

Comprehensive Multi-Platform Dynamic Program Analysis for the Java and Dalvik Virtual Machine

Despite its importance for many software engineering tasks, dynamic program analysis is only insufficiently supported on the Java platform. Existing Java Virtual Machines (JVMs) as well as Android's Dalvik Virtual Machine (DVM) lack dedicated mechanisms for expressing arbitrary dynamic program analysis tasks at a high abstraction level, for ensuring complete code coverage of the analysis, and for isolating analysis tasks from the observed program to prevent interference. For example, the JVM Tool Interface requires analysis tasks to be written in low-level native code, and some virtual machines (e.g., DVM) do not support it. As a consequence, dynamic program analysis tools are often implemented using low-level mechanisms, resulting in error-prone code that is difficult to maintain, and support only a particular virtual machine. Moreover, many analysis tools produce unsound profiles (due to interference of the analysis with the observed program) or incomplete profiles (due to limited code coverage).

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