## 1. DroidRA: Taming reflection to support whole-program analysis of android apps (*Open Access*)

Li, Li (1); Bissyandé, Tegawendé F. (1); Octeau, Damien (2); Klein, Jacques (1)
**Source:** *ISSTA 2016 - Proceedings of the 25th International Symposium on Software Testing and Analysis*, p 318-329, July 18, 2016, *ISSTA 2016 - Proceedings of the 25th International Symposium on Software Testing and Analysis*;
**ISBN-13:** 9781450343909; **DOI:** 10.1145/2931037.2931044; **Conference:** 25th International Symposium on Software Testing and Analysis, ISSTA 2016, July 18, 2016 - July 20, 2016; **Sponsor:** Special Interest Group on Software Engineering (ACM SIGSOFT); **Publisher:** Association for Computing Machinery
**Author affiliation:** (1) SnT, University of Luxembourg, Luxembourg (2) CSE, Pennsylvania State University, United States
**Abstract:** Android developers heavily use reflection in their apps for legitimate reasons, but also significantly for hiding malicious actions. Unfortunately, current state-of-the-art static analysis tools for Android are challenged by the presence of reflective calls which they usually ignore. Thus, the results of their security analysis, e.g., for private data leaks, are inconsistent given the measures taken by malware writers to elude static detection. We propose the DroidRA instrumentation-based approach to address this issue in a non-invasive way. With DroidRA, we reduce the resolution of reflective calls to a composite constant propagation problem. We leverage the COAL solver to infer the values of reflection targets and app, and we eventually instrument this app to include the corresponding traditional Java call for each reflective call. Our approach allows to boost an app so that it can be immediately analyzable, including by such static analyzers that were not reflection-aware. We evaluate DroidRA on benchmark apps as well as on real-world apps, and demonstrate that it can allow state-of-the-art tools to provide more sound and complete analysis results.
 (51 refs)
**Main heading:** Mobile security
**Controlled terms:** Android (operating system) - Data privacy - Malware - Reflection - Software testing - Static analysis
**Uncontrolled terms:** Android - Constant propagation - DroidRA - Security analysis - Sound and complete - Static analyzers - Static detections - Whole-program analysis
**Classification Code:** 723 Computer Software, Data Handling and Applications
**Open Access type(s):** All Open Access, Green
**Database:** Compendex
**Data Provider:** Engineering Village