A Programming Model and Framework for Comprehensive Dynamic Analysis on Android

The multi-process architecture of Android applications combined with the lack of suitable APIs make dynamic program analysis (DPA) on Android challenging and unduly difficult. Existing analysis tools and frameworks are tailored mainly to the needs of security-related analyses and are not flexible enough to support the development of generic DPA tools. We present a framework that, besides providing the fundamental support for the development of DPA tools for Android, enables development of cross-platform analyses that can be applied to applications targeting the Android and Java platforms. The framework provides a convenient high-level programming model, flexible instrumentation support, and strong isolation of the base program from the analysis. To boost developer productivity, the framework retains Java as the main development language, while seamless integration with the platform overcomes the recurring obstacles hindering development of DPA tools for Android. We evaluate the framework on two diverse case studies, demonstrating key concepts, the flexibility of the framework, and analysis portability.

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