iOS Security Decoded

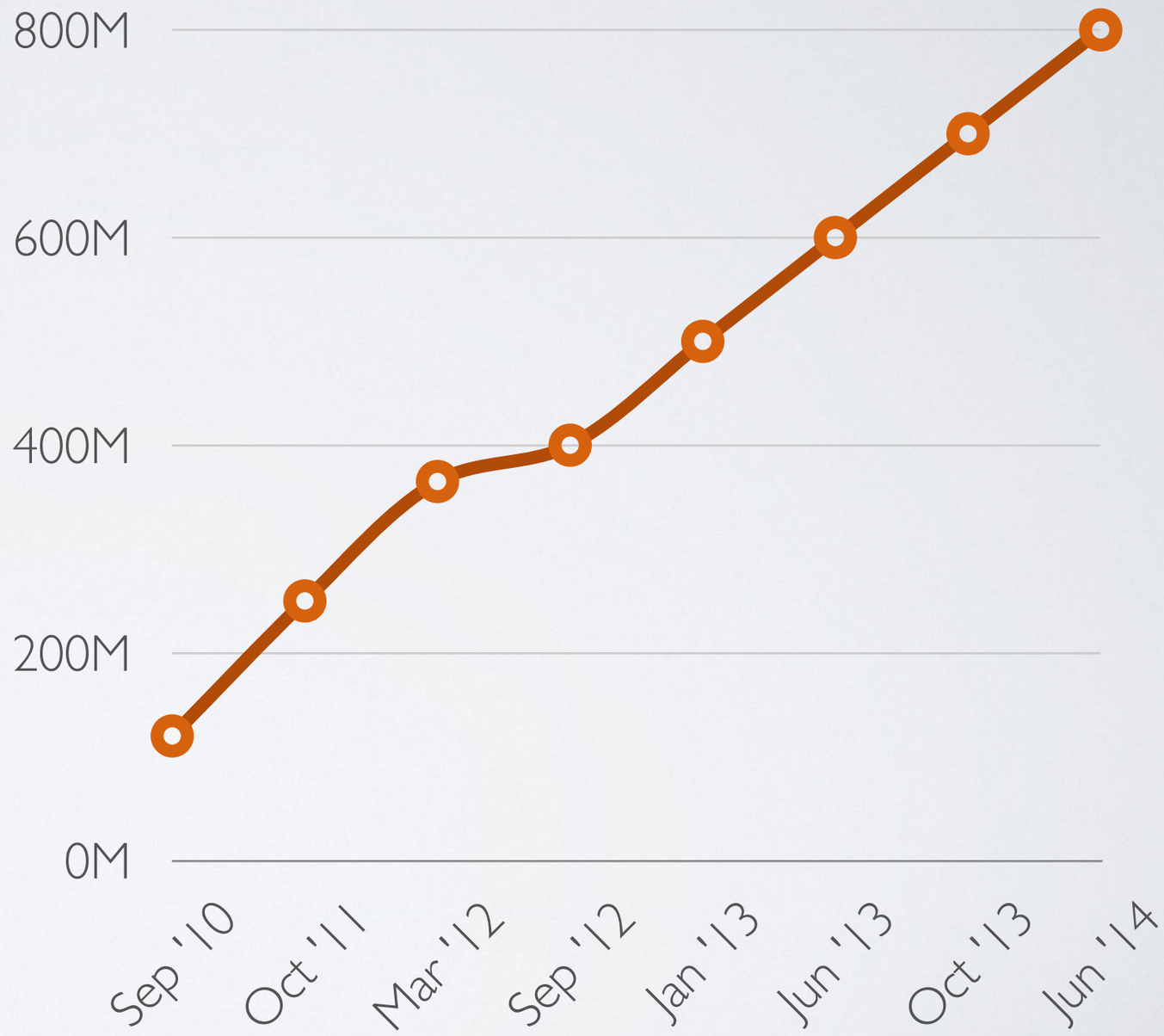
Dave Test
Classroom and Lab Computing
Penn State ITS

2014 MACADMINS CONFERENCE AT PENN STATE

Feedback - http://j.mp/psumac33

Why care about iOS Security?

- 800 million iOS devices activated
- 130 million in last year
- 98% of Fortune 500



Definitions

Public and Private Keys

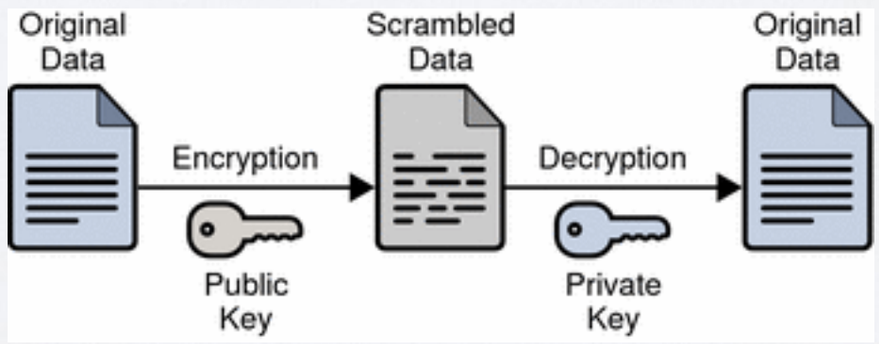
Certificate

AES-256

Definitions

Public and Private Keys

- Two mathematically linked keys
- One is public and can be used to encrypt data
- One is private and can be used by the recipient to decrypt data.



Definitions

AES-256 and SHA-1

- Two specs for encrypting data
- AES-256 generates 256 bit keys
- SHA-1 generates 160 bit keys

Definitions

Certificates and Certificate Authorities

- A certificate is an electronic document used to prove the ownership of a public key.
- A certificate authority (CA) is a trusted group who digitally signs a certificate to signify its veracity.

iOS Security Decoded

Secure Boot Chain

Hardware Security

Software Security

Network Security

Best Practices

Secure Boot Chain

Starts at power on. Each step verifies the next. If any step fails, device enters Device Firmware Upgrade (DFU) mode.

Secure Boot Chain

Step 1 - Boot ROM

- Implicitly trusted
- Cannot be changed
- Verifies signature of next Low-Level Bootloader via embedded Apple Root CA public key
- Runs Low-Level Bootloader

Secure Boot Chain

Step 2 - Low-Level Bootloader (LLB)

- Lowest level of code on device that can be updated
- Verifies signatures of firmware and iBoot
- Runs iBoot

Secure Boot Chain

Step 3 - iBoot

- Verifies signature of iOS Kernel (XNU)
- Starts kernel
- If kernel verification fails, device goes into Recovery Mode (Connect to iTunes Mode)

Secure Boot Chain

Baseband and Secure Enclave have their own secure boot chain processes which run before the kernel is loaded.

Hardware Security

Hardware Security

Crypto Engine

- Co-processor dedicated to AES-256 functions
- Built into DMA path between flash storage and RAM
- Stores UID and GID

Hardware Security

Unique ID (UID)

Exclusive Chip ID (ECID)

Group ID (GID)

AES-256 keys fused into the processor during manufacturing.

Hardware Security

Unique ID (UID)

- Unique to every device processor
- Not recorded by Apple or manufacturer
- Cannot be read by firmware or software

Hardware Security

Exclusive Chip ID (ECID)

- Unique to every device
- Not secret
- Used in device activation process and during software update

Hardware Security

Group ID (GID)

- Shared among devices with a common Apple processor, e.g. A5X or A7

- Used along with ECID to determine proper software update packages

Hardware Security

Secure Enclave

- Co-processor new to A7
- Manages all crypto operations
- Stores keys in encrypted memory
- Not accessible to software, only to processor

Hardware Security

Touch ID

- 550 ppi raster scan of sub-dermal fingerprint

- Forwards data to Secure Enclave, which vectorizes and stores data

- Data never leaves Secure Enclave - processor only receives a “yes” or “no” if fingerprint matches.

Software Security

Software Security

Code Signing

- All executable code must be signed using an Apple-issued certificate
- Apple code is signed internally by Apple
- App Store Code is signed by Apple Developer and Apple
- In-house code is signed with Enterprise Developer Program cert

Software Security

Sandboxing

- Apps cannot access system files or files from other apps
- All access to info from outside sandbox is through approved APIs
- Most built-in & all third-party apps run as non-privileged user
- Apps can share data via custom URL schemes and shared keychain groups

Software Security

ASLR

- Address Space Layout Randomization protects against memory exploitations

- System library locations also randomized at startup

Software Security

Data Protection (1)

- Enabled via use of a passcode
- Every file on data partition is encrypted
- Encryption keys are stored in Effaceable Storage
- When device is wiped, effaceable Storage is securely erased, and data partition is deleted. Device returns to factory state.

Software Security

Data Protection (11)

- Files are marked with a Data Protection Class to determine when they are accessible.
    - Complete protection - only accessible when device is unlocked
    - Protected Unless Open - accessible only if app has file open while device is locked
    - Protected Until First User Authentication - Accessible only after a post-reboot unlock
    - No protection - encrypted, but accessible whether device is locked or unlocked

Software Security

Data Protection (III)

- Keychains and Keybags are protected similarly, with varying levels of assignable protection.

Network Security

Network Security

Firewall?

- No firewall
- Reduces attack surface by limiting entry points
- Apps that open ports are heavily sandboxed

Network Security

VPN

- L2TP, PPTP, IPSec
- Cert-based VPN on Demand
- Per-app VPN

Network Security

Wi-Fi

- WEP (no!)
- WPA/WPA2 Personal and Enterprise
- 802.1x authentication

Network Security

AirDrop

- Bluetooth LE for discovery
- Encrypted peer-to-peer Wi-Fi for transfer

Network Security

Apple Services

- All Apple services that involve user data are encrypted end-to-end.
    - iCloud, iMessage, FaceTime, Siri, Push Notifications, App Store, Software Updates

Network Security

iCloud Backup

- Encrypted files stored on iCloud servers
- Keys for files stored in iCloud backup Keybag based on their protection class
- Keybag is encrypted with a randomized key stored in user's iCloud account
- When restoring to new device, iCloud retrieves key from account and unlocks keybag to allow restore
- Files copied to new device are re-encrypted using new device's UID

Best Practices

Best Practices

Passcode, Passcode, Passcode!

- Data Protection is only enabled when a passcode is used.
- Prevents physical use of almost all device features.
- Data Protection uses passcode + UID to strengthen encryption. Brute force decryption attempts would have to occur on the device.
- Use a complex passcode, or manage via profile
- Turn on “Erase after 10 failed attempts”

Best Practices

Don’t Jailbreak

- Breaks the secure boot chain
- Weakens Data Protection
- Dramatically increases attack surface
- As of June 2014, 8 of 11 known iOS malware threats relied on a jailbroken device.

Best Practices

Avoid Unknown iDEP Apps

- Apps signed with Developer Enterprise Program
- No code review

Best Practices

Enable Find My iPhone

- Find your device if lost, but also…

- Activation Lock - prevents your device from being wiped or re-activated without your iCloud login

Best Practices

Use Apple Configurator or MDM (1)

- Enforce passcode policies
  - allow simple value, require alphanumeric value, minimum length, minimum number of complex chars, max passcode age, passcode history, auto-lock timeout, grace period for device lock. max number of failed attempts, allow touch ID

Best Practices

Use Apple Configurator or MDM (II)

Best Practices

Use Apple Configurator or MDM (III)

- Remote Wipe (MDM)
- Supervised Mode (Configurator)
- Disable Camera, FaceTime, Siri, iCloud, app installs, YouTube, iTunes Store, Safari, and more

References & Resources

- iOS Security - February 2014
  http://images.apple.com/ipad/business/docs/iOS_Security_Feb14.pdf

- Apple iOS 7 Security Technical Implementation Guide
  http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html

- iOS Hardening Configuration Guide
  http://www.asd.gov.au/publications/iOS7_Hardening_Guide.pdf

- iOS Malware Does Exist
  http://blog.fortinet.com/iOS-malware-do-exist/

Q&A

Thanks!

2014
MACADMINS
CONFERENCE
AT PENN STATE

Feedback - http://j.mp/psumac33