Side Channel Analysis Using a Model Counting Constraint Solver and Symbolic Execution

Tevfik Bultan

Dept. of Computer Science, University of California, Santa Barbara, CA, USA
bultan@cs.ucsb.edu

Abstract

A crucial problem in software security is the detection of side-channels [5, 2, 7]. Information gained by observing non-functional properties of program executions (such as execution time or memory usage) can enable attackers to infer secret information (such as a password). In this talk, I will discuss how symbolic execution, combined with a model counting constraint solver, can be used for quantifying side-channel leakage in Java programs. In addition to computing information leakage for a single run of a program, I will also discuss computation of information leakage for multiple runs for a type of side channels called segmented oracles [3]. In segmented oracles, the attacker is able to explore each segment of a secret (for example each character of a password) independently. For segmented oracles, it is possible to compute information leakage for multiple runs using only the path constraints generated from a single run symbolic execution. These results have been implemented as an extension to the symbolic execution tool Symbolic Path Finder (SPF) [8] using the SMT solver Z3 [4] and two model counting constraint solvers LattE [6] and ABC [1].

1998 ACM Subject Classification
D.4.6 Security and Protection, Verification, D.2.4 Software/Program Verification, Formal Methods

Keywords and phrases Side-channels, quantitative information flow, symbolic execution, model counting, constraint solvers

Digital Object Identifier 10.4230/LIPIcs.FSTTCS.2016.6

Category Invited Talk

References


* This material is based on research sponsored by NSF under grant CCF-1548848 and by DARPA under agreement number FA8750-15-2-0087. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

© Tevfik Bultan; licensed under Creative Commons License CC-BY

Editors: Akash Lal, S. Akshay, Saket Saurabh, and Sandeep Sen; Article No. 6; pp. 6:1–6:2
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany
**6:2 Side Channel Analysis**


