IAIK | Institute of Applied Information Processing and Communications

Code Coverage Measurement for Black-box Testing of Unmodified Android Apps

Advisor: **Florian Draschbacher**

Motivation

In black-box testing, compiled applications are executed in an automated testbed to observe their runtime behavior. This analysis technique is commonly used for identifying vulnerabilities or malicious activities of application samples that are only available in binary form and/or heavily obfuscated. For being able to derive well-founded findings from black-box testing, it is crucial for the automated testbed to exercise as much of the application's functionality as possible. However, there currently is no reliable way for measuring fine-grained code coverage in black-box testing scenarios of Android applications. Existing tools do not support recent APK formats and require the application under test to be repackaged. This requirement is detrimental to application compatibility, since repackaging is known to cause functionality degradation in almost any modern Android application due to app-restricted (Google) API keys or runtime integrity checks.

As part of this project, your goal is to design and implement a method for measuring fine-grained code coverage for black-box testing of unmodified Android apps. Your solution will utilise root privileges to avoid the need for repackaging. A sensible approach would involve manipulating the Dalvik executable (DEX) files on-device before they are ahead-of-time compiled. For working around issues with register rearrangement faced by previous solutions, a parameter-less tracing method may be used that collects caller information from the stack trace.

Goals and Tasks

- Get familiar with related literature and suitable instrumentation options
- Design and implement code coverage measurement using system-side instrumentation
- Evaluate the compatibility and accuracy of your solution
- Write down your findings

Literature

- A. Pilgun et al.
  Fine-grained Code Coverage Measurement in Automated Black-box Android Testing
  ACM Trans. Softw. Eng. Methodol. 2020
- M. Backes et al.
  ARTist: The Android Runtime Instrumentation and Security Toolkit
  EuroS&P

Courses & Deliverables

☑ **Introduction to Scientific Working**
Short report on background
Short presentation

☑ **Bachelor Project**
Project code and documentation

☑ **Bachelor's Thesis**
Project code
Thesis
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest and some experience in mobile security
- Programming skills (Java, C/C++)

Advisor Contact

florian.draschbacher@iaik.tugraz.at