World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:14, No:11, 2020

Improving Taint Analysis of Android Applications Using Finite State Machines

Authors : Assad Maalouf, Lunjin Lu, James Lynott

Abstract : We present a taint analysis that can automatically detect when string operations result in a string that is free of taints, where all the tainted patterns have been removed. This is an improvement on the conservative behavior of previous taint analyzers, where a string operation on a tainted string always leads to a tainted string unless the operation is manually marked as a sanitizer. The taint analysis is built on top of a string analysis that uses finite state automata to approximate the sets of values that string variables can take during the execution of a program. The proposed approach has been implemented as an extension of FlowDroid and experimental results show that the resulting taint analyzer is much more precise than the original FlowDroid.

Keywords : android, static analysis, string analysis, taint analysis
Conference Title : ICMDSP 2020 : International Conference on Mobile Device Security and Privacy
Conference Location : Rome, Italy
Conference Dates : November 11-12, 2020