Kick-off: Mobile Application Security

Chair for IT Security / I20
Prof. Dr. Claudia Eckert
Technical University of Munich

Dr. Julian Schuette
julian.schuette@aisec.fraunhofer.de

Dennis Titze
dennis.titze@aisec.fraunhofer.de

Christof Ferreira Torres
christof.torres@aisec.fraunhofer.de

January 30, 2018

Outline

Requirements

The seminar will be organized as a scientific conference. You will present your research in written and in a presentation to your peers.

- Report Elaboration
  - Delivery of a scientific paper with 10-12 pages in length
  - We will provide a Latex template
- Review
  - Each one of you creates two anonymous reviews
  - Review template will be provided
  - Approximately one page in Latex
- Presentation
  - Preparing of the presentation
  - 30-45 minutes presentation
  - 15 minutes discussion

Grading

The Grading is composed of:

1. Report (50%)
2. Presentation (30%)
3. Delivered reviews (20%)

(Active) Participation at the meetings is expected.

Time Table

30.01.18	[Today] Topic Presentations
21.02.18	Start of topic assignments
16.04.18	Submit your outline + preliminary draft
20.04.18	Meeting: Intermediate review and discussion
27.05.18	Submit your pre-final version
28.05.18	Receive papers to review
06.06.18	Submit your reviews
07.06.18	Receive your reviews
18.06.18	Submit your rebuttal + camera-ready-version + presentation
21+22.06.18	Meeting: Presentations and discussion

Topics

- Automated Dynamic Testing
- (Dynamic) Binary App Instrumentation
- How not to keep a secret
- Dynamic Taint Analysis
- Mobile Device Fingerprinting
- Securitymodel Android vs. iOS
- iOS Sandbox Security
- Root Detection
- SE-Linux
- UI-Attacks
- Anti-Analysis

Automated Dynamic Testing

- What are the challenges with dynamic testing?
- Approaches of automated dynamic vulnerability finding
- Assess & classify approaches

- Initial literature
  - "PUMA: Programmable UI-Automation for Large-Scale Dynamic Analysis of Mobile Apps"
  - "Brahmastra: Driving Apps to Test the Security of Third-Party Components" (Bhoraskar)
  - "Harvesting Runtime Data in Android Applications for Identifying Malware and Enhancing Code Analysis" (Rasthofer et al.)
  - "All You Ever Wanted to Know about Dynamic Taint Analysis and Forward Symbolic Execution (but Might Have Been Afraid to Ask)" (Schwarz et al.)
  - "Automated Concolic Testing of Smartphone Apps" (Anand et al.)

(Dynamic) Binary App Instrumentation

- What is DBI, comparison to debugging?
- Hooking techniques: Dex-rewriting vs. `LD_PRELOAD`, `DYLD_INSERT_LIBRARIES`
- Discussion of the approaches of different DBI-tools in the context of iOS/Android (Frida, DynamoRIO, Pin, ...)
- Ways to defeat/detect DBI

- Initial literature
  - Idea: Callee-Site Rewriting of Sealed System Libraries (Styp-Rekowsky et al.)
  - DroidScope: Seamlessly Reconstructing the OS and Dalvik Semantic Views for Dynamic Android Malware Analysis (Yan et al.)
  - Documentation of tools: Intel PIN, Frida, DynamoRIO, etc.

How (not) to keep a secret

- Sketch typical scenarios where apps must keep a secret
- What could possibly go wrong?
- Research the ways how to keep a secret in an Android app
- Think about attack vectors that are still available

- Initial literature
  - "Breaking into the vault: Privacy, security and forensic analysis of Android vault applications"
  - "Analysis of Secure Key Storage Solutions on Android" (Cooijmans et al.)
  - "Exploiting Trustzone on Android" (BlackHat Writeup by @returnsme)
  - Android documentation on Keystore, KeyChain
  - Further literature on (attacks on) Trusted Execution Environments

Dynamic Taint Analysis

- How does DTA work and what is it good for?
- Platform-level vs. application-level DTA
- Challenges in getting DTA right
- Propose ways to break DTA

- Initial literature
  - "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones" (Enck et al.)
  - "TaintART: A Practical Multi-level Information-Flow Tracking System for Android RunTime." (You et al.)
  - "Practical Application-Level Dynamic Taint Analysis of Android Apps" (Schütte et al.)
  - "All You Ever Wanted to Know about Dynamic Taint Analysis and Forward Symbolic Execution (but Might Have Been Afraid to Ask)" (Schwarz et al.)

Mobile Device Fingerprinting

- How does mobile device fingerprinting work?
- What are the different techniques?
- What is the difference between browser fingerprinting and mobile device fingerprinting?
- Are there any countermeasures towards mobile device fingerprinting?

- Initial literature
  - "Efficient Fingerprinting-Based Android Device Identification With Zero-Permission Identifiers." (Wenjia Wu)
  - "Fingerprinting Mobile Devices Using Personalized Configurations." (Andreas Kurtz)
  - "How unique is your web browser?" (Peter Eckersley)
  - "FP-Block: usable web privacy by controlling browser fingerprinting." (Christof Torres)

Securitymodel Android vs. iOS

- What are essential security meachanisms?
- How are they similar?
- How are they different?

- Initial literature
  - “Understanding Android Security” (William Enck)
  - “iOS Security Guide” (Apple)
  - “Android vs. iOS: The security battle” (Fattoh Al-Qershi)
  - “Android vs iOS Security: A Comparative Study” (Ibtisam Mohamed)

iOS Sandbox Security

- How does the sandbox work on iOS?
- Which vulnerabilities and shortcomings exist?

- Initial literature
  - “iOS Security Guide” (Apple)
  - “SandScout: Automatic Detection of Flaws in iOS Sandbox Profiles” (Luke Deshotels)
  - “The Apple Sandbox” (Dionysus Blazakis)
  - “XiOS: Extended Application Sandboxing on iOS” (Mihai Bucicoiu)

Root Detection

- Which capabilities do users get when rooting phones?
- Why is it a security problem?
- What is the difference between a root-exploit and Rooting your phone?
- How can you/an app/the system detect that the phone is rooted?

- Initial literature
  - “Methods for avoiding rooting in Android System” (Haofei Yan)
  - “The Dangers of Rooting: Data Leakage Detection in Android Applications” (Luca Casati)
  - “Android Rooting: An Arms Race between Evasion and Detection” (Long Nguyen-Vu)
  - “PREC: Practical Root Exploit Containment for Android Devices” (Tsung-Hsuan Ho)

SE-Linux

- What is SE-Linux?
- Why is it useful for Android/Android apps?
- What are its limitations?

- Initial literature
  - “Analysis of SEAndroid Policies: Combining MAC and DAC in Android” (Haining Chen)
  - “Security Enhanced (SE) Android: Bringing Flexible MAC to Android” (Stephen Smalley)
  - “Securing Android Powered Mobile devices using SELinux” (Asaf Shabtai)
  - “Securities in Android using SELinux” (S. S. Sambare)

UI-Attacks

- Which attacks have been published on the UI of apps?
- Why is it interesting for an attacker to gain knowledge of the UI?
- How can apps (or the OS) protect against such attacks?

- Initial literature
  - “Ui redressing attacks on android devices” (M Niemietz)
  - “UiRef: Analysis of Sensitive User Inputs in Android Applications” (Benjamin Andow)
  - “Android UI Deception Revisited: Attacks and Defenses” (Earlence Fernandes)
  - “Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop” (Yanick Fratantonio)

Anti-Analysis

- How can apps hide their behavior from dynamic analysis?
- For which analysis techniques is this a problem?
- How can analysis techniques circumvent this?
- Initial literature
  - "Droid-AntiRM: Taming Control Flow Anti-analysis to Support Automated Dynamic Analysis of Android Malware" (Xiaolei Wang)
  - "Triggerscope: Towards detecting logic bombs in android applications" (Yanick Fratantonio)
  - "Harvesting Runtime Values in Android Applications That Feature Anti-Analysis Techniques." (Siegfried Rasthofer)
  - "Rage against the virtual machine: hindering dynamic analysis of android malware" (Thanasis Petsas)

Getting Started

- Objective: Get a comprehensive overview of the topic
  - Initial literature serves as a basis
  - Extension will be necessary
  - Check Sources, follow-up work, and related publications
  - Prioritize, classify, be critical
  - Keep in touch with your supervisor
- Make an outline
  - State your research question
  - Condense & review state of the art
  - Bring in your contribution
  - Provide an outlook to your fellow researchers
- Further info on writing & preparing talks will follow

Q&A ?