A Qualitative Analysis of Android Taint-Analysis Results

Submitted by aekwall on Mon, 01/27/2020 - 10:27am

Title	A Qualitative Analysis of Android Taint-Analysis Results
Publication Type	Conference Paper
Year of Publication	2019
Authors	Luo, Linghui, Bodden, Eric, Späth, Johannes
Conference Name	2019 34th IEEE/ACM International Conference on Automated Software Engineering (ASE)
Keywords	android, composability, Metrics, path conditions, pubcrawl, taint analysis
Abstract	In the past, researchers have developed a number of popular taint-analysis approaches, particularly in the context of Android applications. Numerous studies have shown that automated code analyses are adopted by developers only if they yield a good "signal to noise ratio", i.e., high precision. Many previous studies have reported analysis precision quantitatively, but this gives little insight into what can and should be done to increase precision further. To guide future research on increasing precision, we present a comprehensive study that evaluates static Android taint-analysis results on a qualitative level. To unravel the exact nature of taint flows, we have designed COVA, an analysis tool to compute partial path constraints that inform about the circumstances under which taint flows may actually occur in practice. We have conducted a qualitative study on the taint flows reported by FlowDroid in 1,022 real-world Android applications. Our results reveal several key findings: Many taint flows occur only under specific conditions, e.g., environment settings, user interaction, I/O. Taint analyses should consider the application context to discern such situations. COVA shows that few taint flows are guarded by multiple different kinds of conditions simultaneously, so tools that seek to confirm true positives dynamically can concentrate on one kind at a time, e.g., only simulating user interactions. Lastly, many false positives arise due to a too liberal source/sink configuration. Taint analyses must be more carefully configured, and their configuration could benefit from better tool assistance.
DOI	10.1109/ASE.2019.00020
Citation Key	luo_qualitative_2019

pubcrawl composability Metrics taint analysis android path conditions