Comprehensive Bytecode Instrumentation for Dynamic Program Analysis on Android

Android is a dominant Java-based application platform for mobile devices, built around a virtual machine (Dalvik VM) that executes alternative, register-based bytecode. Designed as the final deployment platform with resource-constrained devices in mind, the Dalvik VM lacks debugging and instrumentation interfaces that Java developers have come to rely upon. This hinders both development and usage of instrumentation-based dynamic program analyses underlying many programming tools, forcing developers to instrument applications offline prior to deployment, and resulting in potentially unsound analyses due to inability to instrument dynamically loaded code. In this demonstration, we present our framework for dynamic program analysis development on Android, offering a high-level programming interface and full bytecode coverage. It is based on the existing ShadowVM framework for Java, which provides load-time bytecode instrumentation and isolates the analysis logic from the observed program by processing the analysis data on-the-fly in an analysis server. Our framework makes these benefits available to Android developers, thus simplifying dynamic program analysis on Android. We will demonstrate our system with an Android-specific network traffic analysis, deployed on both an ARM/Intel-based emulator and a real device.

Author: Walter Binder (walter.binder@usi.ch)