cigital

Mobile Security 2013
Phenomenal Cosmic Power, Itty Bitty Living Space

Joel Scambray
Managing Principal, Cigital

cigital

Software Confidence. Achieved.

The Hype

- Mobile is huge
- Mobile is insecure

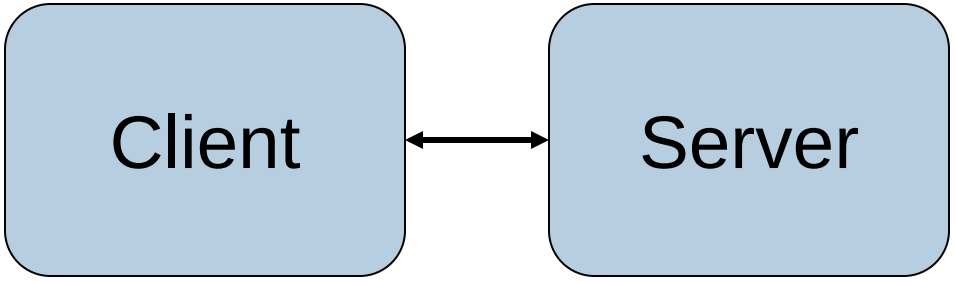
- What do we do?!?

cigital

The Reality: Same Problem…

What's the same:

- Client/server architecture
- Software developers
- Security
- Etc…



cigital

…Different Day

What's different:

- Client risk model
  - Physical
  - Converged communications
  - Promiscuous apps, poor isolation

Probability

Impact

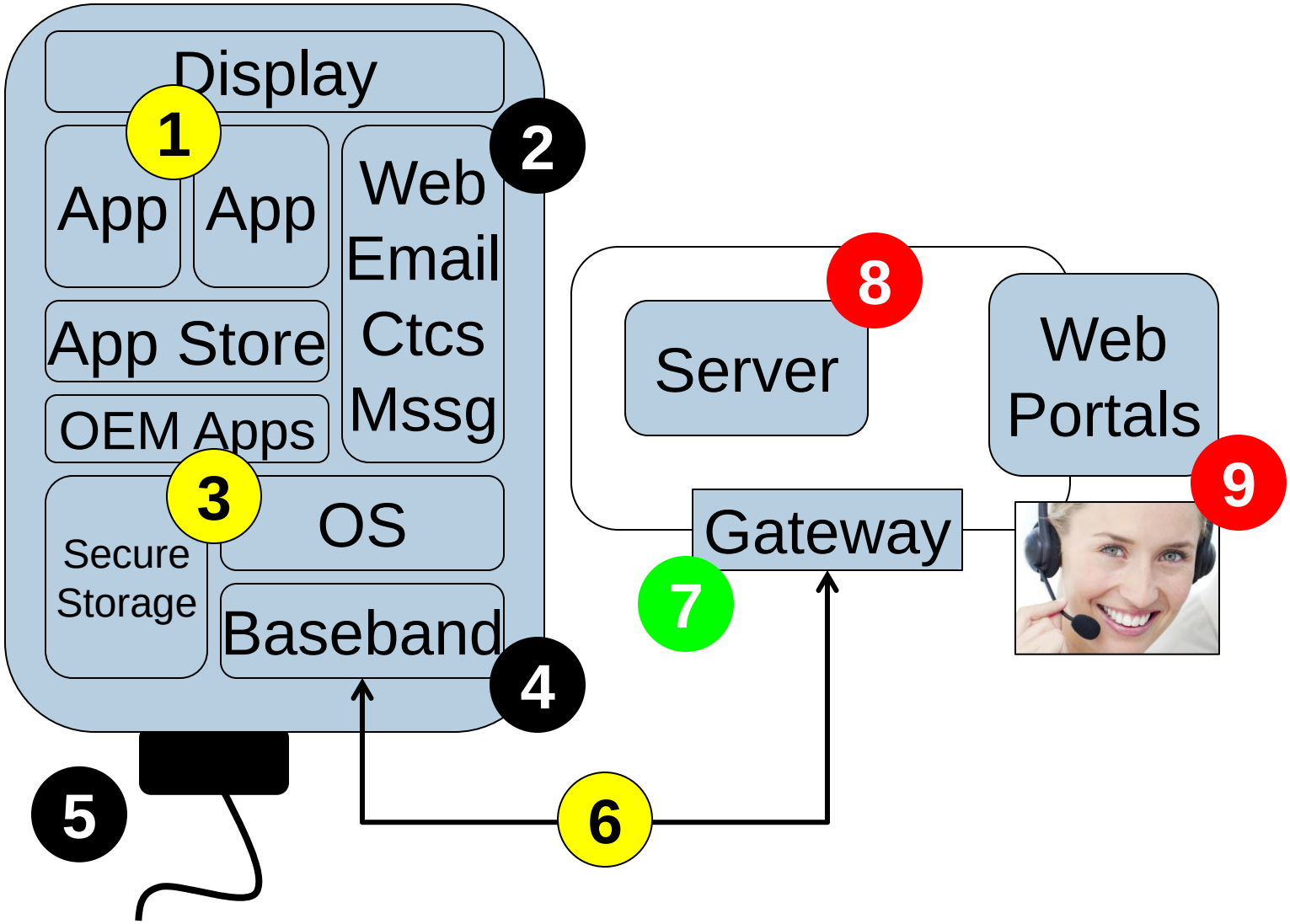
- App Data
- Contacts
- Location
- Camera/photos
- SMS…

Phenomenal Cosmic Power…

…Itty Bitty Living Space.

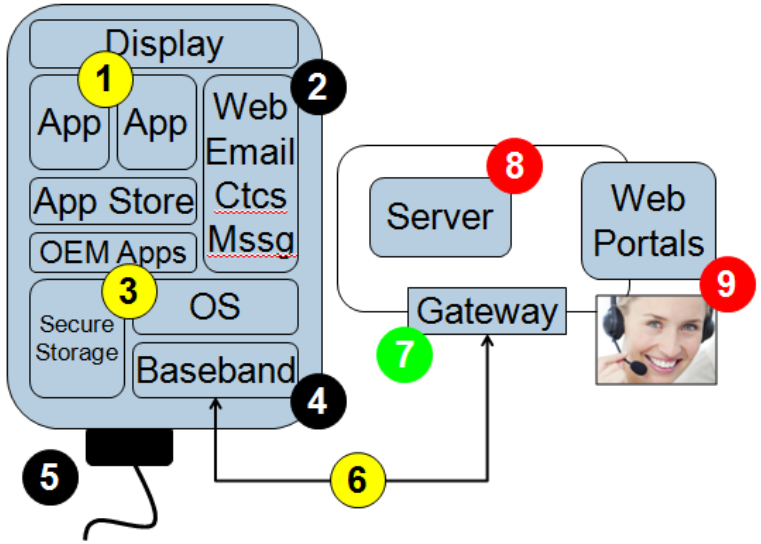
cigital

The Mobile Risk Ecosystem



Mobile Risks

9. Support abuse
8. Web security
7. (Security gateway helps)
6. No SSL/TLS
5. Physical attacks (e.g. jailbreak)
4. “Baseband” radio exploits

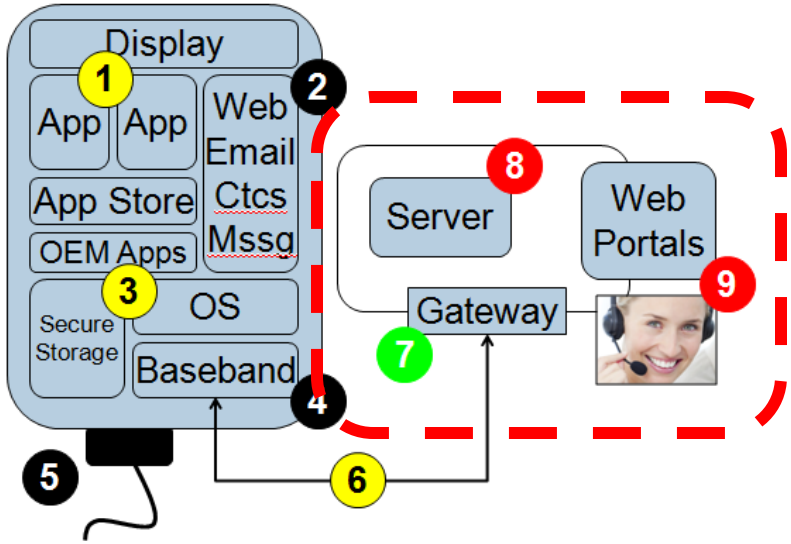


3. (ins)secure storage
2. On-device services
1. Vulnerable apps

cigital

Observation 1: It's The Service, Stupid

- Notice where the red is?
- "That's where the money is"
- Necessary Evil: Support
- Mat Honan "Epic Hack," Apple's iForgot self-help password reset tool, etc.

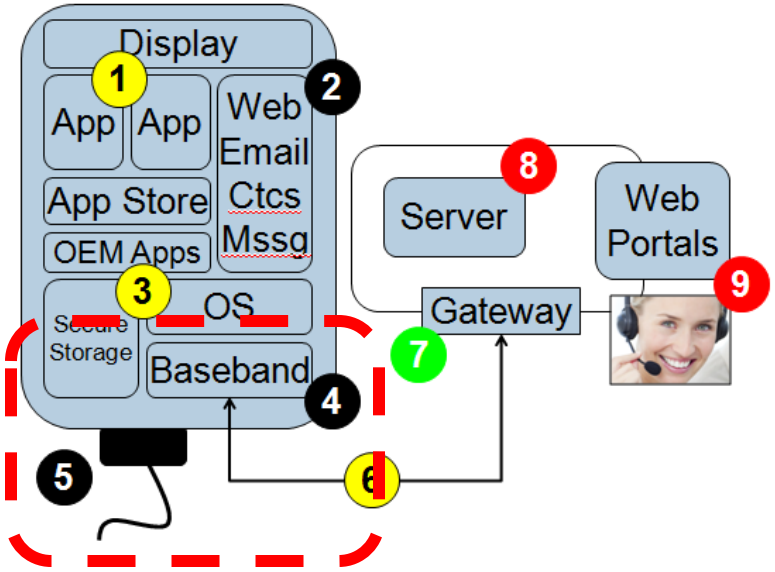


- Silver Lining: Security Gateway

cigital

Observation 2: Physical = Game Over

- Immutable Laws of Computer Security #3: It's not your computer anymore…
- No defense against rogue base station attack
- Debug cable wins

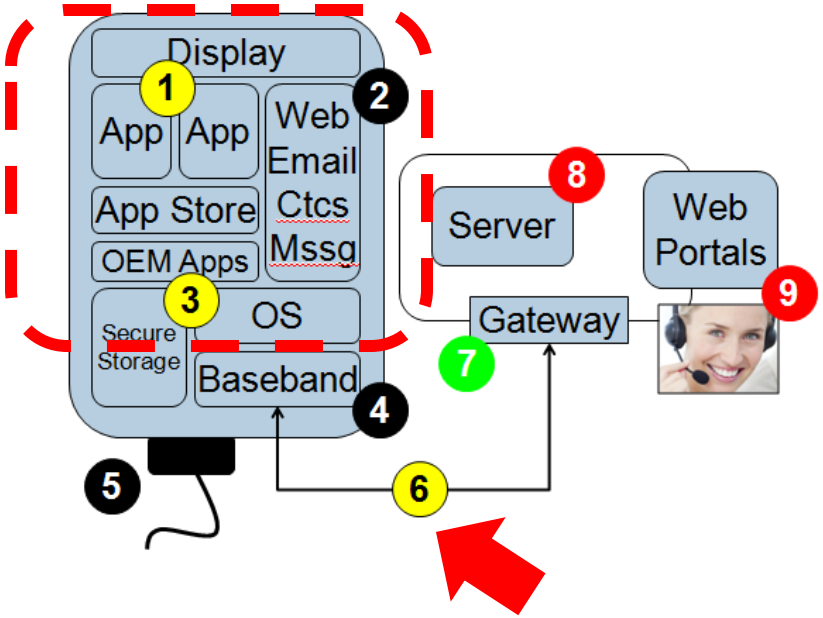


- Silver Lining: Airplane Mode ☺

cigital

Observation 3: It's The Apps, Stupid

- Apps = user-facing functions, data
- Upstream evolution: net/OS/apps/phishing
- Variables:
  - Platform protections
  - Developer savvy



- Silver Lining: iOS apps walled garden

cigital

Mobile App Risks Sampler

- Sensitive information leakage
  - Logs
    - Android: read all if debug on (re-delegation)
    - iOS: disable NSLog statements
  - WebView cache, cookies
  - iOS app screenshots & keyboard cache
- Injection
  - Malicious Android Intents
  - JavaScript `eval`
  - Bridging native OS and JavaScript
  - URL launched from/executed in app context

cigital

How Do We Fix This Stuff?

- MNOs
- OS vendors
- Hardware vendors
- App stores
- MDM vendors
- Cloud services
- Standards bodies (e.g. payment APIs)

- End users, corporate IT, developers, etc. rely heavily on these foundations

cigital

Secure Mobile Dev Guidelines

Prepare:

- Threat Model
- Native vs. Mobile Web vs. Cross-Platform Fx
- MDM
- MAM and App Stores
- Anti-debugging and obfuscation

Develop:

- Traditional Web Application Security ++
- Storing Sensitive Data on the Device
- Authenticating to Mobile Services
- Secure Communications
- WebView Interaction
- Information Leakage Prevention
- iOS - Specific Guidelines
- Android - Specific Guidelines

cigital

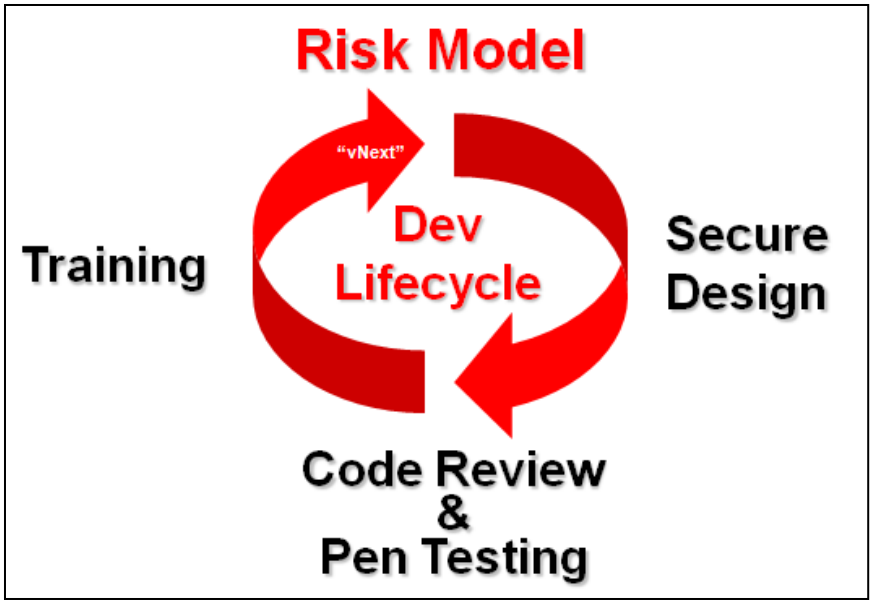
Stick to the Fundamentals: SSDL

Design

- What are you trying to protect?
- Threat modeling

Build

- Security in the development process; code review, pen test, training, etc.

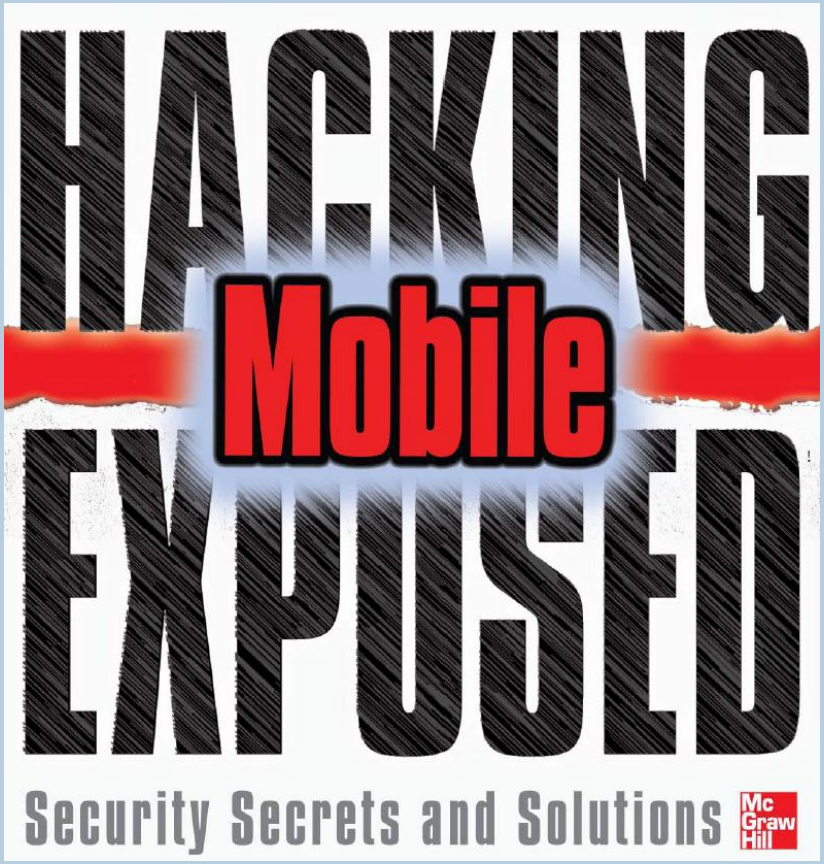


Operate

- Rinse, patch, & repeat (improve) across releases

cigital

Coming Soon!



jscambray_at_cigital_dot_com

cigital

Software Confidence. Achieved.

References

- Mat Honan “Epic Hack”: http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/
- The Verge article “Major security hole allows Apple passwords to be reset with only email address, date of birth (update)” http://www.theverge.com/2013/3/22/4136242/major-security-hole-allows-apple-id-passwords-reset-with-email-date-of-birth
- 10 Immutable Laws of Security: http://technet.microsoft.com/en-us/library/cc722487.aspx
- FTC Complaint and Order with HTC: http://www.ftc.gov/opa/2013/02/htc.shtm

cigital

Secure Mobile Dev References

Resource	Link
Apple's Secure Coding Guide	developer.apple.com/library/mac/documentation/security/conceptual/SecureCodingGuide/SecureCodingGuide.pdf
Android Security Overview	source.android.com/tech/security/
Android Security Best Practices for developers	developer.android.com/training/articles/security-tips.html
NIST SP 800-124 "Guidelines for Managing and Securing Mobile Devices in the Enterprise"	csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf
iOS Developer Library	developer.apple.com

cigital