Mobile Sicherheit unter Berücksichtigung mobiler Bedingungen

Prof. Dr. Michael Waidner
Institutsleiter, Fraunhofer SIT und Direktor, CASED
Customer Requests about Smartphone Security

- How secure is iOS / Android in comparison to BlackBerry?
- How are credentials stored on iOS? Is it secure?
- We want to use MDM solution XY. How secure is it?
- Is it possible to integrate iOS securely in our existing network (e.g., VPN)?
- How secure is App XY? Does it store data securely?
- We are developing an app for iOS / Android. How secure is our concept and implementation?
The App Problem (1/2)

> 1.8 Million Apps combined

100,000 > 775,000 > 800,000 150,000
The App Problem (2/2)

- **Risks** by insecure and malicious apps
  - Devices **collect** a lot of **data**, passwords and are **connected to** corporate **identity** → Successful attacks may have significant impact

- Development and market **different to traditional software**
  - New technology; developers not familiar with **platform security design**
  - Every **platform** may have its own **specific issues**

- **Guideline standardization** is difficult

- **Examples of recent security issues**
  - Path App (address book copied to server) [1]
  - SSL protection flaws (1.000 out of 13.000 apps) [2]
  - WhatsApp (insecure communication by design) [3]

---

[2] [http://www.theregister.co.uk/2012/10/21/android_app_ssl_vulnerability/](http://www.theregister.co.uk/2012/10/21/android_app_ssl_vulnerability/)
How do Enterprises deal with App Protection?

- **Strict Whitelisters**
  - Only verified apps allowed
  - *Who verifies, what and how?*

- **Blacklisters**
  - Forbid insecure apps
  - *Where do they get blacklists from?*

- **Active Protectors**
  - Only scan for known malware
  - *Who verifies the scanner?*

- **Passive Protectors**
  - Only monitor for bad impacts
  - *How do they find malicious impacts?*

- **Those who have already surrendered**
  - The users need it, we can’t stop them
  - *Why are there no promising solutions?*

© Fraunhofer-Gesellschaft 2013
Erfahrungen aus App-Analysen

1. Fehlerhafte Prüfung der Serverauthentizität
2. Anmeldedaten mitesen bei unsicherem Verfahren
3. Mitlesen der Unternehmensdaten bei fehlender Verschlüsselung
4. Fehlende Prüfung der Daten
5. Fehlerhaftes Berechtigungsmanagement mobiles Portal
6. Unbeabsichtigte Informationspreisgabe über Systemfunktionen
7. Unzureichend geschützte Ablage von Unternehmens-Daten & Passwörtern
8. Abruf von Unternehmensdaten in Schad-App
9. Unbeabsichtigte Interaktion mit Unternehmens-App /-Server
10. Nicht autorisierter Nutzung von (Sensor-) Daten / Ressourcen
Systematic Testing of Apps
The Appicaptor Framework of Fraunhofer SIT

Concepts

- Instrumentation for security inspection / enforcement of source or byte code
  - Android:
    - Enforcement of security characteristics by byte code rewriting
    - Analysis of data flows inside apps
  - iOS:
    - Runtime instrumentation for security evaluations
    - Combined with static code analysis
- Analysis framework: Appicaptor
  - Facilitates all steps for test automation
  - Correlates results of different analysis
  - Intended for mobile app tests: iOS, Android (BlackBerry, Windows Phone added at later stage)
Appicaptor Framework

- Framework accumulates workflow and analysis tools for automated and manual app security evaluation
  - Scans for known **malware patterns** and **weak implementations** of security functionality
  - Smartphone **Platform agnostic** and correlates platform results
  - Based on **knowhow** of manual testing and integrates **conceptual research** of CASED
  - Workbench visualizes **interpreted results** and **entry points** for manual investigations
Appicaptor Framework – Analysis workflow

Data Extraction
- App-Bundle
- Binaries
- Metadata

Reversing
- Decrypt
- Decompile
- Disassemble
- Parse, Run ...

Analysis of
- Source code
- Disassembly
- Metadata
- Behavior

Analysis and correlation of
- Raw data
- Indicators

Analysis of
- List of Indicators
- Raw analysis data

Focused Manual Analysis
- Identified relevant Entry Points

Investigation required
- No automated Findings
- Direct Findings

Rating and Documentation
- Focused Manual Analysis

Manual Findings
- Privacy & Security Implications

No Findings
- No automated Findings

No Findings
- Visualization
- Interaction

Fraunhofer SIT

© Fraunhofer-Gesellschaft 2013
Appicaptor Beta Test Phase

- **Current state of development**
  - Sound framework for static and dynamic code analysis (Android / iOS)
  - **Test cases for security relevant platform functionality** available
  - **Redundant result generation** to identify false assumptions
  - **Applying function models** for rating of results (current research project)

- **General assumptions for beta phase**
  - **No obfuscation** of security features or countermeasures to prevent code analysis (standard methods already partly detectable, but not circumvented)
Example: Missing Protection of Stored Data

- iOS functionality to keep files encrypted in storage
- Incorporates passcode as user secret for encryption + bruteforce protection
- Protection for lost/stolen devices
- Rarely used by system apps

Result of control sample
- Also rarely used in analyzed 3rd party apps
- Of 8 apps with office file support, only 2 use data protection

Appicaptor Analysis, German App Store, 8.5.2013
Example: Unexpected Functionality

Ad-/Tracking Frameworks
Top 100 Free Utilities

Number of Frameworks per App

- None: 33%
- 1:15%
- 2:13%
- 3:14%
- 4:10%
- 5-12:15%

Appicaptor Analysis, German App Store, 8.5.2013
Appicaptor Test Process

- **Selection** of apps and test cases
- **Execution** of tests: approx. 5-10 min per app including download, decryption, static analysis, and runtime analysis
- **Process result**
  - Client report or information for manual investigations / findings for evaluators
Planned Services

- Subscription **App Select Analysis** (pre-paid service)
  - Configurable list of apps and test cases
  - Results periodically issued (depending on app update cycle and customer needs)
  - Selectable result format for integration in corporate processes (PDF, XLS, ...)
  - Upper limit of reviewed apps per year pre-paid;
    - Flex Subscription: if limit exceeded → post-paid

- Subscription **App Report Blacklist/Whitelist** (pre-paid service)
  - Regular updated reports with rated apps as black/white
  - Configurable / predefined policies for rating
  - **Premium Subscription**: Results directly integratable with MDM (depends on MDM Solution)
Security Assurance Within Enterprise App Development

- **Generation of tools** ensuring the **security quality of mobile services and apps**
  - **Security Evaluation Tool**
    - **Threat assessment, risk analysis** and **security requirements check** for customer generated Enterprise Apps **within SAP mobile development environments** (e.g., Sybase Unwired Platform) based on Appicaptor Framework
  - **Knowledge Transfer Tool**
    - **Security best practice guide** for mobile development environments based on results of Security Evaluation Tool for **native, hybrid und Web-based apps**
    - Description of **technical potential** for **SAP Apps and frameworks** to increase security on iOS, Android, BlackBerry and Windows Phone devices
Prof. Dr. Michael Waidner
michael.waidner@sit.fraunhofer.de

Fraunhofer-Institut für
Sichere Informationstechnologie (SIT)
Institutsleiter
Rheinstraße 75
64295 Darmstadt
www.sit.fraunhofer.de

Technische Universität Darmstadt
Fachbereich Informatik,
Lehrstuhl Sicherheit in der IT (SIT)
Direktor CASED und EC SPRIDE
Mornewegstraße 30
64289 Darmstadt
www.sit.tu-darmstadt.de