Security in knowledge

# CAN YOU TRUST YOUR MOBILE APPLICATIONS?

Ryan English

HP Fortify On Demand

RSA CONFERENCE 2013

Session ID: SP01-W23B

Session Classification: Intermediate

# Abstract


- Hear the truth behind mobile application security and what choices you have. Learn about the most common mobile application threats and what leading companies are doing to ensure their mobile applications are not the source of a successful breach. In addition to seeing real world examples, benefit from hearing results of comprehensive mobile assessments that HP performed in 2012

# Mobile Application Security Challenge

- Difficult to train and retain staff - very difficult to keep skills up-to-date
- Constantly changing environment
- New attacks constantly emerge
- Compliance Requirements
- Too many tools for various results
- Apps are getting launched on a daily basis with Security not being involved.
- Junior Developers are typically the ones creating the apps.

# How you see your world

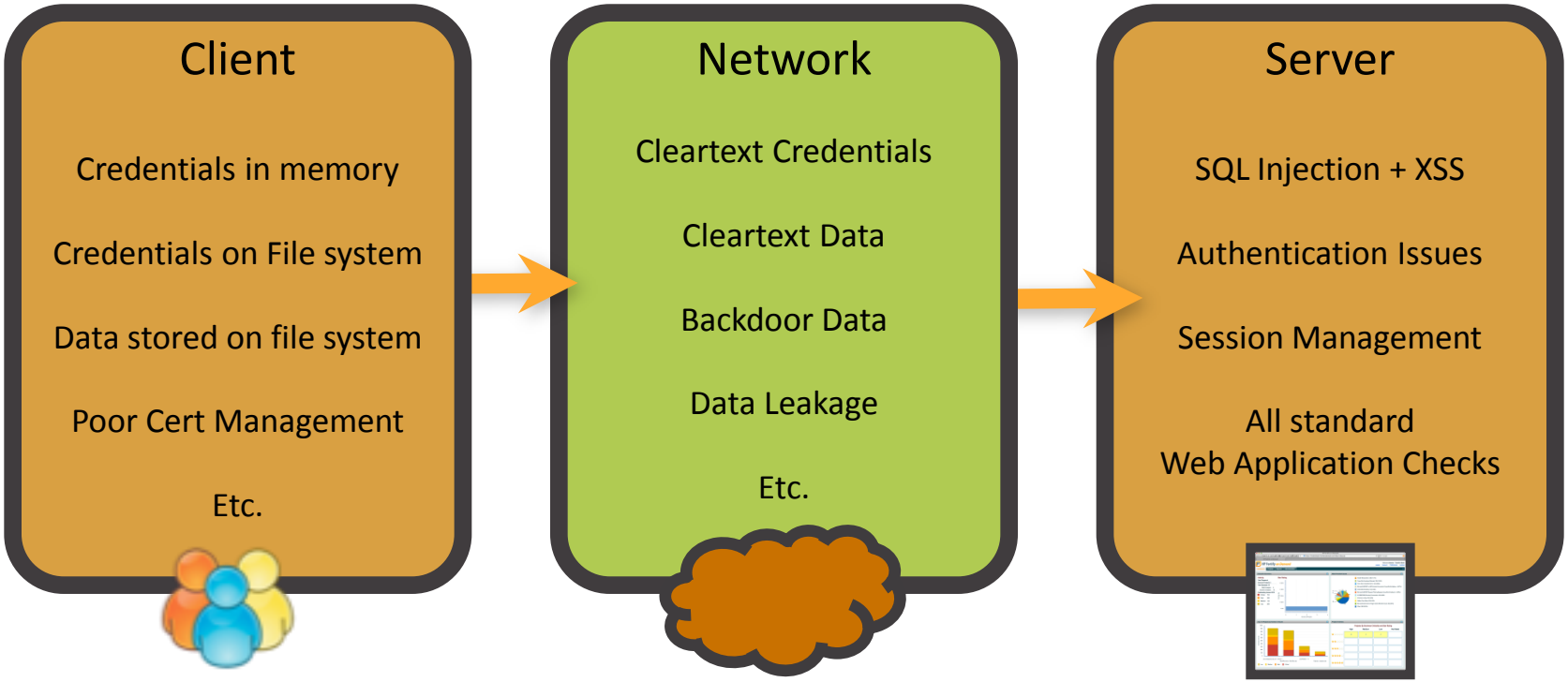
# How an attacker sees your world

# Real-world Mobile Incidents





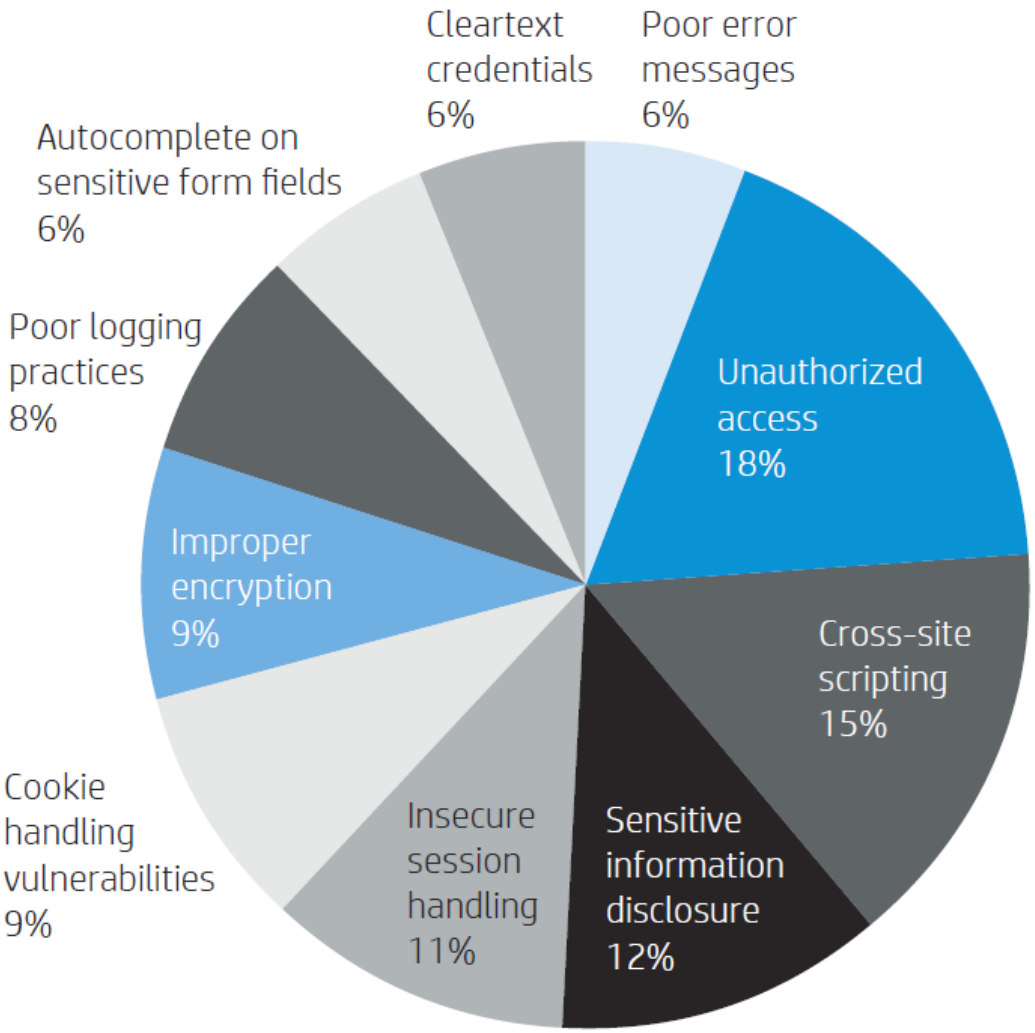
# Mobile Layers



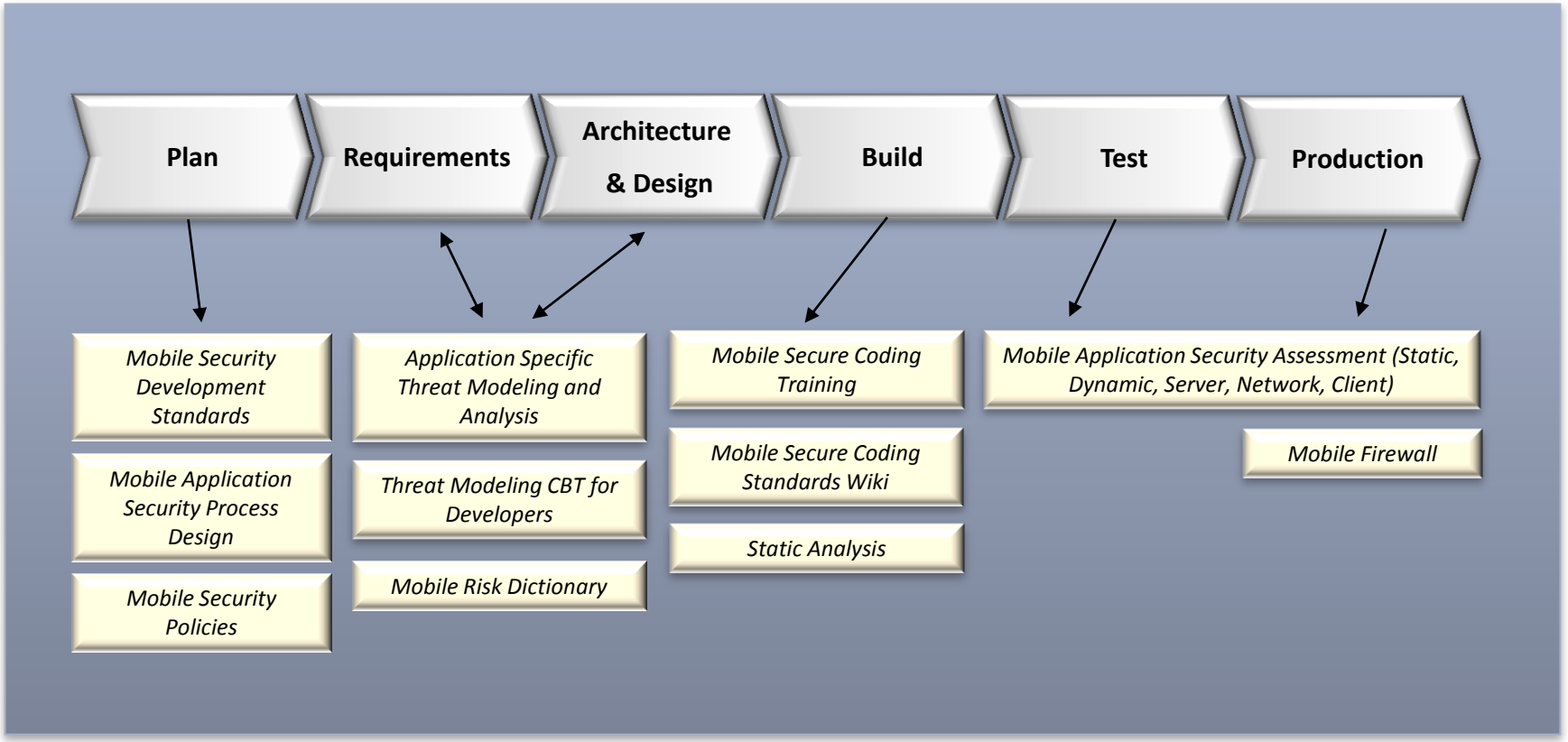
# OWASP Mobile Top 10

- M1-Insecure Data Storage
- M2-Weak Server Side Controls
- M3-Insufficient Transport Layer Protection
- M4-Client Side Injection
- M5-Poor Authorization and Authentication
- M6-Improper Sessions Handling
- M7-Security Decisions via Untrusted Inputs
- M8-Side Channel Data Leakage
- M9-Broken Cryptography
- M10-Sensitive Information Disclosure.

# Top 10 Mobile by Prevalence



# Mobile Application Fundamentals



# Questions?

Security in knowledge