

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Assume a hostile environment: securing mobile data in the app

SESSION ID: MBS-T09

Scott Alexander-Bown

Senior Mobile Developer
viaForensics
@scottyab





DEVELOPERS
DEVELOPERS
DEVELOPERS
DEVELOPERS

The Gap!



Goals

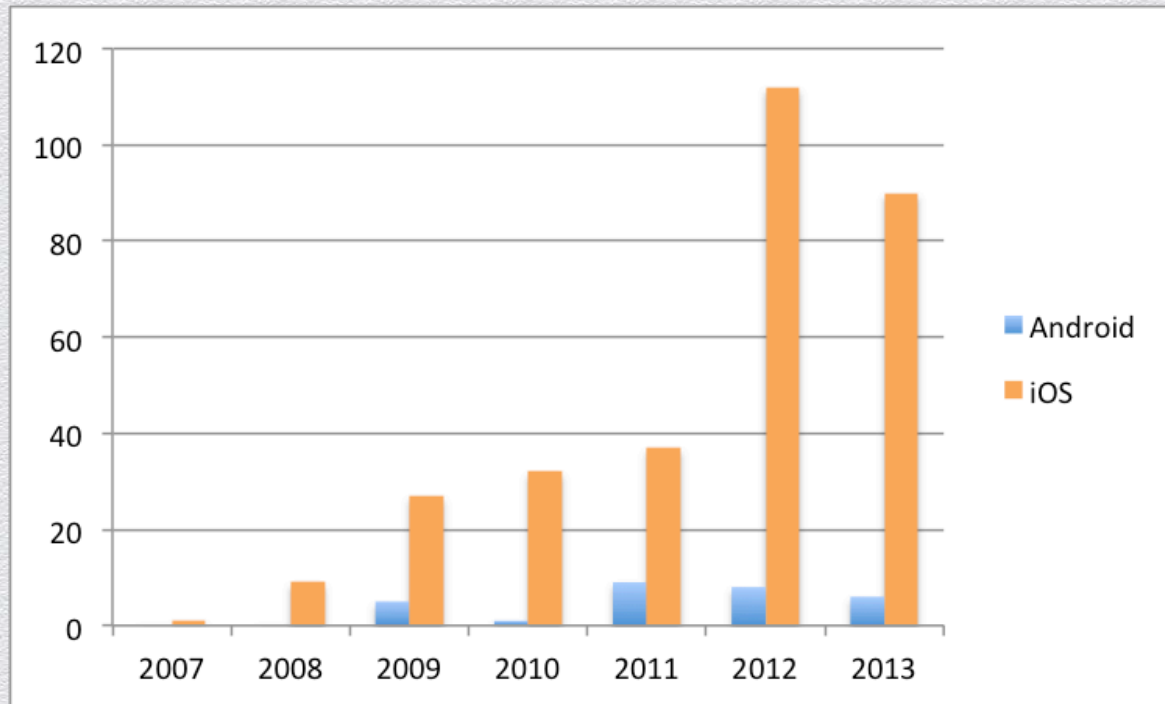
- ◆ Mobile devices are a hostile environment
- ◆ What are the common app vulnerabilities
- ◆ How to protect your apps
 - ◆ With an Android bias
- ◆ Questions to ask your app developers

Non Goals: There Is No 100% Security



Q) Which Is More Secure?





iOS vs Android OS Vulnerabilities

Source: <http://www.cvedetails.com> Dec 2013

iOS: Safer for average hipster Joe



Android can be hardened (power users)



The Environment Is Hostile

- ◆ Lost / Stolen
- ◆ Open Wi-Fi networks
- ◆ SMiShing
- ◆ Untrusted ports/chargers

Devices Are Hostile Environments


- ◆ System updates
- ◆ OEM/Carrier bloatware (Android)
- ◆ MDM
- ◆ Secure Containers
- ◆ System library's i.e KeyChain (iOS)
- ◆ Device Encryption
- ◆ Side load (Android)
- ◆ Vulnerable apps / malware

If devices are hostile environments?

We focus on the app!

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Common App Vulnerabilities

Common App Fails

- ◆ Not encrypting stored data
- ◆ Not using SSL connection
- ◆ Not protecting App components
- ◆ Not validating client data
- ◆ Leaking sensitive data to device log

**WE ENCRYPT OUR APP
DATA**



**BUT... HARDCODE THE
KEYS**

memegenerator.net

WE USE SSL



BUT DON'T USE SSL PINNING

meme-generator.net

Options For App Security

- ◆ MDM security SDK?
- ◆ App Wrapping?
- ◆ Built-in
 - ◆ Distribute via app stores
 - ◆ Better UX
 - ◆ Not relying on others



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Build in App Security

SQL Injection

- ◆ Compiled statements
- ◆ Validate input
- ◆ Sharing data (Android)
 - ◆ Protect components
 - ◆ Custom permissions
 - ◆ Consider read only

Encryption

- ◆ Assess risk of data stored
- ◆ Bundle your own crypto libraries
 - ◆ SpongyCastle adds support:
 - ◆ AES-GCM
 - ◆ Elliptic Curve Cryptography (ECC)
- ◆ Don't seed SecureRandom class



Encryption: Not Storing The Key

- ◆ Password Based Encryption (PBE)
 - ◆ Generate a key from user pin/password
 - ◆ KDF - more iterations the better
 - ◆ Add app time out to clear from memory
- ◆ The KeyStore provider (Android 4.3+)
 - ◆ Hardware backed (on some devices)



Encryption: Android Quick Wins

- ◆ SQLCipher
 - ◆ 256-bit AES Encrypt SQLite database
- ◆ Secure-Preferences
 - ◆ 'obscure' your app's shared preferences
- ◆ IOCipher
 - ◆ Virtual encrypted disk
- ◆ Conceal
 - ◆ Easy to use APIs for fast encryption and authentication of data

SQLCIPHER



THE GUARDIAN
PROJECT
<https://guardianproject.info>

Update required

A critical update is required for this app. Please update to continue.

Stop using app

Update

Timeout / Caching

- ◆ Session timeout
 - ◆ App and Server-side
 - ◆ Clear app data from memory
- ◆ Prevent snapshot cache (iOS)
- ◆ Exclude from recent tasks (Android)

Q) Are you using SSL?



Q) Is Using SSL Enough?

- ◆ A) No



Stronger SSL

- ◆ Use secure SSL/TLS protocols (i.e. SSL v3, TLS v1.1/1.2)
- ◆ Use secure ciphers (128 bit or higher)
- ◆ Validate the certificates
 - ◆ NetCipher
 - ◆ Whole chain validation
 - ◆ Orbot: Proxy with Tor



THE GUARDIAN
PROJECT
<https://guardianproject.info>




SSL Pinning

- ◆ 2 types
 - ◆ Certificate pinning
 - ◆ Public key pinning
- ◆ Prevent compromised CAs from being trusted
- ◆ More difficult for MITM



Watch For This!

```
public class TrustAllX509TrustManager implements X509TrustManager {  
  
    @Override  
    public void checkServerTrusted(X509Certificate[] chain, String authType)  
        throws CertificateException {  
        // do nothing, trust all :(  
    }  
  
    public void checkClientTrusted(X509Certificate[] chain, String authType)..  
  
    public X509Certificate[] getAcceptedIssuers() {..  
}
```



Tamper Detection

- ◆ Simulator/emulator check
 - ◆ System properties
- ◆ Jail break/Root check
 - ◆ Root apps (Cydia, SuperSU etc)
 - ◆ System properties
- ◆ Validate signing key (Android)



Anti Reversing

- ◆ Obfuscation code
 - ◆ Proguard (Android)
- ◆ Restrict Debugging
- ◆ Restrict Logging



DexGuard (Android)

- ◆ ProGuard's bad ass brother
- ◆ Same config as ProGuard
- ◆ Not free but 1 license == ∞ apps
- ◆ Highlights
 - ◆ One line tamper check
 - ◆ 嚙\$鵒.smali, Œ\$鵒.smali
 - ◆ API hiding with String encryption == tough



Further Resources

- ◆ 42+ Secure mobile development best practices
 - ◆ <http://bit.ly/viafor42>
- ◆ OWASP Mobile security recommendations
 - ◆ <http://bit.ly/owaspmobile>



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



What To Ask?

What to ask your app developers?

- ◆ Who is building it and where?
- ◆ Are they certified?
 - ◆ bit.ly/mobilesecuritycert
- ◆ Play/App store account access?
- ◆ How is security assessed?
 - ◆ Code reviews (including 3rd party libs)
 - ◆ Static analysis
 - ◆ Red team black box assessment



Summary

- ◆ Mobile devices are a hostile environment
- ◆ What are the common app vulnerabilities
- ◆ How to protect your apps
- ◆ Questions to ask your app developers

Q&A | Contact | Feedback

◆ Thanks for listening...



@scottyab



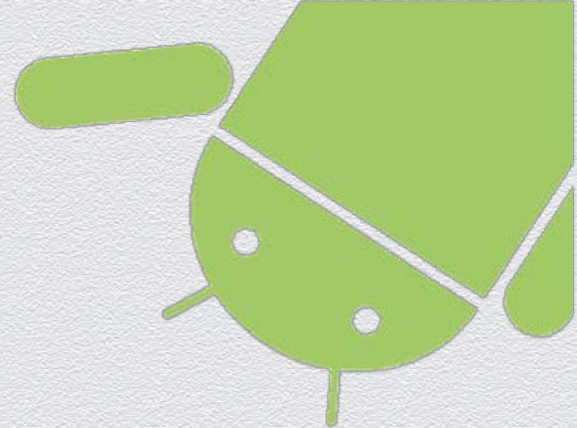
github/scottyab



SAlexander-Bown@viaforensics.com



Book signing tomorrow 3:30pm



Thanks to @thomas_cannon

Build in app security.

Reference

- ◆ <http://github.com/rtyley/spongycastle>
- ◆ Encryption sample projects
 - ◆ <http://github.com/nelenkov/android-pbe>
 - ◆ <http://github.com/nelenkov/android-keystore>
 - ◆ <https://github.com/moxie0/AndroidPinning>
- ◆ NetCipher - <https://github.com/guardianproject/NetCipher>
- ◆ DexGuard - www.saikoa.com/dexguard
- ◆ SQLCipher - <http://sqlcipher.net/sqlcipher-for-android>
- ◆ Secure-Preferences - <http://github.com/scottyab/secure-preferences>
- ◆ IOCipher - <http://guardianproject.info/code/iocipher>
- ◆ Conceal - <http://facebook.github.io/conceal>
- ◆ Android security cookbook ISBN:1782167161
 - ◆ <http://bit.ly/MscEFu>