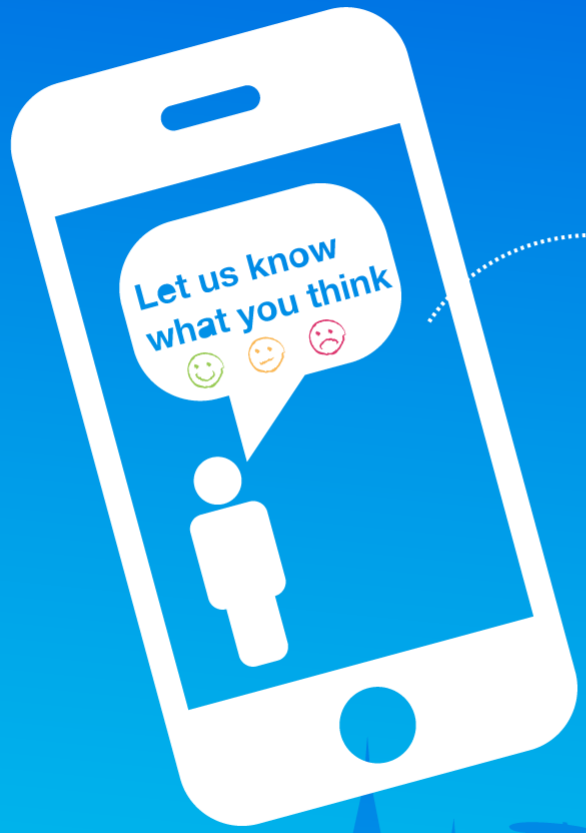
goto; conference

Security threats and mitigations for iOS developers

Emil Kvarnhammar
www.truesecdev.com
Twitter: @emilkvarnhammar

Join the conversation #gotocph

goto; conference



Click ‘engage’
to rate sessions
and ask questions

Join the conversation #gotocph

Isn’t iOS secure?

TrueSec

Q1 2014 : goto fail;

Major Apple security flaw: Patch issued, users open to MITM attacks

Apple rushed the release of iOS 7.0.6 on Friday with a patch for a shockingly overlooked SSL encryption issue that leaves iPhone, iPad and Mac computer users open to a man-in-the-middle (MITM) attack.

By Violet Blue for Zero Day | February 22, 2014 -- 10:30 GMT (10:30 GMT) | Topic: Security

TrueSec

Q4 2014 : Wirelurker (Masque attacks)

Apple Has Shut Down The 'WireLurker' Malware Attacking iPads and iPhones

Sam Colt

Nov. 7, 2014, 12:07 AM 419

TrueSec

Q2 2015 : New Masque Attacks

Hackers discover way to crack into Apple devices

by Jonathan Vanian @JonathanVanian AUGUST 6, 2015, 12:35 PM EDT

TrueSec

Q3 2015 : AirDrop vulnerability

iOS 9, OS X El Capitan close serious AirDrop vulnerability allowing malware infections

By Roger Fingas
Thursday, September 17, 2015, 08:10 am PT (11:10 am ET)

iOS 9 and the forthcoming OS X El Capitan address a vulnerability in Apple's AirDrop feature that could allow malware infections and the theft of sensitive data, according to a security researcher.

Q3 2015 : Xcode Ghost

TrueSec

Xcode Ghost

WeChat

DiDi Taxi

58 Classified - Job, Used Cars, Rent

Gaode Map - Driving and Public Transportation

Railroad 12306

Flush

China Unicom Customer Service (Official Version)*

CarrotFantasy 2: Daily Battle*

Miraculous Warmth

Call Me MT 2 - Multi-server version

Angry Bird 2 - Yifeng Li's Favorite*

Baidu Music - A Music Player that has Downloads, Ringtones, Music Videos, Radio, and Karaoke

DuoDuo Ringtone

NetEase Music - An Essential for Radio and Song Download

Foreign Harbor - The Hottest Platform for Oversea Shopping*

TrueSec

From an attacker's point of view

TrueSec

What's of interest?

- **Extracting app data**
  - Credentials, Documents, Email etc.
- **Execute code**
  - Impersonate legitimate apps
  - Steal app data
  - Phishing (credentials, credit card details etc.)
  - Command & Control (botnets etc.)

What are the security mechanisms?

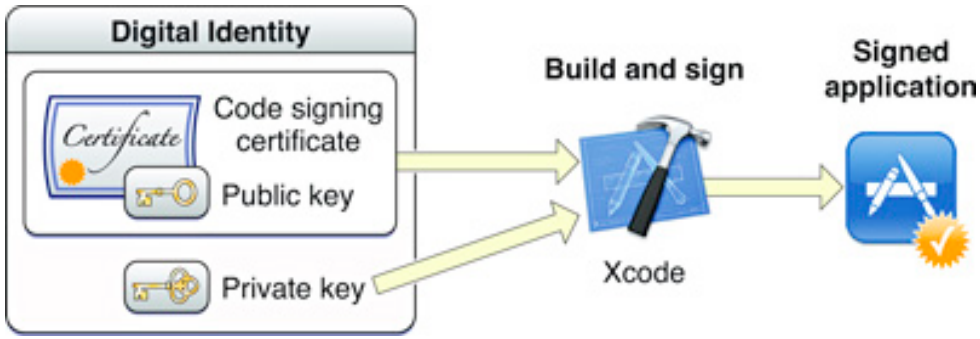
What are the security mechanisms?

1. App store review

TrueSec

What are the security mechanisms?

2. Mandatory code signing



TrueSec

Deploy the next generation of apps to your enterprise.

Get tools and resources to transform your mobile workforce with enterprise-class iOS and Mac apps, distributed seamlessly and securely within your organization. Join the Apple Developer Enterprise program for $299 per year and get everything you need to start distributing proprietary in-house apps to your employees.

Used to bypass app store review!

TrueSec

What are the security mechanisms?

3. Sandboxing

TrueSec

Sandboxing

- Enforced by platform
- Break-out vulnerabilities in almost all versions
  - Used by jailbreaks
  - App store is an extra safety net
- Cross-app access
  - Extensions
  - Custom URI scheme

What are the security mechanisms?

4. Data protection (at rest)

TrueSec

Data protection

- Default encryption since iOS 8 (if passcode set)
  - NSFileProtectionComplete* flags
- Attacks
  - Backups (iCloud or iTunes)
  - Jailbreak
  - Masque attacks

Preventing backup of file

```
BOOL success = [URL setResourceValue: [NSNumber numberWithBool: YES]
                              forKey: NSURLIsExcludedFromBackupKey
                               error: &error];
```

https://developer.apple.com/library/ios/qa/qa1719/_index.html

TrueSec

Keychain items

Use *ThisDeviceOnly access keys

Example: kSecAttrAccessibleAfterFirstUnlockThisDeviceOnly

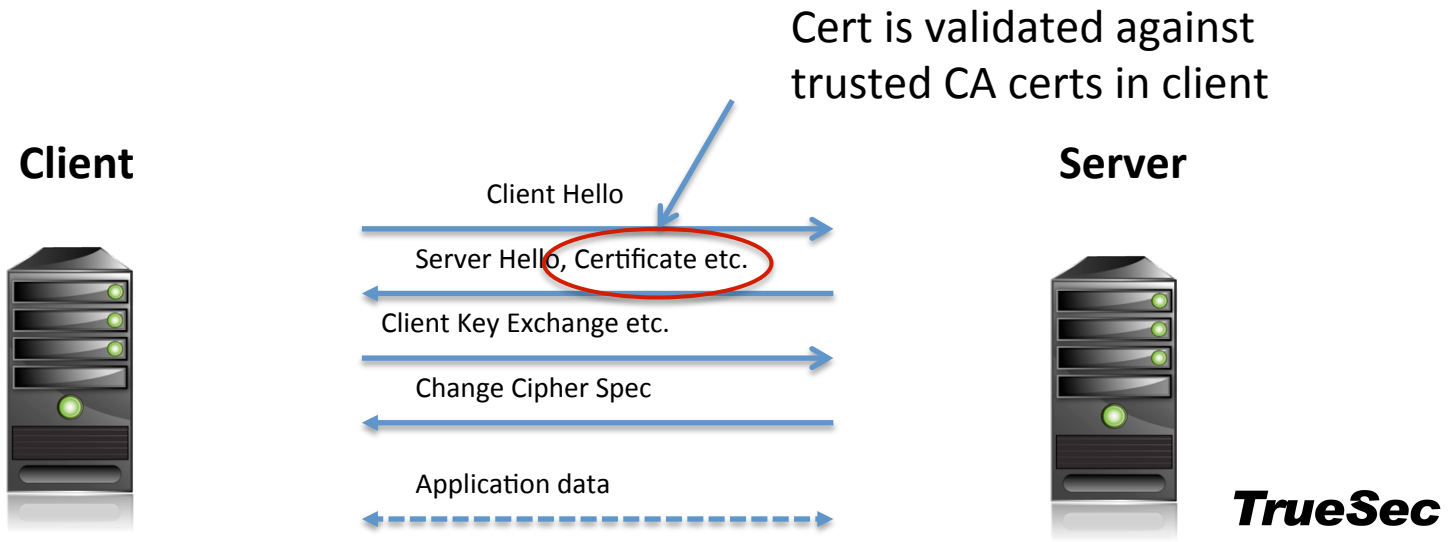
What are the security mechanisms?

5. App Transport Security

TrueSec

SSL/TLS

Authenticity | **Confidentiality** | **Integrity**



TrueSec

App Transport Security

- Enforces best practices for server connections
  - https only
  - Only trusted certificates
  - TLS version 1.2, with forward secrecy

Developers must explicitly opt-out

[Don't opt-out!]

TrueSec

More regarding SSL/TLS…

- **Cert pinning is recommended**
  - Validate certificate chain
  - Validate that cert corresponds to host name
- **If you use AFNetworking…**
  - Your app might be vulnerable to MiTM atttacks
  - Update to latest version

Time for demos…

Masque attacks

- App Masque
- URL Masque
- Extension Masque
- …and more

https://www.fireeye.com/blog/threat-research/2015/06/three_new_masqueatt.html

Injecting code in Xcode

- Steal Apple ID developer account
- Inject code in apps

TrueSec

Summary

Summary

- Several great security mechanisms in iOS
- …but also vulnerabilities
  - Apps can be replaced
  - App data can be stolen
- Attackers attack your developer machines
  - Patch
  - Encrypt
  - Be careful what “tools” you are downloading

Full day about security for developers:

http://oredev.org/2015/security-day

Emil Kvarnhammar
www.truesecdev.com
Twitter: @emilkvarnhammar

TrueSec

goto; conference

Please

Remember to rate this session

Thank you!

Join the conversation #gotocph