Apple iOS 8 Security

Apple iOS 8 Security

Apple iOS 8 Security

What’s this all about?

“For all devices running iOS 8.0 and later versions, Apple will **no longer** be performing iOS data extractions as the data sought will be encrypted and Apple will not possess the encryption key.” -- Apple Legal Process Guidelines for Law Enforcement

Reactions?

“The notion that someone would market a closet that could never be opened – even if it involves a case involving a child kidnapper and a court order – to me does not make any sense”

“The notion that someone would market a closet that could never be opened – even if it involves a case involving a child kidnapper and a court order – to me does not make any sense”

“The company’s slovenly security on iCloud made it the butt of jokes for weeks [...] With the release of iOS 8, Apple made a privacy improvement so dramatic that it should rightly wipe out the taint of these security failures.”

“The notion that someone would market a closet that could never be opened – even if it involves a case involving a child kidnapper and a court order – to me does not make any sense”

“What concerns me about this is companies marketing something expressly to allow people to place themselves beyond the law.”

“The company’s slovenly security on iCloud made it the butt of jokes for weeks [...] With the release of iOS 8, Apple made a privacy improvement so dramatic that it should rightly wipe out the taint of these security failures.”

“The notion that someone would market a closet that could never be opened – even if it involves a case involving a child kidnapper and a court order – to me does not make any sense”

“What concerns me about this is companies marketing something expressly to allow people to place themselves beyond the law.”

“The company’s slovenly security on iCloud made it the butt of jokes for weeks [...] With the release of iOS 8, Apple made a privacy improvement so dramatic that it should rightly wipe out the taint of these security failures.”

“With iOS 8, Apple has finally brought their operating system up to what most experts would consider “acceptable security””

“The notion that someone would market a closet that could never be opened – even if it involves a case involving a child kidnapper and a court order – to me does not make any sense”

“What concerns me about this is companies marketing something expressly to allow people to place themselves beyond the law.”

"It is fully possible to permit law enforcement to do its job while still adequately protecting personal privacy,"

“The company’s slovenly security on iCloud made it the butt of jokes for weeks [...] With the release of iOS 8, Apple made a privacy improvement so dramatic that it should rightly wipe out the taint of these security failures.”

“With iOS 8, Apple has finally brought their operating system up to what most experts would consider “acceptable security””

“The notion that someone would market a closet that could never be opened – even if it involves a case involving a child kidnapper and a court order – to me does not make any sense”

“What concerns me about this is companies marketing something expressly to allow people to place themselves beyond the law.”

"It is fully possible to permit law enforcement to do its job while still adequately protecting personal privacy,"

“The company’s slovenly security on iCloud made it the butt of jokes for weeks [...] With the release of iOS 8, Apple made a privacy improvement so dramatic that it should rightly wipe out the taint of these security failures.”

“With iOS 8, Apple has finally brought their operating system up to what most experts would consider “acceptable security””

“The only actions that have undermined the rule of law are the government’s deceptive and secret mass surveillance programs.”

“The notion that someone would market a closet that could never be opened – even if it involves a case involving a child kidnapper and a court order – to me does not make any sense”

“What concerns me about this is companies marketing something expressly to allow people to place themselves beyond the law.”

"It is fully possible to permit law enforcement to do its job while still adequately protecting personal privacy,"

“With all their wizardry, perhaps Apple [...] could invent a kind of secure golden key they would retain and use only when a court has approved a search warrant.”

“The company’s slovenly security on iCloud made it the butt of jokes for weeks [...] With the release of iOS 8, Apple made a privacy improvement so dramatic that it should rightly wipe out the taint of these security failures.”

“With iOS 8, Apple has finally brought their operating system up to what most experts would consider “acceptable security””

“The only actions that have undermined the rule of law are the government’s deceptive and secret mass surveillance programs.”

“The notion that someone would market a closet that could never be opened – even if it involves a case involving a child kidnapper and a court order – to me does not make any sense”

“What concerns me about this is companies marketing something expressly to allow people to place themselves beyond the law.”

"It is fully possible to permit law enforcement to do its job while still adequately protecting personal privacy,"

“[...] With all their wizardry, perhaps Apple [...] could invent a kind of secure golden key they would retain and use only when a court has approved a search warrant.”

“The company’s slovenly security on iCloud made it the butt of jokes for weeks [...] With the release of iOS 8, Apple made a privacy improvement so dramatic that it should rightly wipe out the taint of these security failures.”

“With iOS 8, Apple has finally brought their operating system up to what most experts would consider “acceptable security””

“The only actions that have undermined the rule of law are the government’s deceptive and secret mass surveillance programs.”

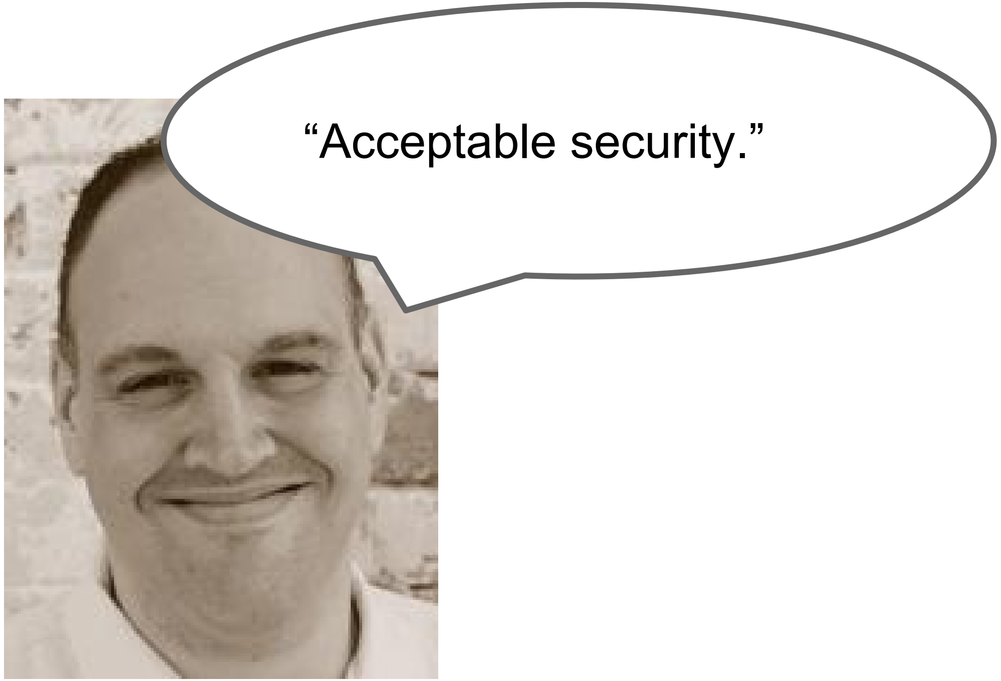
“The iPhone never had a “Backdoor”—just bad security design”

“People beyond the law.”

“A closet that could never be opened.”

“Dramatic security improvement.”

“Government’s deceptive and secret mass surveillance programs.”


“Acceptable security.”

"No backdoor, just bad security."

JUST SECURITY

A FORUM ON LAW, RIGHTS, AND U.S. NATIONAL SECURITY

The Washington Post

The Washington Post

So, what’s actually going on?

iOS Security Overview

- The Secure Enclave is a Coprocessor used for all Encryption, Decryption, and Key Management
    - Has it’s own secure memory for storing and processing information
    - Effaceable Storage is the only location to store/erase keys and in charge of erasing all references to them

iOS Security Overview

- The Secure Enclave is a Coprocessor used for all Encryption, Decryption, and Key Management
  - Has it’s own secure memory for storing and processing information
  - Effaceable Storage is the only location to store/erase keys and in charge of erasing all references to them
- Every device has a UID, GID and Apple Root Certificate
  - UID - Unique to a single device, unknown to Apple
  - GID - Unique to class of processors (e.g. A8 processor has a key common in all A8 processors)
  - Apple Root Certificate - Used for verifying Apple signatures (verifying software)

iOS Security Overview

- The Secure Enclave is a Coprocessor used for all Encryption, Decryption, and Key Management
    - Has it’s own secure memory for storing and processing information
    - Effaceable Storage is the only location to store/erase keys and in charge of erasing all references to them
- Every device has a UID, GID and Apple Root Certificate
    - 🔑 UID - Unique to a single device, unknown to Apple
    - 🔑 GID - Unique to class of processors (e.g. A8 processor has a key common in all A8 processors)
    - 🔑 Apple Root Certificate - Used for verifying Apple signatures (verifying software)
    - 🔑 Passcode - User defined password for accessing phone and contents

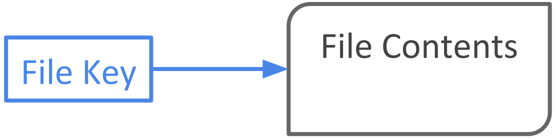
Local Storage

1. User creates a file

File Contents

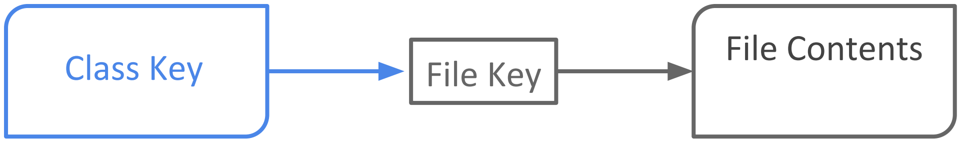
Local Storage

1. User creates a File
2. System creates a File Key specifically for encrypting that file



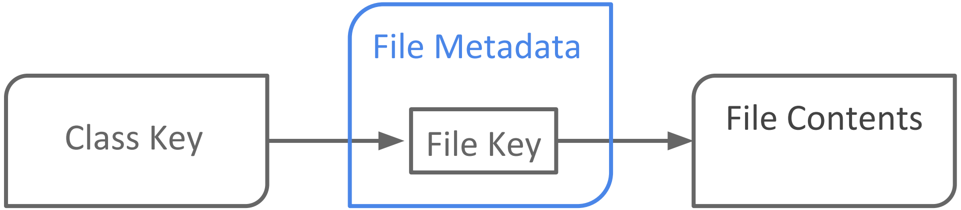
Local Storage

1. User creates a File
2. System creates a File Key specifically for encrypting that file
3. The file key gets encrypted by one of 4 class keys, making sure the file is accessed appropriately



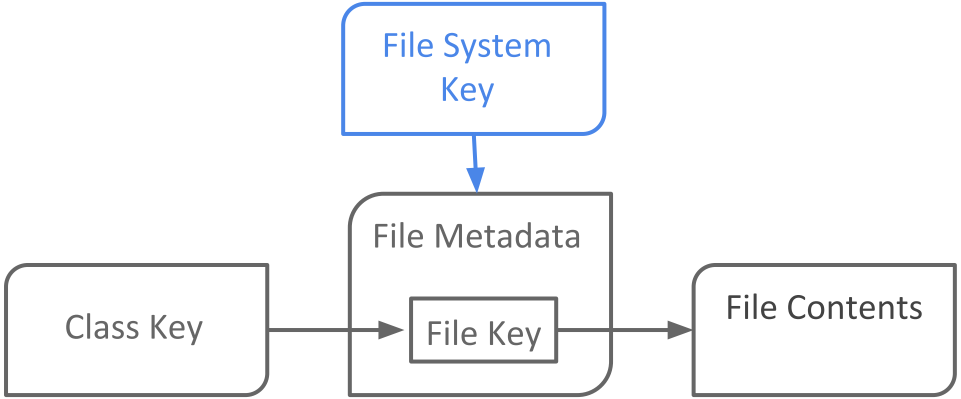
Local Storage

1. User creates a File
2. System creates a File Key specifically for encrypting that file
3. The File Key gets encrypted by one of 4 Class Keys, making sure the file is accessed appropriately
4. The encrypted File Key is stored in the File's Metadata



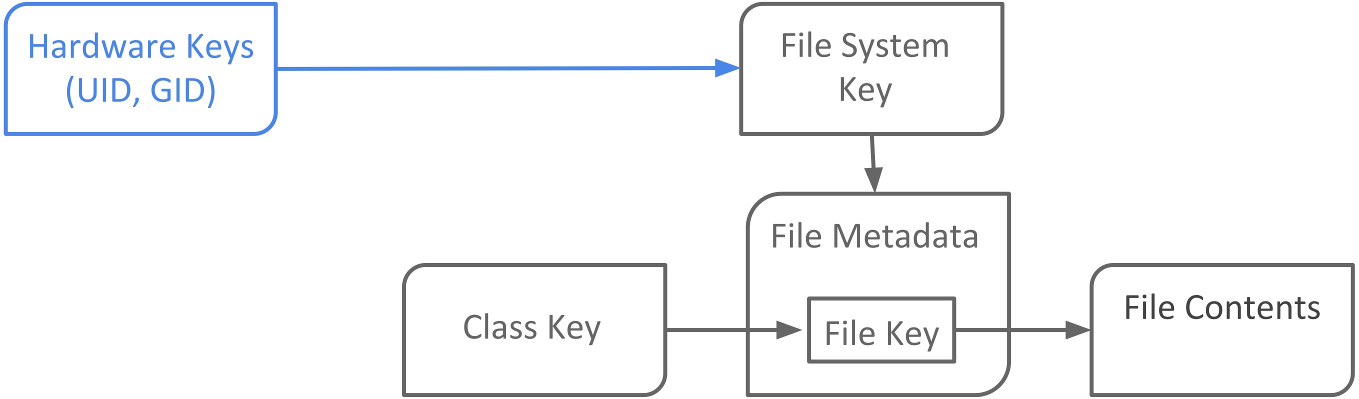
Local Storage

1. User creates a File
2. System creates a File Key specifically for encrypting that file
3. The File Key gets encrypted by one of 4 Class Keys, making sure the file is accessed appropriately
4. The encrypted File Key is stored in the File's Metadata
5. The File Metadata is encrypted with the File System Key



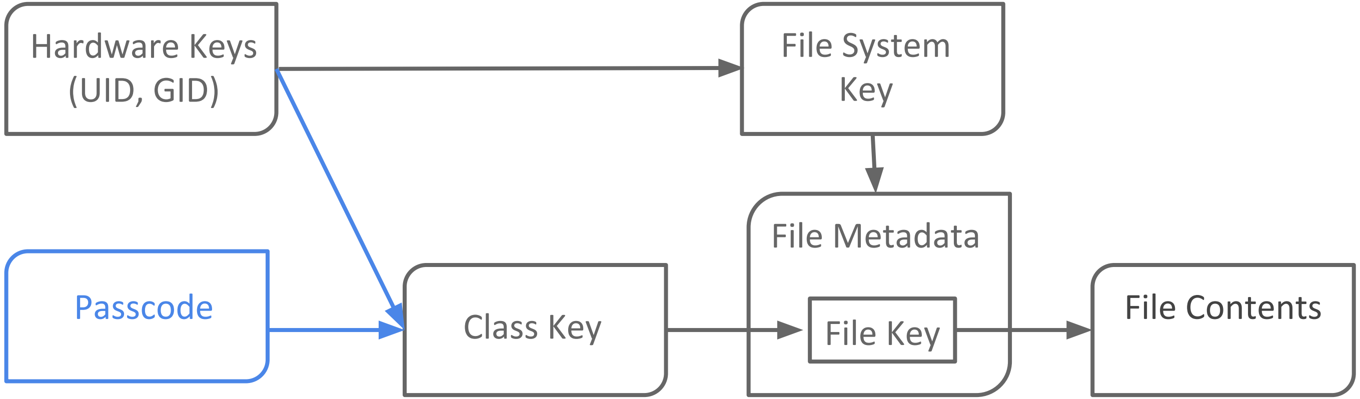
Local Storage

1. User creates a File
2. System creates a File Key specifically for encrypting that file
3. The File Key gets encrypted by one of 4 Class Keys, making sure the file is accessed appropriately
4. The encrypted File Key is stored in the File's Metadata
5. The File Metadata is encrypted with the File System Key
6. The File System Key is encrypted by the UID and the GID



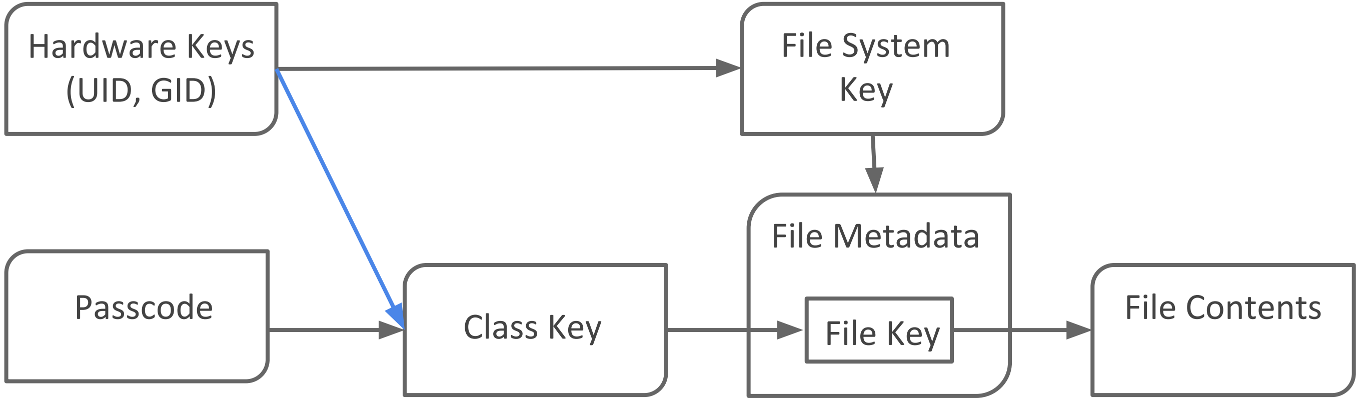
Local Storage

1. User creates a File
2. System creates a File Key specifically for encrypting that file
3. The File Key gets encrypted by one of 4 Class Keys, making sure the file is accessed appropriately
4. The encrypted File Key is stored in the File's Metadata
5. The File Metadata is encrypted with the File System Key
6. The File System Key is encrypted by the UID and the GID
7. 3 out of 4 Class Keys are encrypted by Passcode, UID, and GID (One wrapped by UID and GID)



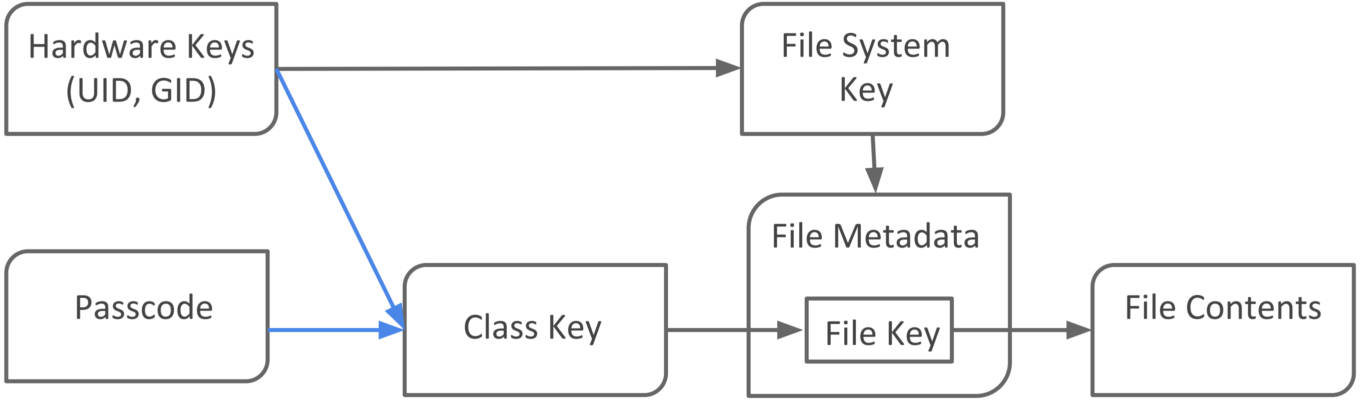
File Classes

- No Protection
  - Only encrypted using UID/GID, same level of encryption as before iOS8



File Classes

- No Protection
  - Only encrypted using UID/GID, same level of encryption as before iOS8
- Protected Until First User Authentication
  - Files are locked until the user first opens them, protects against reboot attacks
- Protected Unless Open
  - The device can be locked but the file open, if not opened the file is protected
- Complete Protection
  - Accessible only on an unlocked device



The “Backdoor”

Before

- “The iPhone never had a ‘backdoor’-just poor security design” **- Julian Sanchez**
- Apple could decrypt files by signing and running an alternate boot-loader that told the device to decrypt all files without asking for a passcode

The “Backdoor”

Before

- “The iPhone never had a ‘backdoor’-just poor security design” **- Julian Sanchez**
- Apple could decrypt files by signing and running an alternate boot-loader that told the device to decrypt all files without asking for a passcode

What’s New

- More files default to more secure file classes
- 3 out of 4 file classes are encrypted using UID/GID <u>and</u> passcode
    - ○ Apple has no access to passcode and therefore cannot decrypt using previous method

Security Incentives

- Apple must balance between usability and security
  - Even when Apple recognizes a threat to their security, it may be difficult to find a user-friendly solution
  - "Four-digit pins are more secure than having no passcode—but they're more annoying to use. And having no passcode at all is the simplest option for the user, but it offers no security"
- Biggest threats to mobile device security:
  1. Friends/Acquaintances/Significant others snooping on your device
  2. Theft of device by common criminals
  3. Targeting of your data by sophisticated attackers
- Previous versions of iOS protected fairly well against 1 and 2, a simple passcode would prevent snoopers and common criminals from gaining access
- Apple and Apple users were not overly concerned at the time about sophisticated attackers (more advanced criminals, law enforcement, government agencies …)

Updated Security Incentives

- Apple users become more aware and thus more concerned about sophisticated criminals
  - Need for better security against the third category of attackers
  - New security changes give users the impression they are more protected, in reality they are still not adequately protected against sophisticated security attacks (like those of law enforcement)

The Real Vulnerability : User Friendliness

- Escrow Keybag
  - A collection of keys that allow access to all of your backup data
  - It’s stored on devices you have paired with the phone (computer, iPad, etc)
  - Allows phone to be reset in case of lost passcode
- Jonathan Zdziarski
  - Trains Police in how to break iOS devices
  - You can access your locked phone contents from a desktop (it’s so user-friendly)
    - This allows current commercial forensic tools to get your camera reel, videos, any recordings, anything on iTunes, all 3rd party application data
    - This requires access to the paired device

Threat Models

Attacker possesses GID (easily obtainable)

- What can the attacker do?
- Not much, since the Class Key is derived from the UID + GID

Attacker possesses GID + UID (not practical, but theoretically possible to get UID)

- What can the attacker do?
- Before iOS-8 the attacker could access all files
- with iOS-8 the attacker can only access files in “No Protection” class

Threat Models cntd.

Attacker possesses GID + UID + user passcode (generally hard to do, only user should know the user passcode)

- What can the attacker do?
- Attacker can access all file types

Attacker gains access to iCloud of user (can be easy if password chosen badly, no two step verification setup)

- What can the attacker do?
- Attacker can access any files backed up on the iCloud

Threat Models cntd.

Attacker gains access to macbook of user (easy enough for law enforcement)

- What can the attacker do?
- Use recovery to get the escrow keybag and gain access to the files on the phone

Attacker forges Apple Root Certificate (hard to do)

- What can the attacker do?
- Before iOS-8, the Root Certificate could be used to decrypt all files
- With iOS-8 only files in no encryption class

Bibliography

Apple iOS8 Security Doc

Gizmodo's Article about Zdziarski Finds

Jonathan Zdziarski's Blog about iOS 8 Vulnerabilities

Apple iOS7 Technical Document

Apple Backdoor before iOS8

iOS Encryption General Overview

Apple Legal Process Guidelines

Bibliography cntd.

http://www.bloomberg.com/news/articles/2015-01-06/new-york-prosecutor-calls-for-law-to-fight-apple-data-encryption

http://www.theguardian.com/commentisfree/2014/sep/30/iphone-6-encrypted-phone-data-default

http://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html

http://appleinsider.com/articles/14/09/17/apple-says-incapable-of-decrypting-user-data-with-ios-8-even-for-government-agencies

http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf

http://support.apple.com/en-us/HT202303

Bibliography cntd.

http://appleinsider.com/articles/14/09/30/us-attorney-general-voices-concern-over-apples-ios-8-security-features

http://h30499.www3.hp.com/t5/Fortify-Application-Security/Mobile-Security-Threat-Modeling-Apple-s-TouchID/ba-p/6215627#.VNwXR53F-xV

Apple iOS 8 Security