Secure Programs via Game-based Synthesis

Somesh Jha
Tom Reps
Bill Harris
University of Wisconsin (Madison)

ABSTRACT

Several recent operating systems provide system calls that allow an application to explicitly manage the privileges of modules with which the application interacts. Such privilege-aware operating systems allow a programmer to a write a program that satisfies a strong security policy, even when the program interacts with untrusted modules. However, it is often non-trivial to rewrite a program to correctly use the system calls to satisfy a high-level security policy.

This paper concerns the policy-weaving problem, which is to take as input a program, a desired high-level policy for the program, and a description of how system calls affect privilege, and automatically rewrite the program to invoke the system calls so that it satisfies the policy. We describe a reduction from the policy-weaving problem to finding a winning strategy to a two-player safety game. We then describe a policy-weaver generator that implements the reduction and a novel game-solving algorithm, and present an experimental evaluation of the generator applied to a model of the Capsicum capability system. We conclude by outlining ongoing work in applying the generator to a model of the HiStar decentralized-information-flow control (DIFC) system.

SHORT BIOGRAPHIES

Somesh Jha received his B.Tech from Indian Institute of Technology, New Delhi in Electrical Engineering. He received his Ph.D. in Computer Science from Carnegie Mellon University in 1996. Currently, Somesh Jha is a Professor in the Computer Sciences Department at the University of Wisconsin (Madison), which he joined in 2000. His work focuses on analysis of security protocols, survivability analysis, intrusion detection, formal methods for security, and analyzing malicious code. Recently he has also worked on privacy-preserving protocols. Somesh Jha has published over 100 articles in highly-refereed conferences and prominent journals. He has won numerous best-paper awards. Somesh also received the NSF career award in 2005.

Thomas W. Reps is Professor of Computer Science in the Computer Sciences Department of the University of Wisconsin, which he joined in 1985. Reps is the author or co-author of four books and more than one hundred seventy-five papers describing his research (see http://www.cs.wisc.edu/ reps/). His work has concerned a wide variety of topics, including program slicing, dataflow analysis, pointer analysis, model checking, computer security, code instrumentation, language-based program-development environments, the use of program profiling in software testing, software renovation, incremental algorithms, and attribute grammars.

His collaboration with Professor Tim Teitelbaum at Cornell University from 1978 to 1985 led to the creation of two systems the Cornell Program Synthesizer and the Synthesizer Generator that explored how to build interactive programming tools that incorporate knowledge about the programming language being supported. The systems that they created were similar to modern program-development environments, such as Microsoft Visual Studio and Eclipse, but pre-dated them by more than two decades. Reps is President of GrammaTech, Inc., which he and Teitelbaum founded in 1988 to commercialize this work.

Since 1985, Professor Reps has been co-leader, with Professor Susan Horwitz, of a research group at the University of Wisconsin that has carried out many investigations of program slicing and its applications in software engineering. His most recent work concerns program analysis, computer security, and software model checking.

In 1996, Reps served as a consultant to DARPA to help them plan a project aimed at reducing the impact of the Year 2000 Problem on the U.S. Department of Defense. In 2003, he served on the F/A-22 Avionics Advisory Team, which provided advice to the U.S. Department of Defense about problems uncovered during integration testing of the planes avionics software.

Professor Reps received his Ph.D. in Computer Science from Cornell University in 1982. His Ph.D. dissertation won the 1983 ACM Doctoral Dissertation Award.

Repss 1988 paper on interprocedural slicing, with Susan Horwitz and his then-student David Binkley, was selected as one of the 50 most influential papers from the ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI), 1979-99. According to Google Scholar, the 1988 paper and the subsequent journal version have received over 1,600 citations.

His 2004 paper about analysis of assembly code, with his student Gogul Balakrishnan, received the ETAPS Best-Paper Award for 2004 from the European Association for Programming Languages and Systems (EAPLS). His 2008 paper about a system for generating static analyzers for machine instructions, with his student Junghee Lim, received the ETAPS Best-Paper

ISBN 978-0-9835678-3-7/13.

Award for 2008 from EAPLS. In 2010, his 1984 paper ”The Synthesizer Generator”, with Tim Teitelbaum, received an ACM SIGSOFT Retrospective Impact Paper Award. In 2011, his 1994 paper ”Speeding up slicing”, with Susan Horwitz, Mooly Sagiv, and Genevieve Rosay, also received an ACM SIGSOFT Retrospective Impact Paper Award.

Three of his students, Gogul Balakrishnan, Akash Lal, and Junghee Lim have been the recipients of the Outstanding Graduate Student Research Award given by the University of Wisconsin Computer Sciences Department. Akash Lal was also a co-recipient of the 2009 SIGPLAN Outstanding Doctoral Dissertation Award, and he was named as one of the 18 awardees selected for the 2011 India TR-35 list (top innovators under 35).

In 2003, Reps was recognized as a ”Highly Cited Researcher” in the field of Computer Scienceone of 230 worldwide who received such recognition by the Institute for Scientific Information. As of February 2013, Reps was ranked 8th (citations) and 4th (field rating) on Microsoft Academic Searchs list of most-highly-cited authors in the field of Programming Languages, and 23rd (citations) and 13th (field rating) on its list of most-highly-cited authors in the field of Software Engineering.

Reps has also been the recipient of an NSF Presidential Young Investigator Award (1986), a Packard Fellowship (1988), a Humboldt Research Award (2000), and a Guggenheim Fellowship (2000). He is also an ACM Fellow (2005).

Reps has held visiting positions at the Institut National de Recherche en Informatique et en Automatique (INRIA) in Rocquencourt, France (1982-83), the University of Copenhagen, Denmark (1993-94), the Consiglio Nazionale delle Ricerche in Pisa, Italy (2000-2001), and the University Paris Diderot Paris 7 (2007-2008).

William Harris is a PhD student and research assistant at the University of Wisconsin-Madison, where he is advised by Somesh Jha and Thomas Reps. His current research focuses on applying formal methods to problems in computer security. He received his B.S. from Purdue University in 2007, and received his M.S. from the University of Wisconsin-Madison in 2011. He has worked as a visiting researcher for NEC Labs America and Microsoft Research. He was a Microsoft Research Fellow from 2010 - 2011.