CENSUS
IT Security Works

The Mobile Threatscape

Dimitrios Glynos
dimitris@census-labs.com

InfoCom Mobile World Conference 2015
CENSUS S.A.

www.census-labs.com

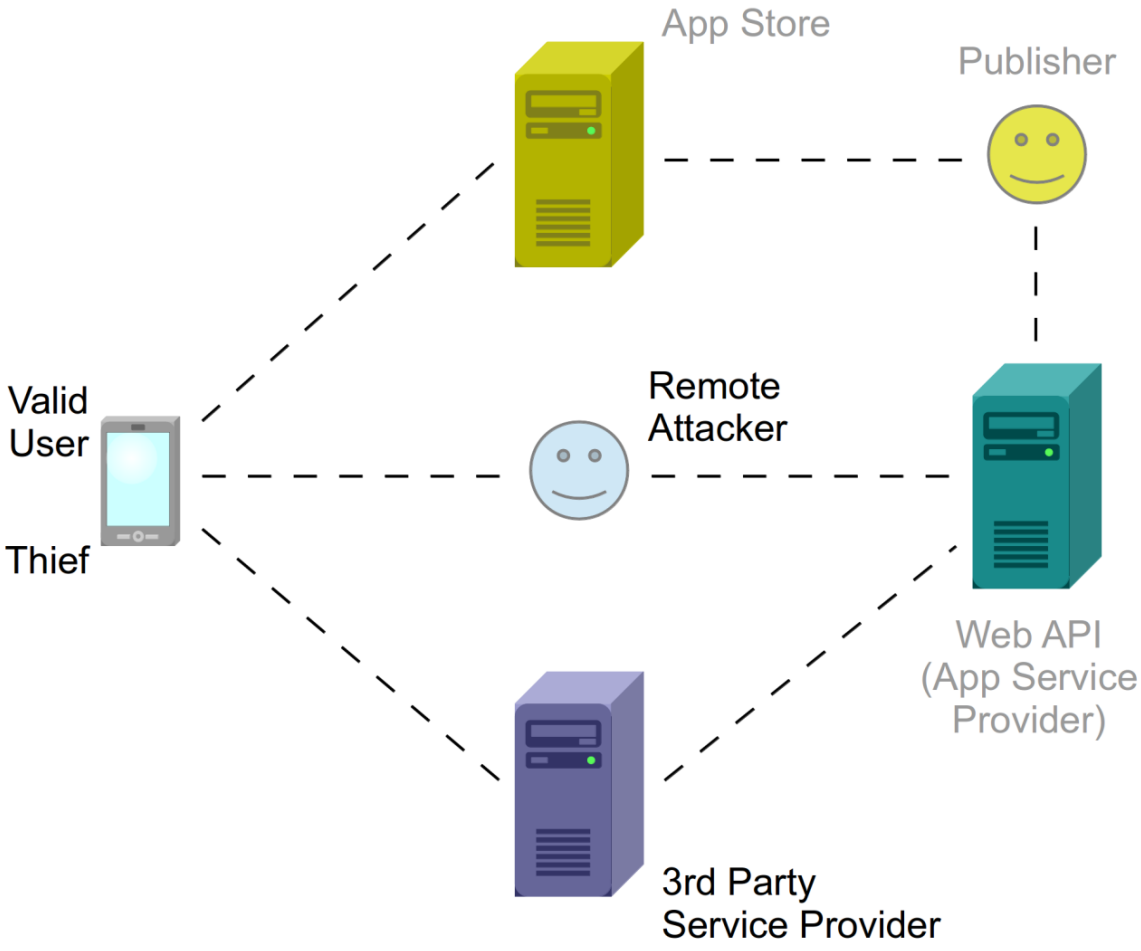
The Mobile Threatscape

An overview of the threat landscape affecting

- mobile app publishers
- mobile app (web) service providers
- users of mobile apps

…with example issues from real apps!

Key Threat Agents



Thief - Threats

- Collection of sensitive app data from device storage
  - Unencrypted storage of credentials / keys / session-IDs / private user information etc.
- Collection of sensitive data from app memory
  - Bank transaction information not wiped after end of user session.
- Impersonation attacks
  - App depends solely on device-local data to authenticate user to Web API.

Remote Attacker - Threats

- Eavesdropping
  - Transmission of credentials over shared medium (WiFi) and insecure transport (HTTP)
- Man-in-the-Middle attack
  - App accepts (malicious) payload from any server presenting a valid certificate
- Direct transmission of malicious data to device
  - NFC relay attack
- Social engineering
  - Victim is persuaded to install malware app / malicious certificate / resigned app
- Web API exploitation (unauthenticated calls)
  - User enumeration attack

3rd Party Service - Threats

- 3rd Party Service can create Denial of Service condition to app (or Web API)
- App (or Web API) leaks sensitive information to 3rd Party Service
  - User Session-ID
- 3rd Party Service may inject malicious code to app (or Web API)
  - JavaScript injection to app WebView

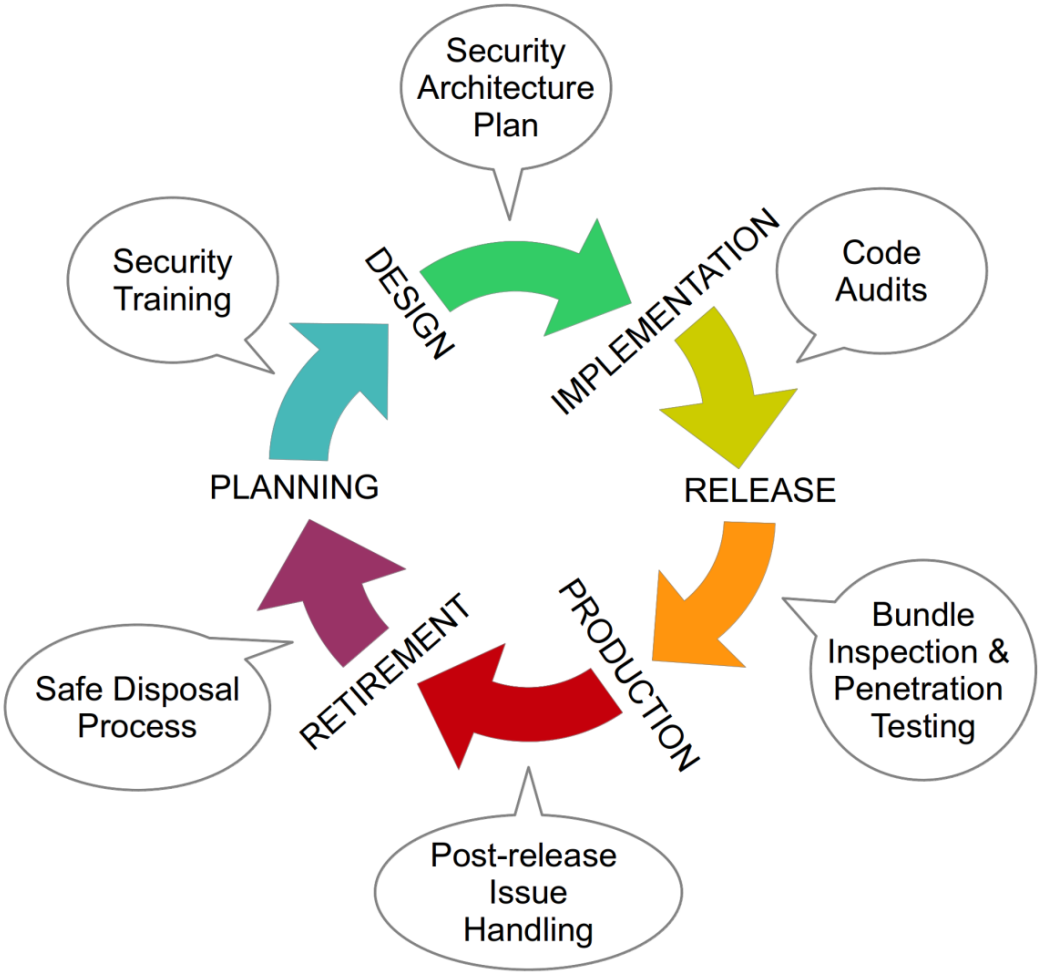
Valid User - Threats

- Users can easily modify the app logic (e.g. to disable in-app advertisements)
  - No tamper protection
- Users can easily gain access to sensitive app code / data
  - No obfuscation
- Web API exploitation (authenticated calls)
  - SQL injection, missing Access Control checks, etc.

Challenges in Handling Threats

- No time (“Traction now, security later!”)
  - Fixing a security issue after release comes with an increased cost / impact.
- No budget (“Our clients don't mind!”)
  - Quality is the definitive attribute of leaders in competitive markets.
- No expertise (“Is this really a threat?”)
  - Gain the needed insight through Security Consultancy services.

Integrating Security into the SDLC



Thank you!

CENSUS

IT Security Works