Secure Mobile App Development Lifecycle

Dimitrios A. Glynos
{ dimitris *at* census-labs.com }

CENSUS S.A.

InfoCom Apps 2014 / Athens, Greece

Global investment in mobile apps

- **Marketing:** 19% of all ad spending in 2013 was spent on mobile marketing, up from 12% in 2009 (source: Forrester Research, Inc.)
- **Growth:** 102b app downloads (2013), up from 24.9b in 2011 (source: Gartner)
- **Revenue:** Worldwide app revenue of $26.6b in 2013, includes in-app sales (source: Gartner)
- **Investment:** VCs have invested $3.7b in 2013 in mobile apps (source: CB Insights)

State of security in mobile apps

Out of 40 home banking applications:

- 40% are vulnerable to MitM attacks
- 20% come with no compile-time protections (stack cookies, PIE, etc.)
- 90% do not use SSL
- 50% are vulnerable to XSS attacks
- 90% do not employ jailbreak detection
- 40% reveal sensitive information in system logs
- 30% come with hardcoded credentials in their code
- 70% are vulnerable to a variety of information leaks

Source: Ariel Sanchez, IOActive

State of security in greek apps

Home banking app of major greek bank

- No certificate pinning
- Sends exact location info to the bank's servers
- Debugging info found in the build (test servers etc.)

Popular transportation-related app

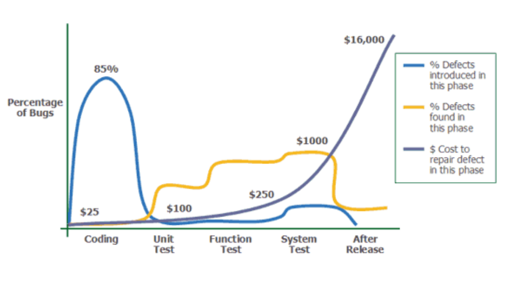
- No SSL (auth. tokens and location info sent in cleartext to web service)
- XSS vulnerability
- No obfuscation (trivially reversed to Java source)

Limited research performed in 8 hours, investigating only the (Android) app side of each service.

Handling software security bugs

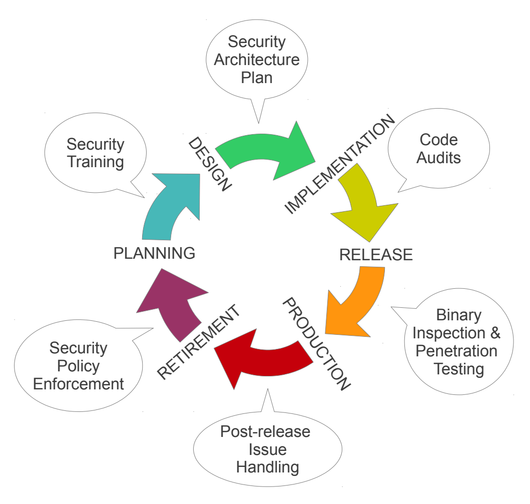
What if we were to treat software security bugs as defects introduced within the SDLC ?

Cost of a defect within the SDLC



Source: Applied Software Measurement, Capers Jones, 1996

Minimize costs - build security in!


Security Architecture Plan
Security Training
DESIGN
IMPLEMENTATION
Code Audits
PLANNING
RELEASE
Binary Inspection & Penetration Testing
PRODUCTION
RETIREMENT
Security Policy Enforcement
Post-release Issue Handling

census

Training and Consulting

Training

- Update developers and stakeholders on current threat landscape
- Train developers on finding security bugs
- Train staff on managing security risks

Consulting

- Bring in security experts to review your app's Security Architecture Plan
- Consult with experts on the handling of critical issues and procedures

Code Audits and Binary Inspection

Code Audits

- Identification of security bugs via code examination
- Frequency: per milestone / per release
- Combined with functional testing on demo setup to allow for faster identification of complex issues

Binary Inspection

- Security inspection of app bundle
- Identifies build defects such as the presence of debugging or other sensitive information
- Tests the effectiveness of obfuscation and tamper protection mechanisms

Penetration Tests

Penetration Testing

- Deployment of real attacks on both the app and its server counterpart
- Tests the effectiveness of security controls
- Documents possible attack paths leading to critical assets
- Evaluates the risk of each exploited vulnerability
- Most effective when the app and related services have been configured for production use

What can we do to help?

- We provide code auditing, binary inspection and penetration testing services for apps of all major platforms:
  - iOS
  - Android
  - Windows Phone
  - Blackberry OS / 10
- We provide vulnerability research services for new platforms & devices
- Finally, we provide consulting and training services to help you build your own Secure SDLC!

Questions?