TUM Seminar
WS 2012/2013
Mobile Systems Security
http://goo.gl/8l8NS

Philipp Stephanow
Julian Schütte
Gerd Brost
Purpose of this seminar

- Understand current challenges and research approaches in the security of mobile systems (speak: smartphones)
- Learn what current interests in industry and research in this topic are
- Address a question systematically and in a scientific way
1. Motivation letter („abstract“) 29th July 2012
   - What motivates you to participate?
   - Name three scientific publications corresponding to your topic
   - State the research questions you think are most relevant to your topic

2. Paper (Seminararbeit) 6th January 2013
   - max. 10 pages in IEEE format (LaTeX)
   - Two Peer-Reviews

3. Presentation
   - 6.2., 7.2., 8.2.2013 (planned)
   - Each presentation: 20 min plus 10 min Q&A
<table>
<thead>
<tr>
<th>Description</th>
<th>Dates</th>
<th>Visibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper Submission Deadline</td>
<td>2013-01-06</td>
<td>public</td>
</tr>
<tr>
<td>Peer Review</td>
<td>2013-01-07 - 2013-01-20</td>
<td>authors</td>
</tr>
<tr>
<td>Seminar</td>
<td>2013-02-06 - 2013-02-08</td>
<td>public</td>
</tr>
</tbody>
</table>
Evaluation

- Motivation letter (abstract): 0 % (required)
- Paper: 60 %
- Presentation: 30 %
- Reviews: 10%

- What counts:
  - Content: Comprehensive, most relevant aspects comprised
  - Systematic preparation
  - Autonomous way of working
  - Quality of results’ presentation

- Opinions displayed in peer reviews are not subject to grading of reviewed work
Strategy Development for Secure Deployment of Mobile Device in Corporate Environments

- Elicit security requirements for mobile platforms, e.g. smartphones and tablets (specify target state on a technical level)
  - Factor in attributes of different environment (e.g. SME, assets etc.)
  - specify corresponding technologies to fit these requirements

- Develop an approach to elicit the current state of Mobile Devices’ secure deployment (e.g. architecture-driven)

- (Apply approach to Fraunhofer AISEC)
Remote Device Management

- Review technical approaches (APIs, protocols) of current solutions for current OS
  - Specification review of different mobile OS
  - Comparison of remote management capabilities

- How can remote management be circumvented?
  - by users, by attackers
  - Is it possible to bind a device so that operation is only possible with running device management?

- Develop ideal set of remote management capabilities
  - Consider usability issues arising through rigorous device management
Mobile Device Business Apps

- What solutions (products) exist?
  - Example: Good App for Android, iOS, …
  - Features (Remote Wipe of App data, …)?

- Limitations and practicability of available apps

- Security model of the solution
Known attacks on mobile platforms and their economic incentives (technical analysis)

- Review existing exploits and attack vectors on mobile apps and webapps
- What are the business models of attackers?
- Create a map of attack vectors and criminal business model
Security models and potential future threats of web applications on mobile platforms

- Supported web technologies and limitations of mobile browser engines (WebKit, …)
- Known attack vectors in HTML5 and their relevance to mobile platforms
- Security models and potential threats of web-based apps
Firefox OS (a.k.a. Boot2Gecko) security

- Review of the Firefox OS including comparison with the Mozilla Application Framework (MAF)

- Review of the underlying security model in all three layers
  - Gonk – HAL
  - Gecko – Layout engine
  - Gaia – User interface

- Discussion of potential attack vectors in each layer
Spyware and Android

- Review of current functionality and spreading techniques

- Review and classification of available spyware and their hooks into the operating system
  - StealthGenie
  - CarrierIQ
  - MobiStealth

- Development and discussion of possible countermeasures
  - in particular without manipulating the device
Context awareness in mobile devices

- How should a mobile platform look like to gather proven context information?

- How could context information be used to amend existing authentication and authorisation (AA) mechanisms (e.g. Location, presence of external tokens (NFC), usage patterns) → identify use cases

- How can data security be bound to these contexts?
Mobile Identity: How to use a mobile device as an identification token

- Review existing mobile signature solutions (e.g. in Finland, Sweden, Turkey etc.)
- What are novel ways to manage identities on a mobile device?
- How can pseudonymic but still trustworthy identities be realized? What kind of apps and what app storage is suitable? Phone? Secure Element? UICC?
Privacy and mobile Devices

- Analyze which data is transmitted on Smartphones and what can be done with it
- What part of the data is encrypted, what unencrypted?
- Create a simple model of information channels from and to the device (GSM, UMTS, NFC, …)
- Android event log, iOS locations, etc.
Security models of mobile platforms

- Investigate security mechanisms currently deployed on mobile devices
  Android (Dalvik vs. NDK), iOS, MeeGo/Tizen, B2G, ...

- Compare with respect to
  - permission model,
  - application sandboxing,
  - user and rights management,
  - remote control possibilities,
  - application distribution and deployment,
  - update cycles
  - ...
Discussion of isolation approaches on the Android platform and their usefulness for practical application in BYOD scenarios

- Review and compare concepts
  - full virtualisation
  - linux containers (LXC)
  - Microkernels (L4Android)
  - App containers
  - ...

- Create a criteria catalogue for practicability of such approaches for isolating business data from personal data on the phone in a BYOD setting
Topics
[list of topics: http://goo.gl/8I8NS]

Approaches on data usage control for mobile platforms

- Review mechanisms to control data usage on mobile phones and to track illegitimate or unwanted usage
  "Where is my data?"
- Discuss available solutions vs. research approaches

- Discuss possibilities of
  - policy specification
    (c.f. OSL, Android DeviceAdmin, Exchange Active Sync policies)
  - enforcement mechanisms
    (c.f. taintdroid, etc.)
Common development flaws and secure coding guidelines for mobile apps

- Review Android’s security mechanisms at Dalvik and NDK layer and derive potential consequences of bad programming
- Create a catalogue of best practices
- Make suggestions how applications could be checked for these best practices -- in a whitebox and a blackbox scenario
Static analysis of Android apps

- Review the state of the art on methods for static analysis to uncover security flaws - in code and in binaries

- Research which of these methods are available for Android (if any, already)

- Sketch the most promising ways to port existing tools for other formats to Android/Dalvik (cf. Scandroid, dexpler/soot, Wala, etc.)
Trust anchors for mobile devices

- Review and compare different hardware security anchors in mobile devices (TPM, MTM, SEs (GlobalPlatform), TEEs)
  - Features, Security model
  - Availability and prerequisites
- Discuss which types of applications would profit from the different solutions (Mobile Payment, VPN, S/MIME)
- Discuss questions of practical applicability (complexity, available devices, etc.)
Vorgehen bei Themenauswahl

- Excel liste
  - Angabe der Präferenzen (1, 2, 3)
AISEC: Mit Sicherheit innovativ!

AISEC Kompetenzen

- Eingebettete Systeme
- Smartcard & RFID Sicherheit
- Produktschutz
- Cloud & Service Sicherheit
- Netzwerksicherheit
- Automotive Sicherheit
- IT Frühwarnung
- Smart Grid & CPS
- Sicherheits-Evaluation
Offene Stellen am Fraunhofer AISEC

- Studentische Hilfskräfte
  - [http://www.sec.in.tum.de/jobs/](http://www.sec.in.tum.de/jobs/)

- Bachelor- und Masterarbeitsthemen
  - [http://www.sec.in.tum.de/student-work/](http://www.sec.in.tum.de/student-work/)

- Wissenschaftliche Mitarbeiter für Forschungsbereiche:
  - »Embedded Security and Trusted OS«
  - »Netzsicherheit und Frühwarnsysteme«
  - [http://www.aisec.fraunhofer.de/de/jobs.html](http://www.aisec.fraunhofer.de/de/jobs.html)