iOS Security

9 May 2018

But First

- https://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conversation.html
- https://www.theverge.com/2018/5/8/17332480/google-maps-augmented-reality-directions-walking-ar-street-view-personalized-recommendations-voting

Apple Devices

iOS, not Mac OS

Source

- https://www.apple.com/business/docs/iOS_Security_Guide.pdf

- This tells many of the high level concepts, but does not get into the bits and blips of security at Apple.

Introduction of the iPhone

- Introduction: 29 June 2007
- The Steve Jobs reality distortion field.
- Steve Jobs introduces the iPhone: 3 minutes
- https://www.youtube.com/watch?v=MnrJzXM7a6o

Apple vs Android

- All software running on Apple iOS is blessed and approved by Apple.
- You can get an iPhone directly from Apple without all the adware of Droid. This happened early when AT&T wanted to get into the market badly.
- Enables software fixes to be implemented quickly when a problem is found.
- Droid requires Google to make an update. Then the Verizon/ AT&T have to update their adware.
- Droids are more flexible. You can modify them if you wish.

Hints

- I will cover a lot of steps in making an iOS device secure.
- At the end of each concept, I will tell you what I want you to remember.

iOS System Security

- iOS System Security
  - Secure Boot Chain
  - System software authorization
  - Secure Enclave
  - Touch ID

Secure Boot Chain

- Ensure system security is designed so that both hardware and software are secure across all core components of every IOS device.
- You cannot run any software on iOS without approval from Apple.
- Other than money, what technical reason is there that iOS will not run on a non Apple device?

Secure Boot Chain

- Each step of startup process has components, h/w and s/w that are crypto signed.
- This ensures integrity and authentication
- CIAN
- When iOS device is booted, the application runs code from read only memory called the Boot ROM.
- Contains the Apple root CA **public** key

Secure Boot Chain

- Verifies the Low-Level Bootloader (LLB) is signed by Apple before allowing it to load.
- LLB runs the next-stage boot loader, iBoot which in turn verifies and runs the iOS Kernel. This means the ROM is signed by Apple.
- This ensures from the time the device is booted, only Apple approved hardware and software are running.
- Else, we will not go any further.

Secure Boot Chain

- Latest CPU from Apple is A11. Designed by Apple.
  - iPad
  - iPhone 8 and 10
- Includes Secure Enclave Coprocessor (will discuss this coming up). This also uses the secure boot to ensure the hardware and software are verified and signed.
- If any of these processes fail, device will go in recovery mode. This is called fail, closed. This is a good thing.

System Software Authorization

- How do updates get to Apple devices?
- Apple provides regular updates to iOS for all supported devices.
- Only Apple signed code from the App Store will be pushed.
- Each update is uniquely customized to the software on each device.
- Since every Apple device contains only software approved by Apple, updates can be quick if a problem is found.
- Apple has a forced update. Only used twice.
- This is different on Android and since the phone has value added software from a carrier. (Except Google Pixel)

System Software Authorization

- During an iOS upgrade, iTunes connects to the Apple installation authorization server. This happens even when locked. It must be on WiFi.
- Sends a list of cryptographic keys for the software to be run on this device
- Also, sends a nonce and the device's Unique ID. (ECID)
- The UID is not stored at Apple. This is only on the device and is unique to each iPhone.
- Authorization server checks the registered device and what it is allowed to have. For example, an iPhone 4S lacks iPay, the fingerprint reader features on a iPhone 6. And the iPhone X has FaceID.

System Software Authorization

- Boot time chain of trust evaluation on the device verifies the signature came from Apple.
- Going to a previous level of software is not allowed. Why?
- A nonce is used to further assist in crypto and prevent a replay attack.

System Software Authorization

- A lot of slides were presented.
- Summary:
  - The h/w and s/w is signed
  - Crypto is used to ensure only Apple approved s/w and h/w is on this device.
  - Each device receives a customized update.

Secure Enclave

- The Secure Enclave is a physical coprocessor in the Apple CPU
- Stores the passcode and representation of fingerprint
  - In other words, it is the /etc/password and /etc/shadow
- This is for authentication, but not authorization
- Provides all crypto operations for Data Protection key management
- Maintains the integrity even if the kernel has been compromised.
- It utilizes its own secure boot.

Secure Enclave

- Uses encrypted memory
- A UID is the equivalent to a serial number burned into each processor that identifies each processor's Secure Enclave uniquely.
- Apple claims the UID is not directly accessible by other parts of the device.
- This information is stored in regular memory, but encrypted using the key, UID.
- When a UID or any other information is stored on a chip, it is very difficult to directly access.

Secure Enclave

- Responsible for determining the validity of a fingerprint, or a face.
- Processor sends the “measurement” of the fingerprint or face to the Secure Enclave, but cannot read it.
- The Secure Enclave responds with a yes or no answer. Is there a match?
- Even though the CPU and Secure Enclave are in the same device, they are physically separate.

Secure Enclave

- The measurement of the finger print is encrypted and authenticated with a session key in the Secure Enclave.
- Session key exchange uses AES key wrapping with both sides providing a random key.
- This is seriously complicated encryption by Apple.

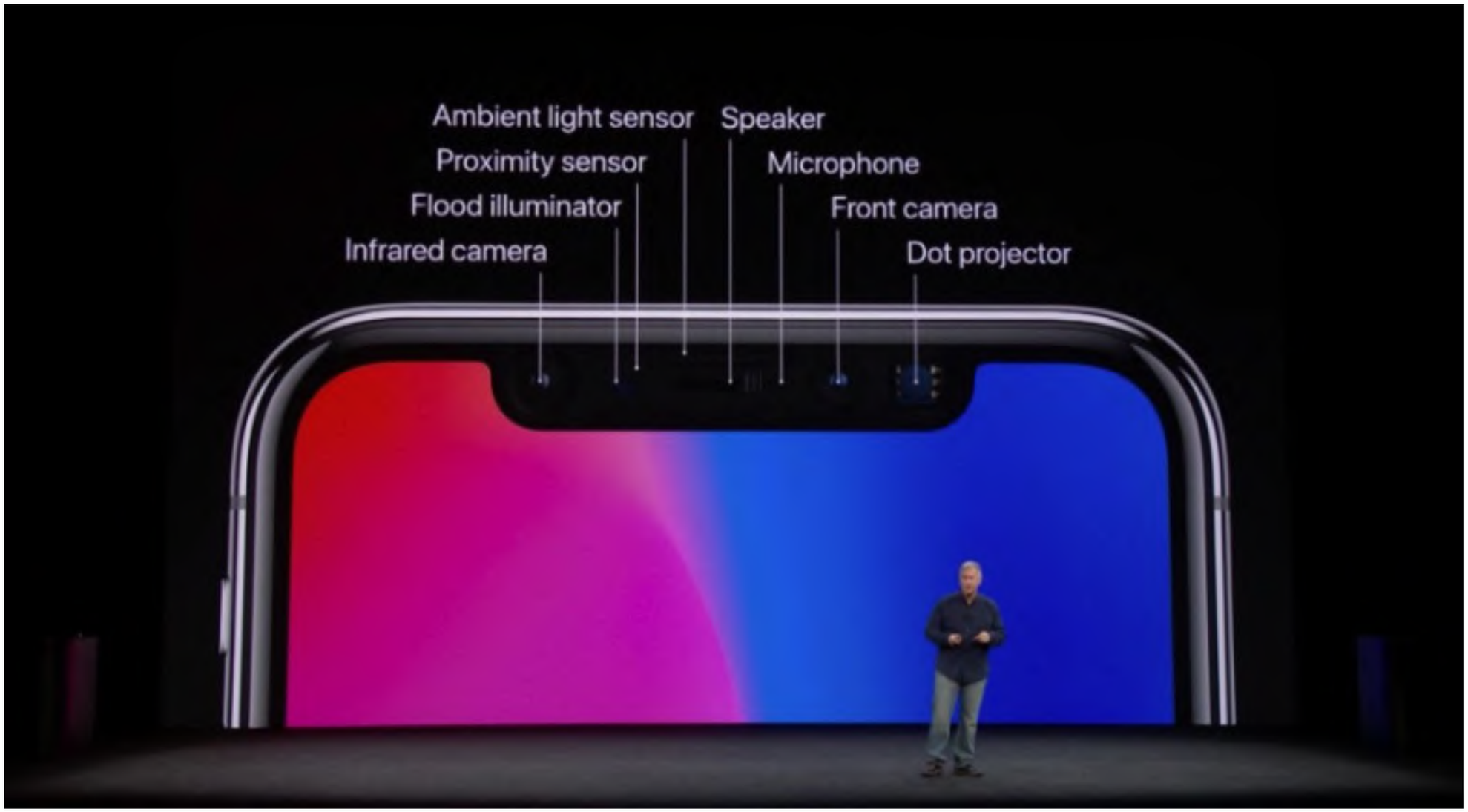
Secure Enclave
Just the facts

- The Secure Enclave holds the fingerprint and pass code.
- The Secure Enclave is separate from the CPU.
- The CPU verifies the authenticity of the user.

Finger Print Reader

Touch ID

iPhone 10 Sensors



Touch ID

- Fingerprint reader
- Goal is to replace passwords
- Fingerprints are unique
- Makes a longer more complex password
- Allows you to log in to some enabled applications

Touch ID

- Passcode can always be used instead of TouchID
- Required in the following cases:
  - Device has been restarted
  - Has not been unlocked for > 48 hours
  - Has received a remove lock command
  - Five unsuccessful attempts to match fingerprint
  - Enrolling new finger in TouchID

Touch ID
Just the facts

- Used most of the time instead of pass code.
- Pass code can be used at all times.
- Touch ID cannot be used at all times.

Encryption and Data Protection

- Coming up:
  - **Hardware Security Features**
  - File Data Protection
  - Passcodes
  - *Data Protections classes*
  - *Keychain Data Protection*

Hardware Security Features

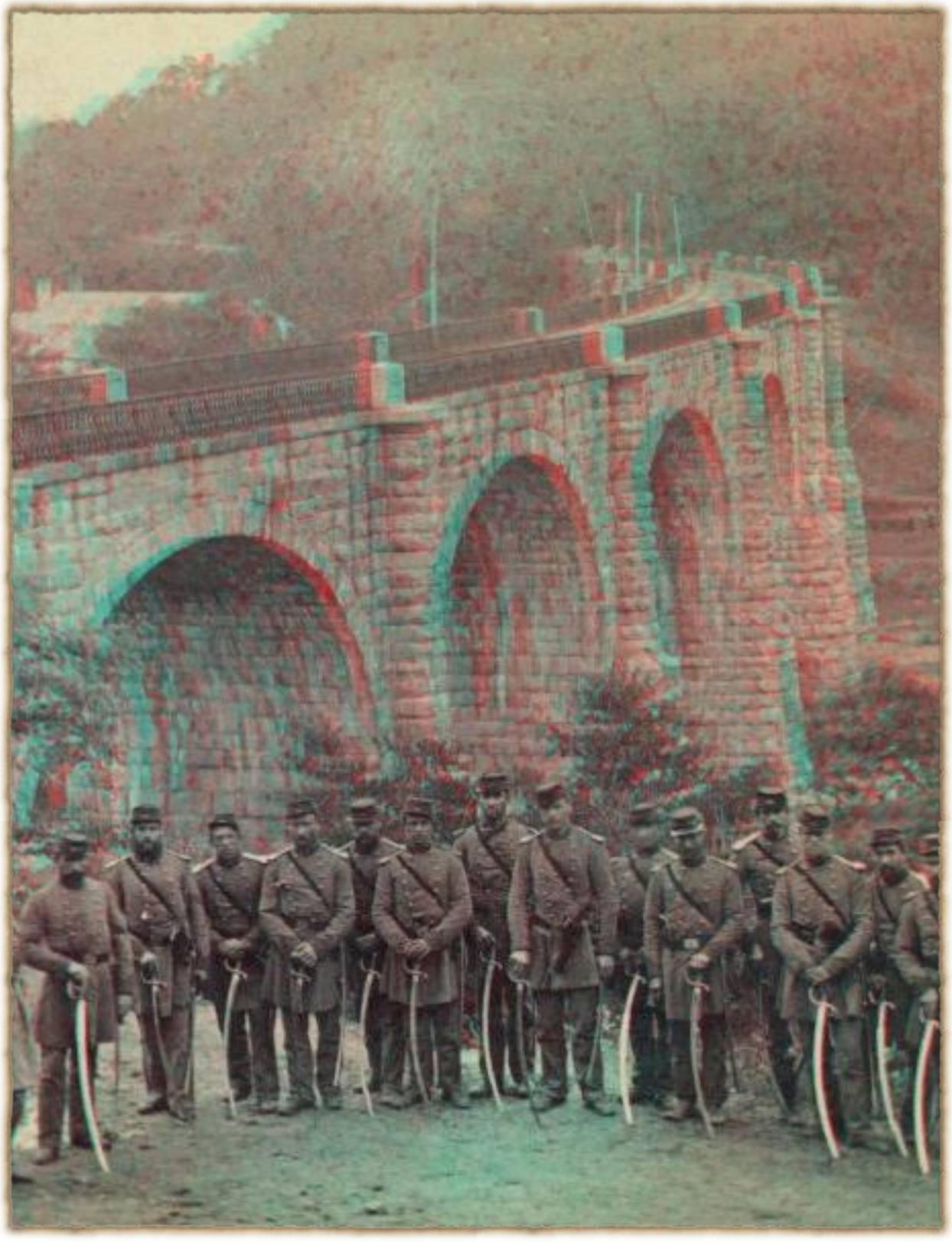
- A11 is an ARM processor. This is a RISC chip.
  - **A**corn **R**ISC **M**achine or **A**dvanced **R**ISC **M**achine
- Mobile devices run on a battery.
- Crypto operations are complex
- Each iOS devices has a dedicated AES crypto engine.
- This engine is built into the DMA path between flash and system memory.
- For performance and energy savings.

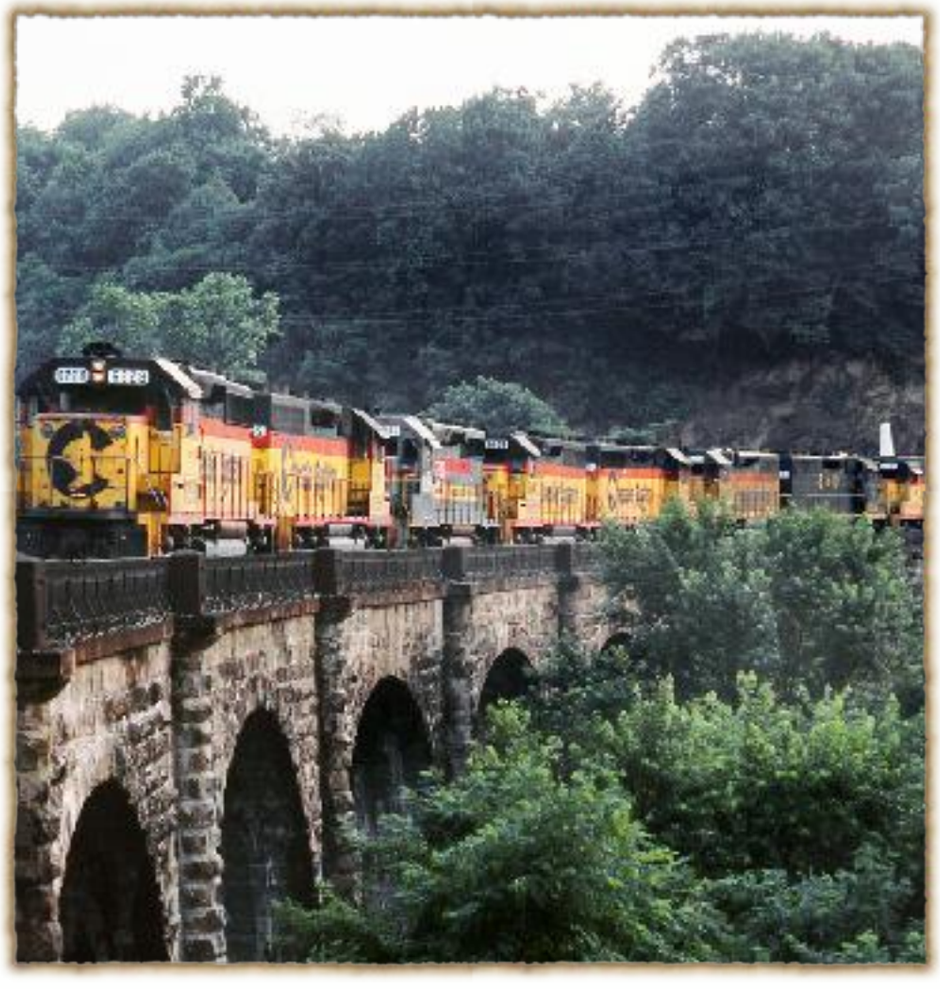
Hardware Security Features

- Secure Enclave has in hardware:
  - Device Unique ID (UID)
  - Device group id (GID) Identifies hardware
- UID is unique for each device. Apple claims it cannot read it.
- This ensures that the software installed on one computer cannot be run on another.
- Discourages forensics
- Software is tied to a single device.
  - Cannot install a license and run it on another computer

Hardware Security Features

- Wear leveling means multiple copies of keys might exist.
  - Spinning drives have bad sections.
- Forensics tools might be able to find.
- Effaceable Storage resolves this with secure erase.



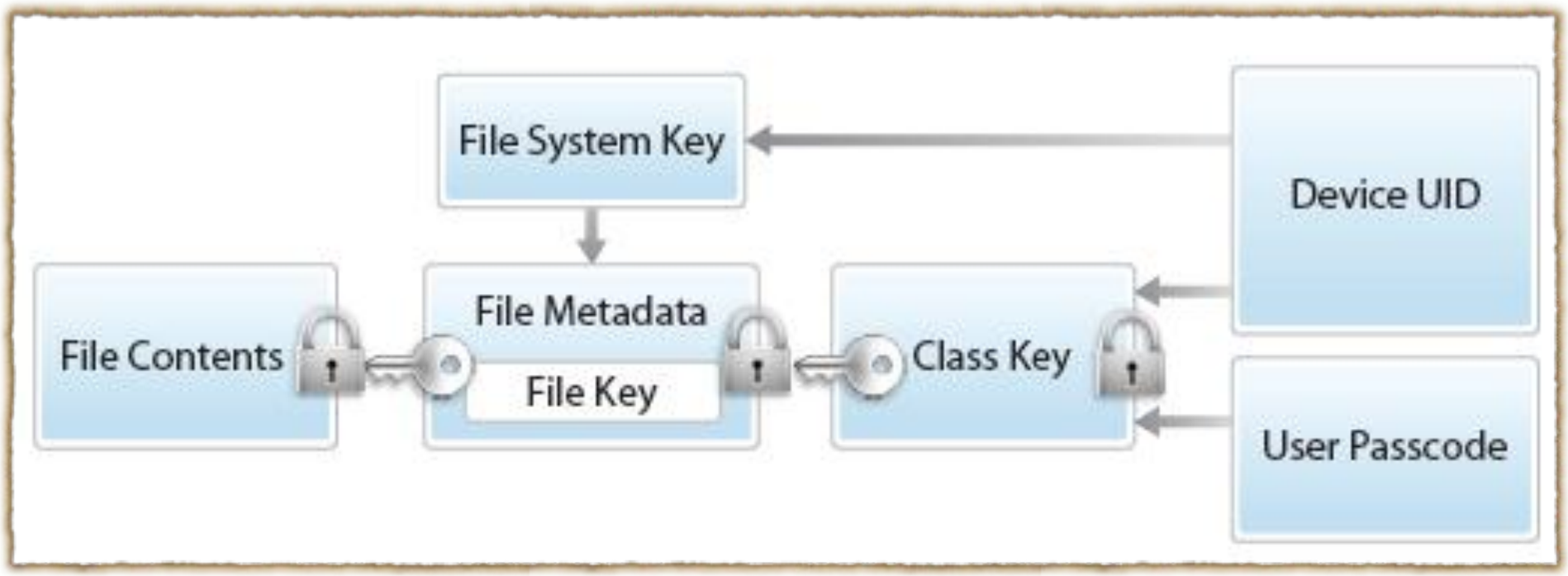


Encryption and Data Protection

- Coming up:
  - Hardware Security Features
  - **File Data Protection**
  - Passcodes
  - *Data Protections classes*
  - *Keychain Data Protection*

File Data Protection

- When a file is created, Data Protection creates a new 256 bit key
- Key given to AES encryption engine to encrypt the file.
- Also, the meta data is encrypted



Keys involved in opening a file

Erase the Device

- To zero out the device memory, what needs to be done?

Erase the Device

- To initialize the device, what needs to be done?
  - Clear Effaceable Storage
  - Actually, any of the above key should do it.
  - Even if you have forensics tools, you still have to decrypt the data once you got it off the device.

Encryption and Data Protection

- Coming up:
  - Hardware Security Features
  - File Data Protection
  - **Passcodes**
  - *Data Protections classes*
  - *Keychain Data Protection*

Passcodes

- Setting up a passcode enables Data Protection.
- Provides entropy for certain encryption keys
- Touch ID allows you to have a longer passcode.
- The longer the passcode, the more secure the device.

New in iOS 11.4

- https://blog.malwarebytes.com/security-world/2018/03/graykey-iphone-unlocker-poses-serious-security-concerns/
- Lightning port will be disabled to data after 7 days of not accessing the device.
- Power still works.
- Either by passcode, fingerprint, or facial recognition.

Summary

- Secure Boot Chain
- System software authorization
- Secure enclave structure
- Files are encrypted to include meta data

Last slide

- See subject.