1. Taming Reflection: An Essential Step Toward Whole-program Analysis of Android Apps

Xiaoyu Sun (1); Li Li (1); Bissyandé, T.F. (1); Klein, J. (1); Octeau, D. (1); Grundy, J. (1)

Source: *ACM Transactions on Software Engineering and Methodology*, v 30, n 3, p 32 (36 pp.), May 2021; **ISSN:** 1049-331X; **DOI:** 10.1145/3440033; **Publisher:** ACM, USA

Author affiliation: (1) Monash University, Clayton, VIC, Australia

Abstract: Android developers heavily use reflection in their apps for legitimate reasons. However, reflection is also significantly used 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 incomplete, given the measures taken by malware writers to elude static detection. We propose a new instrumentation-based approach to address this issue in a non-invasive way. Specifically, we introduce to the community a prototype tool called DroidRA, which reduces the resolution of reflective calls to a composite constant propagation problem and then leverages the COAL solver to infer the values of reflection targets. After that, it automatically instruments the app to replace reflective calls with their corresponding Java calls in a traditional paradigm. Our approach augments an app so that it can be more effectively statically analyzable, including by such static analyzers that are not reflection-aware. We evaluate DroidRA on benchmark apps as well as on real-world apps, and we demonstrate that it can indeed infer the target values of reflective calls and subsequently allow state-of-the-art tools to provide more sound and complete analysis results. (0 refs)

Inspec controlled terms: Android (operating system) - invasive software - Java - mobile computing - program diagnostics - security of data - smart phones
Uncontrolled terms: taming reflection - essential step toward whole-program analysis - Android apps - Android developers - current state-of-the-art static analysis tools - reflective calls - reflection targets - reflection-aware - state-of-the-art tools - complete analysis results
Classification Code: C6130S Data security - C6150G Diagnostic, testing, debugging and evaluating systems - C6190V Mobile, ubiquitous and pervasive computing
IPC Code: G06F9/44 - G06F9/46 - G06F11/36 - G06F21/00 - H04M1/725
Treatment: Practical (PRA)
Database: Inspec
Data Provider: Engineering Village