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

1 Abdulbaki Aydin, Lucas Bang, and Tevfik Bultan. Automata-based model counting for string constraints. In *Proceedings of the 27th International Conference on Computer Aided Verification (CAV)*, pages 255–272, 2015.

2 Michael Backes, Boris Kopf, and Andrey Rybalchenko. Automatic Discovery and Quantification of Information Leaks. In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, SP'09, pages 141–153, Washington, DC, USA, 2009. IEEE Computer Society.

3 Lucas Bang, Abdulbaki Aydin, Quoc-Sang Phan, Corina S. Pasareanu, and Tevfik Bultan. String analysis for side channels with segmented oracles. In *Proceedings of the 24th ACM*

* 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.

36th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2016).
Editors: Akash Lal, S. Akshay, Saket Saurabh, and Sandeep Sen; Article No. 6; pp. 6:1–6:2
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

SIGSOFT International Symposium on the Foundations of Software Engineering (FSE), 2016.

4 Leonardo Mendonça de Moura and Nikolaj Bjørner. Z3: an efficient SMT solver. In *Proceedings of the 14th International Conference on Tools and Algorithms for the Construction and Analysis of Systems, TACAS 2008, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2008, Budapest, Hungary, March 29-April 6, 2008*, pages 337–340, 2008.

5 Boris Köpf and David A. Basin. An information-theoretic model for adaptive side-channel attacks. In *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007*, pages 286–296, 2007.

6 Jesús A. De Loera, Raymond Hemmecke, Jeremiah Tauzer, and Ruriko Yoshida. Effective lattice point counting in rational convex polytopes. *Journal of Symbolic Computation*, 38(4):1273–1302, 2004. Symbolic Computation in Algebra and Geometry.

7 Corina S. Păsăreanu, Quoc-Sang Phan, and Pasquale Malacaria. Multi-run side-channel analysis using Symbolic Execution and Max-SMT. In *Proceedings of the 2016 IEEE 29th Computer Security Foundations Symposium*, CSF'16, Washington, DC, USA, 2016. IEEE Computer Society.

8 Corina S. Păsăreanu, Willem Visser, David Bushnell, Jaco Geldenhuys, Peter Mehlitz, and Neha Rungta. Symbolic PathFinder: integrating symbolic execution with model checking for Java bytecode analysis. *Automated Software Engineering*, pages 1–35, 2013.