers

Internet services

- Apple ID
- iMessage



For group conversations, this process is repeated for each recipient and their devices.

Device controls

- Passcode protection
- iOS pairing model
- Configuration enforcement
- Mobile device management (MDM)
- Device restrictions
- Remote wipe
- Find My iPhone and Activation Lock

Privacy controls

- Location Services
- Access to personal data
 - Contacts
 - Microphone
 - Calendars
 - Camera
 - Reminders

Result of the court case

“The government has now successfully accessed the data stored on Farook’s iPhone and therefore no longer requires the assistance from Apple Inc. mandated by Court’s Order” the filing reads.

- The filing doesn’t elaborate on the method used by FBI.
- Sources claim for relations between FBI and a 3rd party, probably an Israeli firm, **Cellebrite**, after whose help FBI withdrew the case.