How iOS Security Really Works

Session 705

Ivan Krstić Head of Security Engineering & Architecture
Mobile Devices Today

Unprecedented record of our lives

Gb of Data
Mobile Devices Today

Unprecedented record of our lives

Gb of Data
Mobile Devices Today
Unprecedented record of our lives
Mobile Devices Today

Unprecedented record of our lives

Gb of Data
Who Might Be an Attacker
Who Might Be an Attacker

Criminals
Who Might Be an Attacker

Criminals
Business competitors
Who Might Be an Attacker

Criminals
Business competitors
Service providers
Who Might Be an Attacker

- Criminals
- Business competitors
- Service providers
- Nation states
Who Might Be an Attacker

Criminals
Business competitors
Service providers
Nation states
Romantic partners, family, friends
Who Might Be an Attacker

Criminals
Business competitors
Service providers
Nation states
Romantic partners, family, friends
Cats
What Do Attackers Want?
What Do Attackers Want?

Personal stalking and surveillance
What Do Attackers Want?

Personal stalking and surveillance

Corporate espionage
What Do Attackers Want?

- Personal stalking and surveillance
- Corporate espionage
- Direct financial benefit
How Do We Know This?
We see it on other platforms
But Not on iOS

No malware has affected iOS devices at scale
iOS Security
iOS Security

Decade-long effort to protect customers from security problems
iOS Security

Decade-long effort to protect customers from security problems

Incredible scale
iOS Security

Decade-long effort to protect customers from security problems

Incredible scale

Every single iOS security feature is designed to thwart a real security threat
iOS Security Pillars
iOS Platform Security

Users Upgrading their Software

Developers Building Secure Apps
iOS Platform Security

Users Upgrading their Software

Developers Building Secure Apps
<table>
<thead>
<tr>
<th>Traditional Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>physical security</td>
</tr>
<tr>
<td>secure configuration</td>
</tr>
<tr>
<td>installing latest patches</td>
</tr>
<tr>
<td>password policy</td>
</tr>
<tr>
<td>vetted apps</td>
</tr>
<tr>
<td>mandated policies</td>
</tr>
<tr>
<td>Traditional Security</td>
</tr>
<tr>
<td>-----------------------------------</td>
</tr>
<tr>
<td>physical security</td>
</tr>
<tr>
<td>secure configuration</td>
</tr>
<tr>
<td>installing latest patches</td>
</tr>
<tr>
<td>password policy</td>
</tr>
<tr>
<td>vetted apps</td>
</tr>
<tr>
<td>mandated policies</td>
</tr>
</tbody>
</table>
1. Secure Boot
2. Data Protection
3. Sandboxing
4. Code Signing
5. Touch ID
1. Secure Boot
2. Data Protection
3. Sandboxing
4. Code Signing
5. Touch ID
Trust built from silicon up
Application Processor
Apple Public Key

Boot ROM

Application Processor
Application Processor

Apple Public Key
Boot ROM

Low-Level Bootloader (LLB)

iBoot

Kernel

Apple Public Key
Application Processor

Boot ROM

Low-Level Bootloader (LLB)

iBoot

Kernel

iOS

Apple Public Key
Trusting Secure Boot
Trusting Secure Boot

Keys are securely provisioned and managed by Apple
Trusting Secure Boot

Keys are securely provisioned and managed by Apple
Software updates are authorized individually for each device
Secure Boot

Data Protection

Sandboxing

Code Signing

Touch ID
Secure Boot

Data Protection

Sandboxing

Code Signing

Touch ID
Data Protection
Data Protection

User data is encrypted at rest with keys derived from the passcode.
Data Protection

User data is encrypted at rest with keys derived from the passcode
Entangled with hardware key in SEP
Data Protection
Data Protection

SEP refuses to unlock after more than 10 incorrect passcode attempts
Data Protection

SEP refuses to unlock after more than 10 incorrect passcode attempts
‘Erase Data’ only controls erasure, not ability to unlock
Standard algorithms
Internal security audits
3rd-party code review
Cryptographic Libraries

The same libraries that secure iOS and OS X are available to third-party developers to help them build advanced security features.

Security Framework
Security Framework provides interfaces for managing certificates, public and private keys, and trust policies. It supports the generation of cryptographically secure pseudorandom numbers. It also supports the storage of certificates and cryptographic keys in the keychain, which is a secure repository for sensitive user data.

Common Crypto
The Common Crypto library provides additional support for operations like symmetric encryption, hash-based message authentication codes, and digests.

corecrypto
Both Security Framework and Common Crypto rely on the corecrypto library to provide implementations of low level cryptographic primitives. This is also the library submitted for validation of compliance with U.S. Federal Information Processing Standards (FIPS) 140-2 Level 3. Although corecrypto does not directly provide programming interfaces for developers and should not be used by iOS or OS X apps, the source code is available to allow for verification of its security characteristics and correct functioning.

Download corecrypto source
1. Secure Boot
2. Data Protection
3. Sandboxing
4. Code Signing
5. Touch ID
Secure Boot
Data Protection
Sandboxing
Code Signing
Touch ID
Isolating data between apps
Allow "Maps" to access your location while you use the app?

Your location may be shown on the map and is used to provide things such as directions and nearby search results.

[Buttons: Don't Allow, Allow]
Transparency

Consent

Control

Allow "Maps" to access your location while you use the app?

Your location may be shown on the map and is used to provide things such as directions and nearby search results.

Don't Allow  Allow
1. Secure Boot
2. Data Protection
3. Sandboxing
4. Code Signing
5. Touch ID
1. Secure Boot
2. Data Protection
3. Sandboxing
4. Code Signing
5. Touch ID
Code Signing
Code Signing

Attacker’s first step: code execution

iOS code signing covers not just the OS, but every app that runs
Secure Boot

Data Protection

Sandboxing

Code Signing

Touch ID
1. Secure Boot
2. Data Protection
3. Sandboxing
4. Code Signing
5. Touch ID
Average user unlocks per day

80
Easy
Fast
Protects user data
Secure Enclave

Touch ID

Sensor

Secure Enclave
Touch ID

Sensor

Link encrypted with Shared Secret

Secure Enclave
Touch ID

Sensor → Secure Enclave

Link encrypted with Shared Secret
Touch ID

Sensor

Secure Enclave

Link encrypted with Shared Secret
Touch ID

Sensor

Link encrypted with Shared Secret

Secure Enclave
Touch ID

Sensor

Link encrypted with Shared Secret

Secure Enclave

01001010
10100101
01010001
01010001
11100001
Touch ID

Sensor

Secure Enclave

Link encrypted with Shared Secret

01 01 10
10 0 101
010 0 1
1 10 0
Passcode usage before Touch ID

49%
Passcode usage after Touch ID

89%
iOS Platform Security

Users Upgrading their Software

Developers Building Secure Apps
iOS Platform Security

Users Upgrading their Software

Developers Building Secure Apps
Smaller install footprint

<table>
<thead>
<tr>
<th>Size</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5GB</td>
<td></td>
</tr>
<tr>
<td>4GB</td>
<td></td>
</tr>
<tr>
<td>3GB</td>
<td></td>
</tr>
<tr>
<td>2GB</td>
<td></td>
</tr>
<tr>
<td>1GB</td>
<td></td>
</tr>
</tbody>
</table>
Smaller install footprint

<table>
<thead>
<tr>
<th>Size (GB)</th>
<th>iOS 8</th>
<th>iOS 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Smaller install footprint

- iOS 8: 4.6GB
- iOS 9: 5GB
- iOS 4GB: 4GB
- iOS 3GB: 3GB
- iOS 2GB: 2GB
- iOS 1GB: 1GB
Smaller install footprint

- iOS 8: 4.6GB
- iOS 9: 1.3GB
Software Update

iOS 9.3.1 is available for your iPhone and is ready to install.

Install Now
Later
Details
Android Installed Base

- Earlier: 89.9%
- 6.0: 10.1%
iOS Platform Security

Users Upgrading their Software

Developers Building Secure Apps
iOS Platform Security

Users Upgrading their Software

Developers Building Secure Apps
Follow Best Practices
Follow Best Practices

Touch ID
App Transport Security
Follow Best Practices

Touch ID

App Transport Security

• Required by App Store at end of 2016
Follow Best Practices

Touch ID

App Transport Security

• Required by App Store at end of 2016

• TLS v1.2, with exceptions for already-encrypted bulk data like media streaming
Know Your Code
Know Your Code

You are responsible for third-party code you include in your apps
Know Your Code

You are responsible for third-party code you include in your apps.
Libraries you use may undermine app security.
Know Your Code

You are responsible for third-party code you include in your apps
Libraries you use may undermine app security
Keep them current!
iOS Platform Security

Users Upgrading their Software

Developers Building Secure Apps
iOS Platform Security

Users Upgrading their Software

Developers Building Secure Apps
How well are we doing?
No iOS malware at scale
5-10 vulnerabilities
$1 million
Security is a process, not a destination
More Information

https://developer.apple.com/wwdc16/705
<table>
<thead>
<tr>
<th>Session</th>
<th>Location</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>What’s New in Security</td>
<td>Nob Hill</td>
<td>Tuesday 5:00PM</td>
</tr>
<tr>
<td>Engineering Privacy for Your Users</td>
<td>Pacific Heights</td>
<td>Wednesday 4:00PM</td>
</tr>
<tr>
<td>Labs</td>
<td>Frameworks Lab C</td>
<td>Wednesday 9:00AM</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Security &amp; Privacy Lab 1</td>
<td>Frameworks Lab C</td>
<td>Wednesday 9:00AM</td>
</tr>
<tr>
<td>Security &amp; Privacy Lab 2</td>
<td>Frameworks Lab B</td>
<td>Thursday 9:00AM</td>
</tr>
</tbody>
</table>