iOS Security

András Gazdag

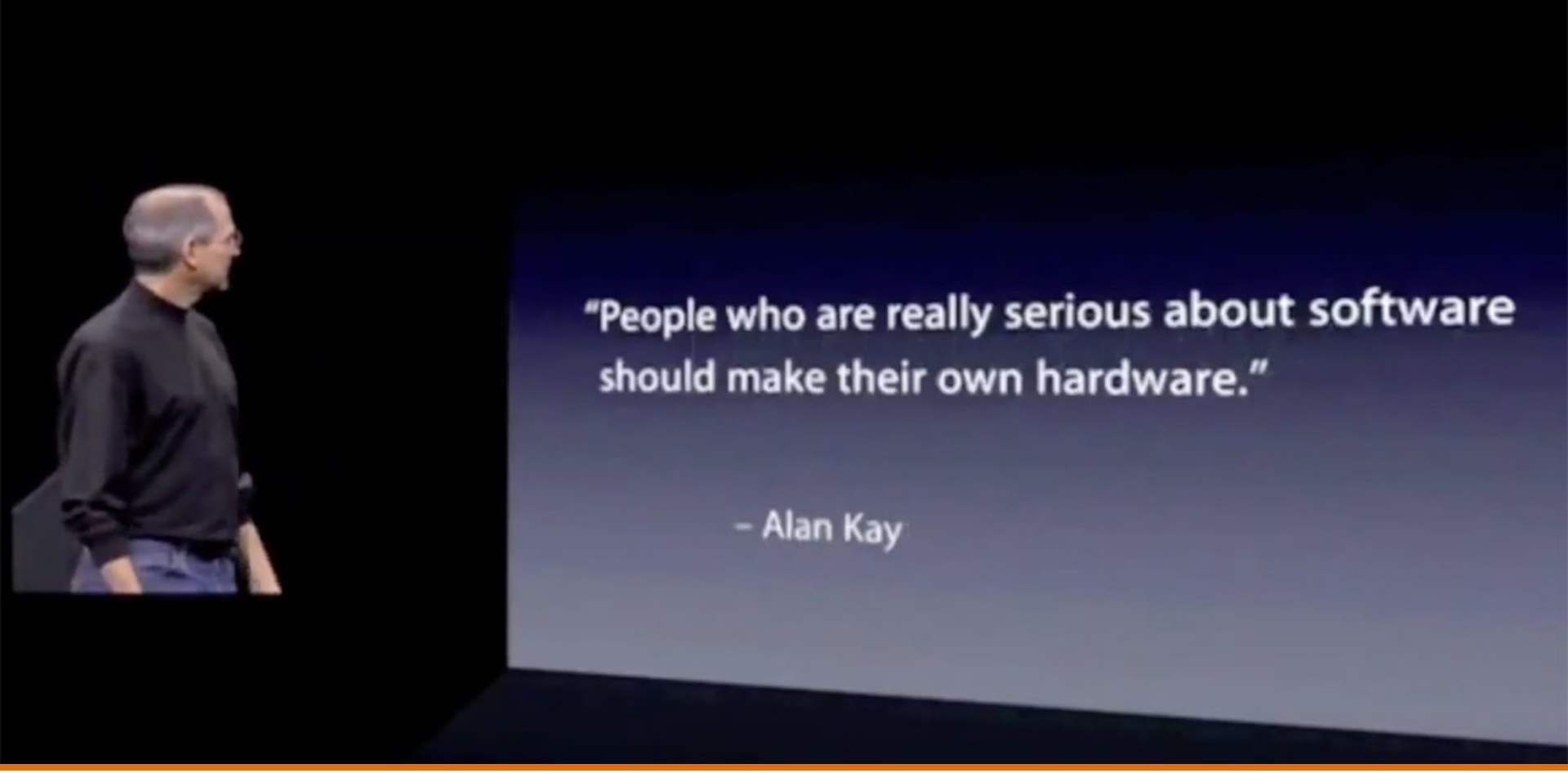
CrySyS Lab, BME HIT

andras.gazdag@crysys.hu


9:41
Clock
Camera
375/500CAL
19/30MIN
4/12HRS
TV
Stocks
Activity
Mail
Files
FRIENDS
Photos
App Store
Weather
Health
Home
Chromatica
Lady Gaga
News
Photos
Music


9:41
Monday, June 22
FaceTime
MON
22
Calendar
Clock
Home
Photos
Camera
MONDAY
22
Kickoff meeting wi...
10:30–1:00 PM
Bicycle tune-up
1:30–2:15 PM
San Francisco
61°
Mostly Sunny
H:70° L:53°
Reminders
Notes
Voice Memos
Contacts
Maps
Find My
Top Stories
Climate concerns as Siberia experiences record-breaking heat
Traditional Sports Look to Gamers to Reshape Viewers' Experience
App Store
Books
Podcasts
TV
News
Stocks
Chromatica
Lady Gaga
Measure
Settings

iOS + iPadOS

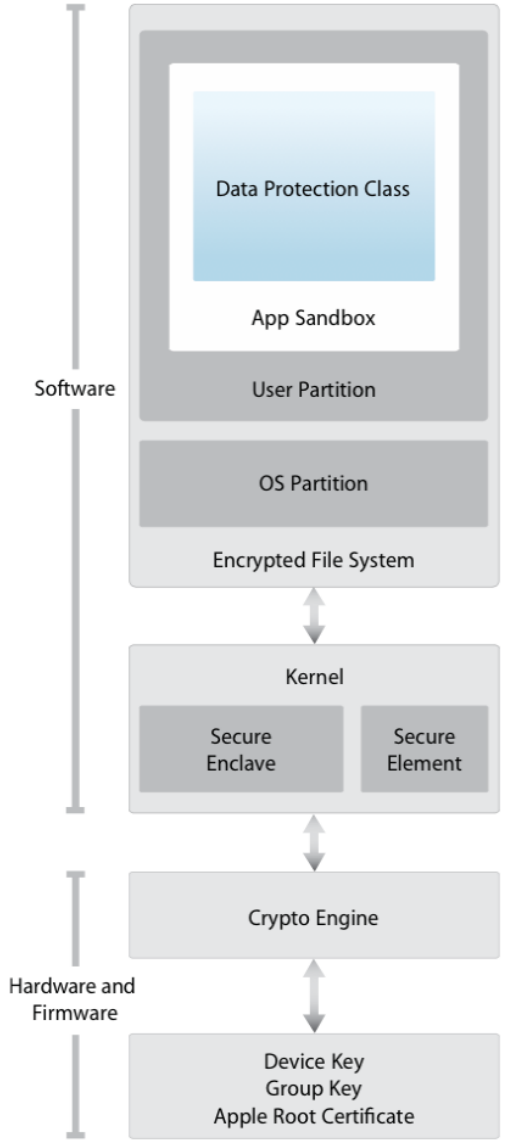


"People who are really serious
about software should make their own hardware."

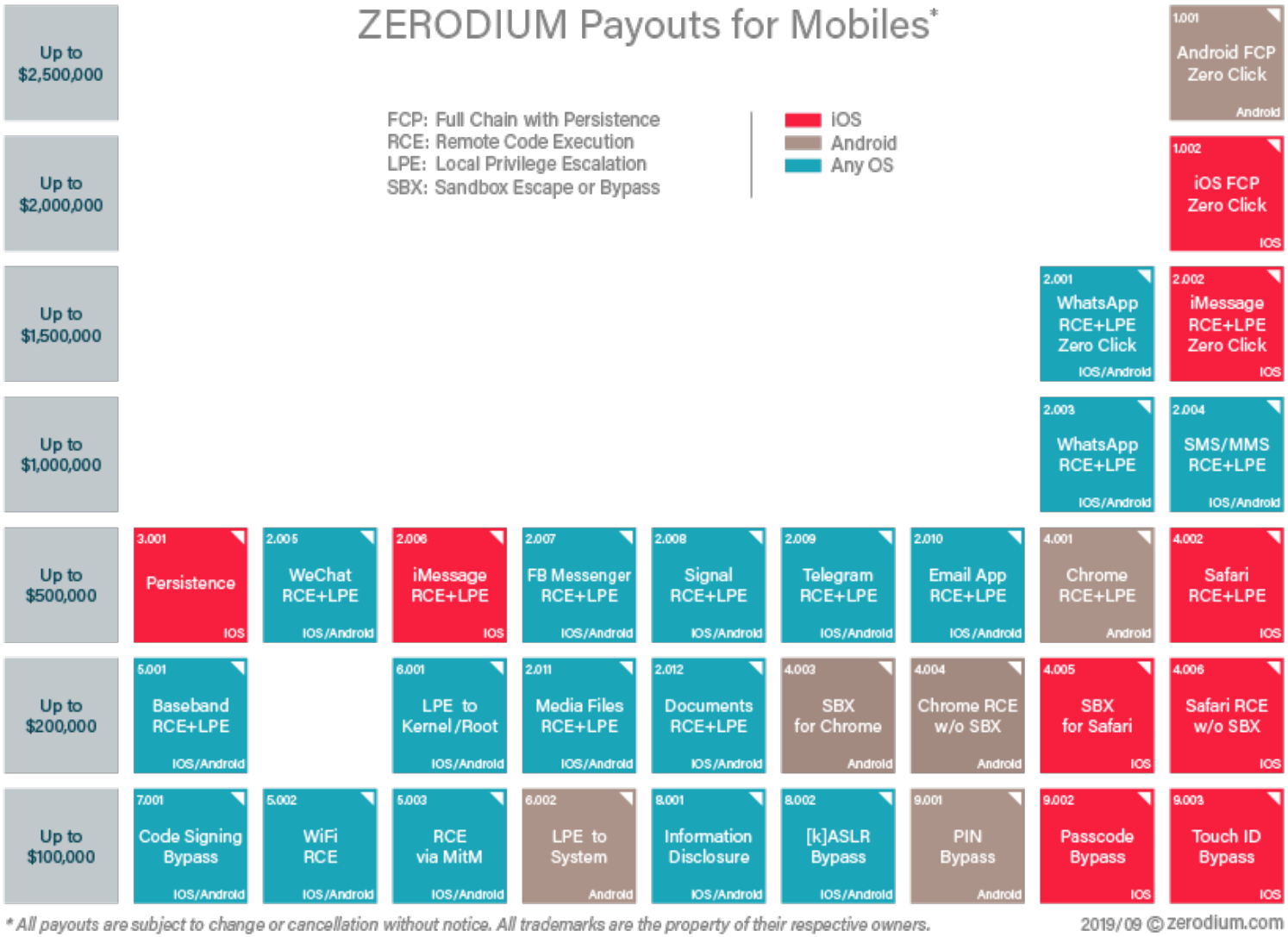
“People who are really serious
about software should make their own hardware.”

Contents - iOS

- System Security
- Encryption and Data Protection
- App Security
- Services Security



How much for a 0-day?



SYSTEM SECURITY

System Security - Secure boot

- Goals:
  - Ensure integrity of the software components
    - » Lowest levels of software are not tampered with
  - Proceed only after verifying the chain of trust
    - » This includes the bootloaders, kernel, kernel extensions, and baseband firmware
    - » iOS runs only on validated Apple devices

- Secure Enclave coprocessor: separate secure boot
  - The Boot Progress Register (BPR) is used by the Secure Enclave to limit access to user data in different modes and is updated before entering the next boot step (processor dependent)

- On devices with cellular access, the baseband subsystem also utilizes its own similar process of secure booting

System Security - Secure boot

- Secure boot chain:
  - Boot Rom
    - » read-only
    - » hardware root of trust
    - » Apple Root CA key
  - iBoot
  - iOS Kernel

- If load fails
  - During Boot rom or iBoot → DFU mode
  - During the verification of the next level → Recovery mode

System Security - Update

- System Software Authorization: downgrade prevention

- During an iOS upgrade (in the case of OTA software updates), the device connects to the Apple installation authorization server and sends it
  - a list of cryptographic measurements for each part of the installation bundle to be installed (for example, iBoot, the kernel, and OS image)
  - a random anti-replay value (nonce)
  - the device's unique **Exclusive Chip Identification (ECID)**

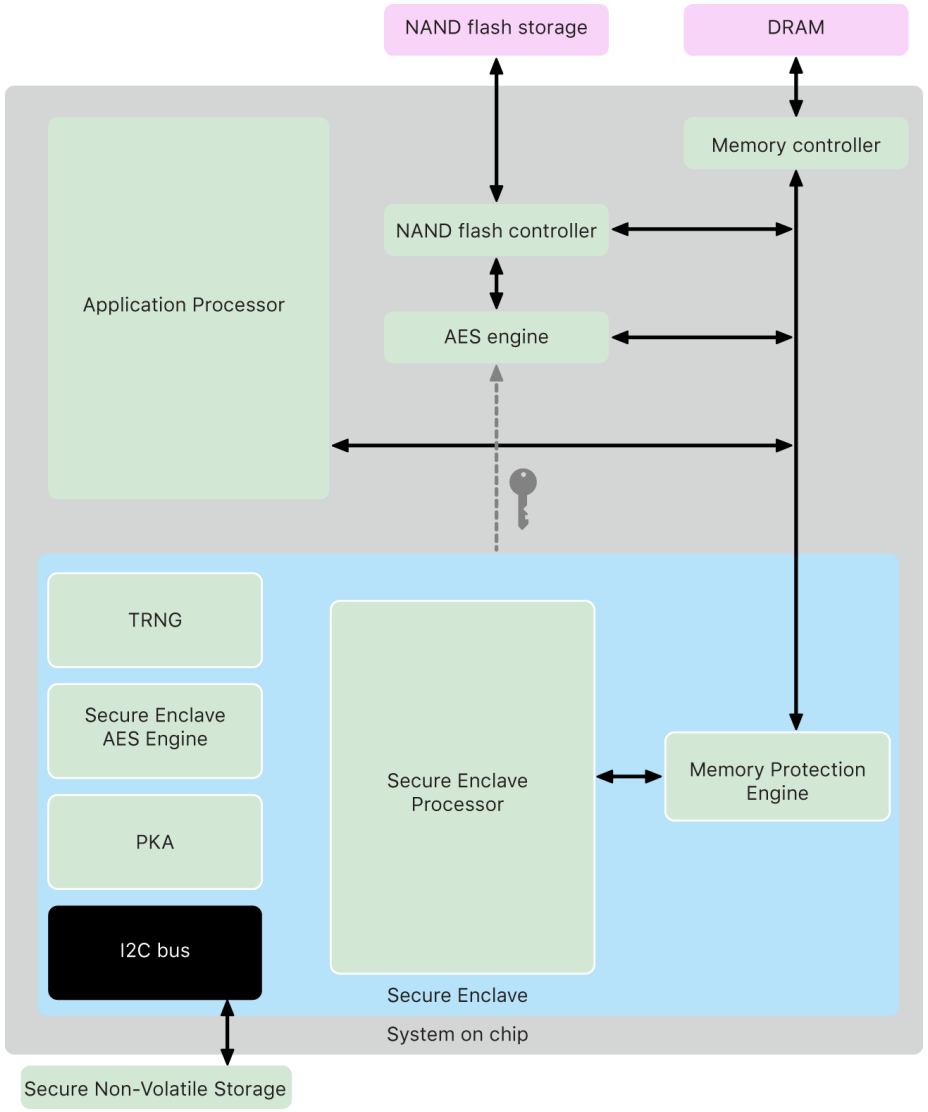
- The authorization server checks the presented list of measurements against versions for which installation is permitted

- Adding the ECID "personalizes" the authorization for the requesting device

System Security - Secure Enclave

- A7 or later: security subsystem
  - A coprocessor fabricated within the system on chip (SoC)
  - Secure Enclave is isolated from the main processor to provide an extra layer of security and is designed to keep sensitive user data secure even when the Application Processor kernel becomes compromised
- It uses encrypted memory
  - Ephemeral key is derived from the UID of the Secure Enclave
- Includes a hardware random number generator
- Provides all cryptographic operations for **Data Protection** key management and maintains the integrity of Data Protection even if the kernel has been compromised
- Responsible for processing fingerprint and face data from the Touch ID and Face ID sensors

System Security - Secure Enclave



System Security - Secure Enclave

- Runs the sepOS (Secure Enclave firmware) based on an Apple-customized version of the L4 microkernel
- Includes a dedicated Secure Enclave Boot ROM
  - Establishes the hardware root of trust for the Secure Enclave
- The Secure Enclave memory is also authenticated with the memory protection key
- Data saved to the file system by the Secure Enclave is encrypted with a key entangled with the UID and an anti-replay counter
  - The anti-replay counter is stored in a dedicated nonvolatile memory integrated circuit (IC).

- Mobile feature that came to the Macs → T2 chip

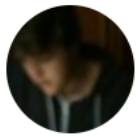
System Security – Low Level protections

- **Kernel Integrity Protection**
  - After the iOS kernel completes initialization, KIP is enabled to prevent modifications of kernel and driver code
  - After boot completes, the memory controller denies writes to the protected physical memory region
  - MMU is configured to
    - » prevent mapping privileged code from physical memory outside the protected memory region
    - » prevent writeable mappings of physical memory within the kernel memory region
- **System Coprocessor Integrity Protection**
  - System coprocessors are dedicated to a specific purpose, and the iOS kernel delegates many tasks to them
  - SCIP uses a mechanism like Kernel Integrity Protection to prevent modification of coprocessor firmware

System Security – Low Level protections

- **Pointer Authentication Codes**
  - Pointer authentication codes (PACs) are used to protect against exploitation of memory corruption bugs.
  - System software and built-in apps use PAC to prevent modification of function pointers and return addresses (code pointers)
  - Doing so increases the difficulty of many attacks
    - » E.g. Return Oriented Programming (ROP)
  - PAC is supported on A12 and S4 SoCs.

System Security – Low Level protections



qwertyoruiop
@qwertyoruiopz

Following

T8020 has pointer authentication ayyyyyyyyyyyyyyyyyy iOS exploitation is great again

9:32 PM - 12 Sep 2018

shipped this already.

10:24 PM - 12 Sep 2018

32 Retweets **185** Likes

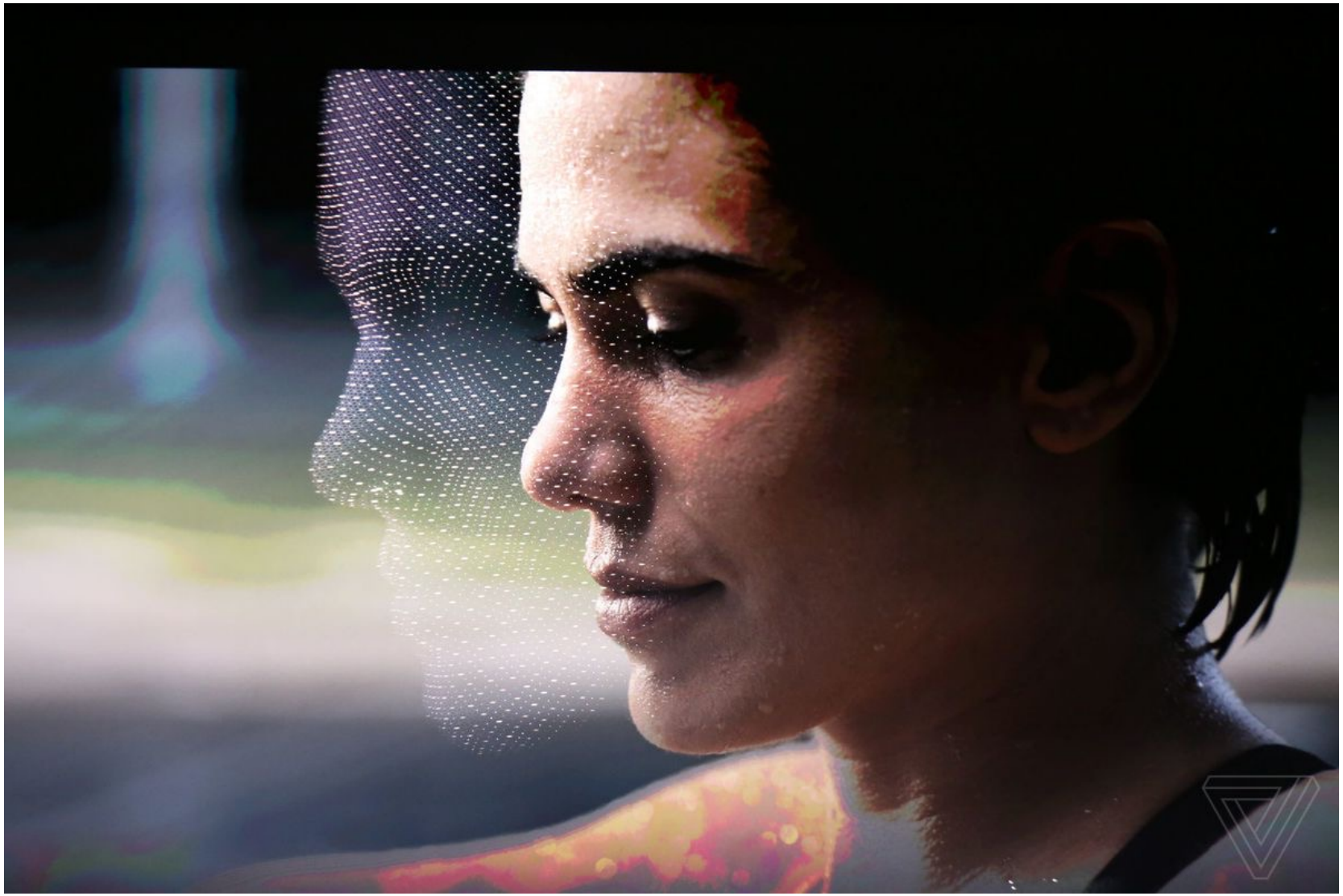
10 32 185

System Security

- Touch ID
  - Allows the use of stronger passwords
  - Chance of random match: 1:50.000 (after 5 mismatches it is disabled)
  - System provided APIs for third party apps

- Face ID
  - Allows the use of stronger passwords
  - Chance of random match: 1:1.000.000 (after 5 mismatches it is disabled)
    - » The probability of a false match is different for twins and siblings that look like you as well as among children under the age of 13, because their distinct facial features may not have fully developed
    - » “If you're concerned about this, we recommend using a passcode to authenticate”
  - System provided APIs for third party apps

Face ID



Face ID

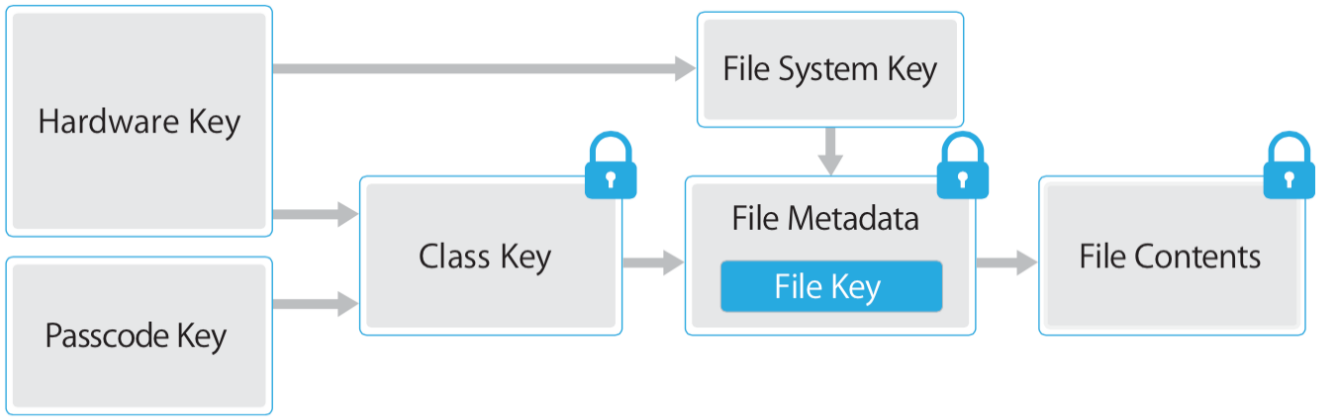
- Face ID confirms attention and intent to unlock by detecting that your eyes are open and directed at your device
- TrueDepth camera projects and reads over 30,000 infrared dots to form a depth map of the face, along with a 2D infrared image
- The sequence of 2D images and depth maps, which are digitally signed and sent to the Secure Enclave
- The TrueDepth camera randomizes the sequence of 2D images and depth map captures, and projects a device-specific random pattern
  - To counter both digital and physical spoofs
- A17 Bionic processor's neural engine (within the Secure Enclave)
  - transforms this data into a mathematical representation
  - compares that representation to the enrolled facial data

ENCRYPTION AND DATA PROTECTION

Encryption and Data Protection

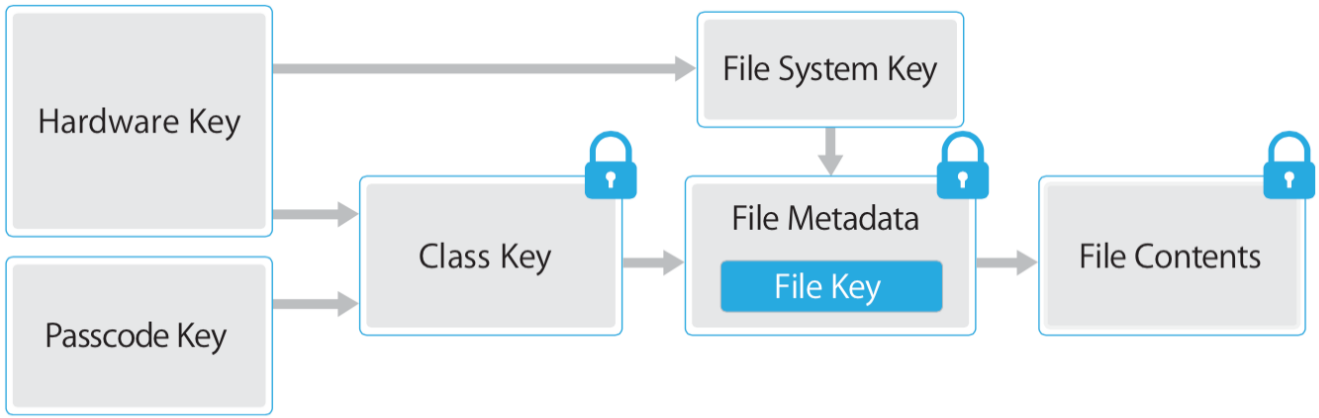
- Dedicated AES 256 engine in the DMA path
- Key: UID of the device fused during fabrication, not available through any API or JTAG
- Data is cryptographically tied to the device: if the memory chip is switched, decryption will fail
- System random number generator
  - Timing during boot
  - Interrupt timings after boot
- Secure Enclave
  - True hardware random: multiple ring oscillators
- All cryptographic modules in iOS: FIPS 140-2 Level 1
- Keys stored in Effaceable Storage
  - Solves problems with flash storage – keys can be deleted

Encryption and Data Protection



- File Data Protection
  - Data Protection is implemented by constructing and managing a hierarchy of keys, and builds on the hardware encryption technologies built into each iOS device
  - Per-file keys: 256 bit AES keys (AES128 in XTS mode)
  - File system key: generated at iOS install, constant for all files
  - With the advent of the Apple File System (APFS), the file system is now able to further sub-divide the keys into a per-extent basis (portions of a file can have different keys)

Encryption and Data Protection



- Data Protection classes
  - Complete Protection
  - Protected Unless Open
  - Protected Until First User Authentication
  - No Protection

Passcode

- By setting up a device passcode, the user automatically enables Data Protection
- iOS supports six-digit, four-digit, and arbitrary-length alphanumeric passcodes
- In addition to unlocking the device, a passcode provides entropy for certain encryption keys
- This means an attacker in possession of a device can’t get access to data in specific protection classes without the passcode.

Passcode

- The stored passcode is entangled with the device's UID, so brute-force attempts must be performed on the device under attack
- A large iteration count is used to make each attempt slower:
  - The iteration count is calibrated so that one attempt takes approximately 80 milliseconds
  - This means it would take more than five and a half years to try all combinations of a six-character alphanumeric passcode with lowercase letters and numbers.
- On devices with Secure Enclave, the delays are enforced by the Secure Enclave coprocessor
  - If the device is restarted during a timed delay, the delay is still enforced, with the timer starting over for the current period
- To improve security while maintaining usability, iOS 11.4.1 or later requires Touch ID, Face ID, or passcode entry to activate the USB interface if USB hasn't been used recently

Express Cards with power reserve

- If iOS isn't running because iPhone needs to be charged, there may still be enough power in the battery to support Express Card transactions.

- Supported iPhone devices automatically support this feature with:
  - A transit card designated as the Express Transit card
  - Student ID cards with Express Mode turned on

- This feature isn't available when a standard user initiated shutdown is performed

Network Security

- Support for TLS 1.0 – TLS 1.3
  - In iOS 11 or later and macOS High Sierra or later, SHA-1 certificates are no longer allowed for TLS connections unless trusted by the user
- Per App VPN, Always on VPN
- Randomized MAC address when searching for Wi-Fi
- System support for SSO to enterprise networks
  - Works with Kerberos-based networks

- AirDrop
  - Bluetooth Low Energy (BLE)
  - Apple-created peer-to-peer Wi-Fi
  - iCloud identity certificates
  - TLS

APP SECURITY

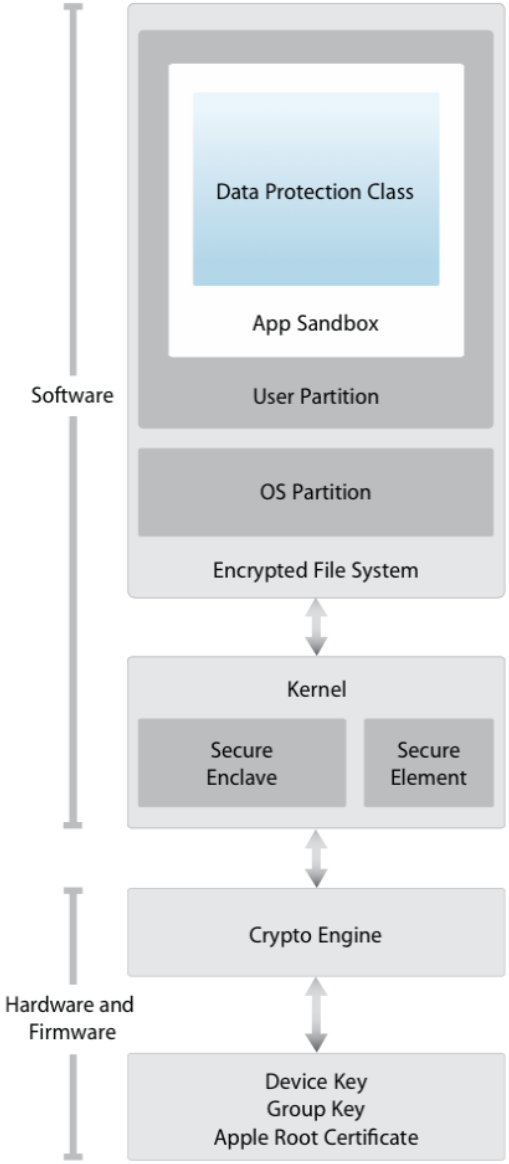
App Security

- Signed, Verified and Sandboxed applications

- Code signing
  - All executable code must be signed with Apple-issued certificate
  - Extends the concept of chain of trust
  - Prevents the load of external code or self-modifying code
  - Apps can be traced back to developers
  - In-house app development with Provisioning Profiles (enterprise apps)
  - Code signature checks at runtime as well

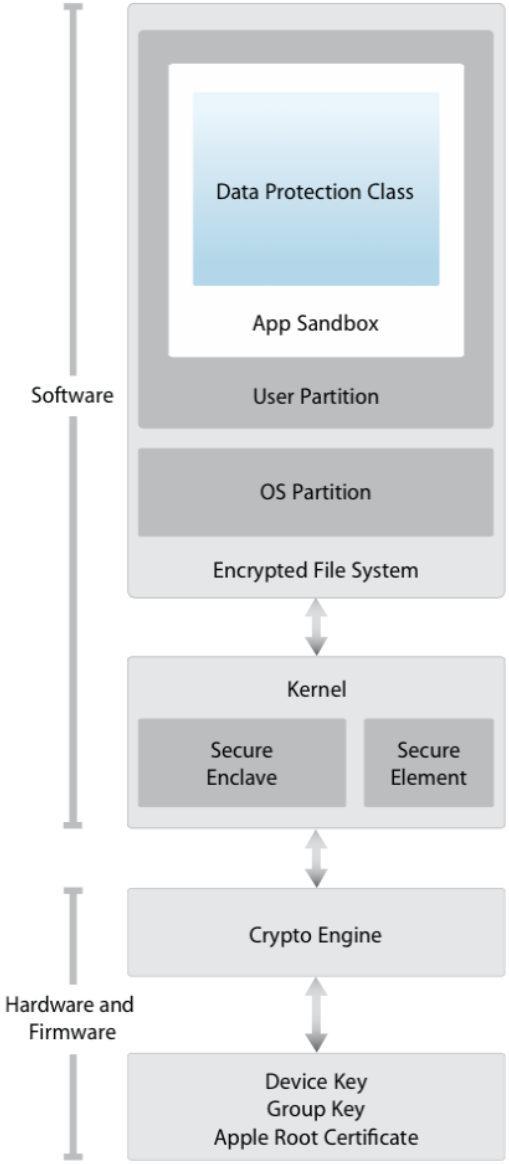
App Security

- Runtime process security
  - Third party apps are sandboxed
  - Unique random home directory for every app (assigned at install)
  - Access to any other information is only possible through iOS services
  - OS partition is read-only
  - Majority of iOS, as well as third party apps run as non-privileged user
  - Unnecessary tools (such as remote login services) are removed
  - Built-in apps and third party apps (by default) are compiled with ASLR turned on (exploitation of memory corruption is harder)



App Security

- Runtime process security
  - Apps on writable AND executable memory pages are controlled tighter: Apple-only dynamic code-signing entitlement
    - » Only for Safari JIT JavaScript complier
  - ARM's Execute Never (XN) protection on pages
  - App Extensions
    - » Run in own address space
    - » IPC only through system framework
    - » Separate container than containing app
    - » Same access and privacy controls
  - Custom keyboards
    - » Enabled by the user for the entire system
    - » Any text field, except: Passcode, secure text
    - » Restricted sandbox: no network access
    - » Default sandbox can be requested



App Security

- App Groups
  - Apps from the same developer can share content if they are part of an App Group
    - » Shared on-disk container
    - » Shared preferences
    - » Shared keychain items

- Accessories
  - MFi program
  - Apple-provided certificate for device authentication
  - Apple-provided custom integrated circuit (transparent to the accessory)
  - All communication are encrypted

SERVICE SECURITY

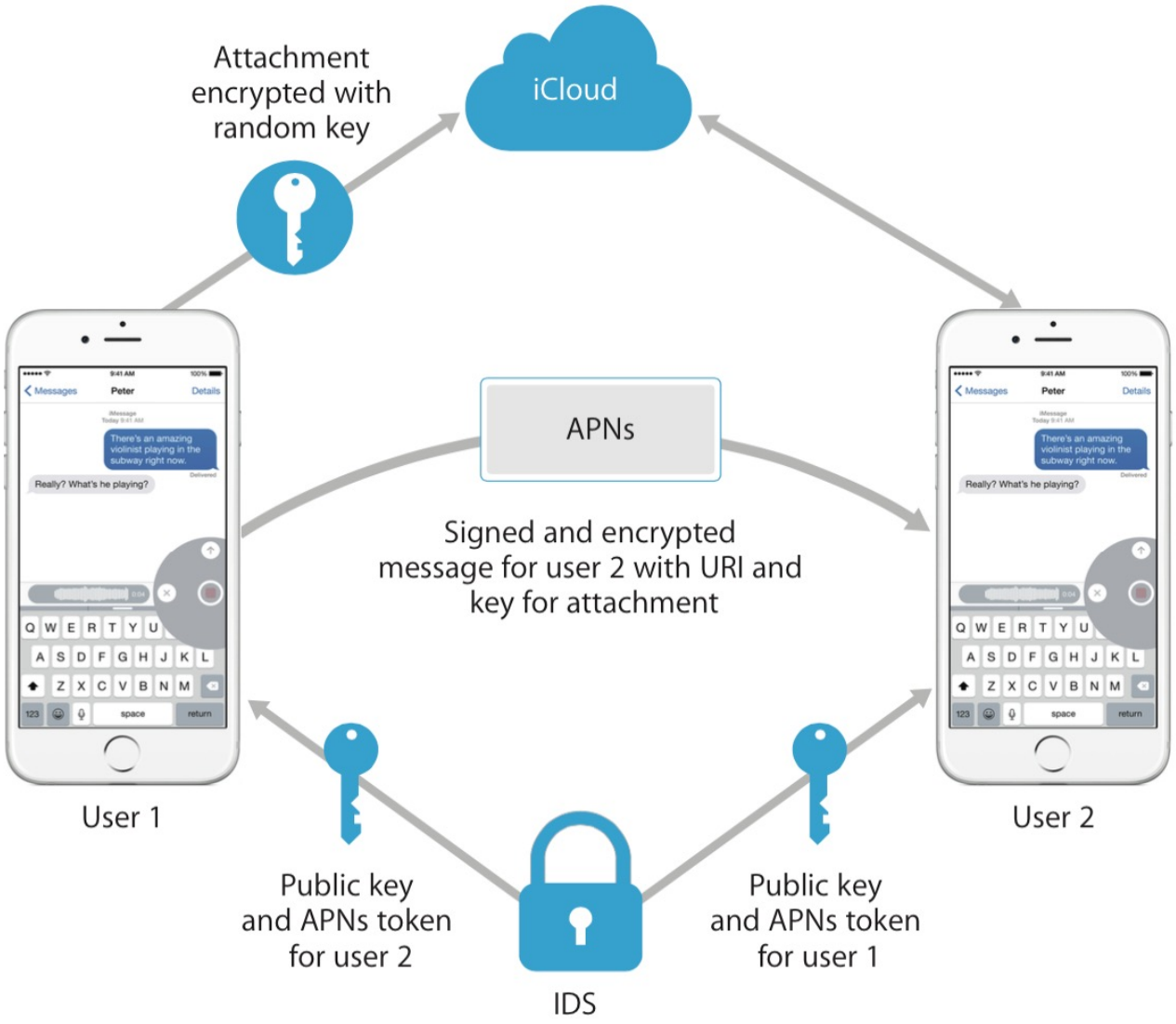
Apple Pay

- Apple securely sends the card information, along with other information about user's account and device, to the respective bank
- Full card numbers are not stored on the device or on Apple servers
- Unique Device Account Number is created, encrypted, and then stored in the Secure Element
- Apple receives anonymous transaction information
- Lost Mode automatically deletes all sensitive information

Internet Services

- Apple ID: iCloud, iMessage, FaceTime, iTunes Store, iBooks Store, App Store
- Two-step verification
- iMessage
  - End-to-end encryption
  - Apple doesn't log messages or attachments
  - RSA 1280 bit key for encryption and ECDSA 256 bit key for signing
  - Public keys are stored at Apple directory service (IDS)
  - Signalling through Apple Push Notification (APN) service
  - Each message is encrypted individually for each of the recipient's devices
  - Communication with APNs is encrypted with TLS
  - Attachments are encrypted with random keys, and uploaded to iCloud
  - Messages are deleted from APNs when delivered
  - Messages for offline devices are queued for up to 7 days

Internet Services



Internet Services

- FaceTime
  - Initial connection: Apple Push Notification
  - Peer-to-peer connection with end-to-end encryption
  - Session management: SIP, streaming: SRTP
- iCloud
  - Handles every file the same way: collection of bytes
  - File chunk-based encryption
  - Encrypted chunks, without user-identifying information, are stored at third party storage services: e.g., Amazon S3, Windows Azure
  - Keychain is protected by a UID-tangled key
    - » It can only be restored to the same device
    - » No one can access its content
    - » Third party keychain items are not synchronized by default
    - » Keychain recovery is important if Safari password suggestions are turned on

Internet Services

- Siri
  - Uses a random identifier for voice recognition (it can be regenerated on demand)
  - Sends additional data: music library data, reminders, relationships, user first and last name, rough location, etc.
  - Additional information is only sent if needed: e.g. fine location info
  - After 10 minutes all session information is discarded
  - Voice recordings are saved for 6 month
- iPhone Cellular Call Relay
  - Signaling through APNs
  - Secure peer-to-peer connection for call relay
- Handoff
  - APN based signaling for Bluetooth connection establishment
  - Secure app validation before Handoff activity is forwarded

Device Controls

- Passcode protection
  - Protected against brute-force attacks
- Configuration enforcement
  - Force policies on users, predefined configurations
  - Configuration profiles can be locked to a device
  - Apple Configurator app for OS X makes it easy to deploy iOS devices
- Remote wipe
  - Instant remote wipe
    - » Discards the block storage encryption key from Effaceable Storage, rendering all data unreadable
  - Users can also wipe devices in their possession using the Settings app
- Find My iPhone and Activation Lock
  - The device can't be reactivated without entering the owner's Apple ID

PRIVACY

Privacy Controls

- Location Services
  - GPS, Bluetooth, crowd-sourced Wi-Fi hotspots, cell tower locations
  - Can be enabled globally or only for specific applications
  - Can be disabled for system services
  - Options for apps (allowed): never, when in use, always
- Access to personal data
  - App needs to have permission for every resource
  - If user is signed-in to iCloud: iCloud Drive access is granted by default
  - Developer does not need to explicitly declare a permission request
  - Permission request happens at runtime, when feature is used
  - Contacts, Calendars, Reminders, Photos, Motion information, Social account information, Microphone, Camera, HomeKit, HealthKit, Bluetooth sharing

Privacy Controls

References

Apple Platform Security

https://support.apple.com/en-gb/guide/security/welcome/web

QUESTIONS

Questions

- How does secure boot work on iOS?
- What is the Secure Enclave?
- What biometric authentications are available on iOS devices?
- Describe file system encryption on iOS.
- What can code signing guarantee on iOS?
- What runtime process security features are available on iOS?