Lecture Notes in Computer Science 12031

More information about this series at http://www.springer.com/series/7408

Supratik Chakraborty · Jorge A. Navas (Eds.)

Verified Software

Theories, Tools, and Experiments

11th International Conference, VSTTE 2019
New York City, NY, USA, July 13–14, 2019
Revised Selected Papers

Springer

Editors
Supratik Chakraborty
Indian Institute of Technology Bombay
Mumbai, India

Jorge A. Navas
SRI International
Menlo Park, CA, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-41599-0 ISBN 978-3-030-41600-3 (eBook)
https://doi.org/10.1007/978-3-030-41600-3

LNCS Sublibrary: SL2 – Programming and Software Engineering

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the contributed and invited papers presented at VSTTE 2019, the 11th Working Conference on Verified Software: Theories, Tools, and Experiments held on July 13–14, 2019 in New York City, USA. The working conference was co-located with the 31st International Conference on Computer-Aided Verification (CAV 2019).

The Verified Software Initiative (VSI), spearheaded by Tony Hoare and Jayadev Misra, is an ambitious research program for making large-scale verified software a practical reality. VSTTE is the main forum for advancing the initiative. VSTTE brings together experts spanning the spectrum of software verification in order to foster international collaboration on the critical research challenges.

There were 17 submissions to VSTTE 2019, with authors from 19 countries. The Program Committee consisted of 32 distinguished computer scientists from all over the world. Each submission was reviewed by three Program Committee members in single-blind mode. In order to ensure that topic-specific expert reviews were obtained, help was also sought from five external reviewers. After a comprehensive discussion on the strengths and weaknesses of papers, the committee decided to accept nine papers. The technical program also included four invited talks by Prof. Tevfik Bultan (University of California, Santa Barbara, USA), Prof. Marsha Chechik (University of Toronto, Canada), Prof. Aarti Gupta (Princeton University, USA) and Prof. Antonine Miné (Sorbonne Université, CNRS, LIP6, Paris, France).

Partial funding for the working conference was provided by the CAV 2019 organizers. We greatly acknowledge their help. We are also thankful to EasyChair for providing an easy and efficient mechanism for submission of papers, management of reviews, and eventually in the generation of this volume.

December 2019

Supratik Chakraborty
Jorge A. Navas
Natarajan Shankar

Organization

Program Committee

Aws Albarghouthi	University of Wisconsin-Madison, USA
Supratik Chakraborty	IIT Bombay, India
Xinyu Feng	Nanjing University, People's Republic of China
Graeme Gange	Monash University, Australia
Ashutosh Gupta	IIT Bombay, India
Arie Gurfinkel	University of Waterloo, Canada
Liana Hadarean	Synopsys, USA
Joxan Jaffar	National University of Singapore, Singapore
Dejan Jovanović	SRI International, USA
Aditya Kanade	Indian Institute of Science, India
Yunho Kim	Korea Advanced Institute of Science and Technology, South Korea
Tim King	Google, USA
Yi Li	Nanyang Technological University, Singapore
Nuno P. Lopes	Microsoft, UK
David Monniaux	CNRS and VERIMAG, France
Jose F. Morales	IMDEA Software Research Institute, Spain
Yannick Moy	AdaCore, France
Kedar Namjoshi	Nokia-Bell Laboratories, USA
Nina Narodytska	VMware Research, USA
Jorge Navas	SRI International, USA
Aina Niemetz	Stanford University, USA
Oded Padon	Stanford University, USA
Venkatesh R	Tata Consultancy Services, India
Philipp Ruemmer	Uppsala University, Sweden
Peter Schrammel	University of Sussex, UK
Natarajan Shankar	SRI International, USA
Rahul Sharma	Microsoft, India
Jing Sun	The University of Auckland, New Zealand
Michael Tautschnig	Queen Mary University of London, UK
Tachio Terauchi	Waseda University, Japan
Aditya Thakur	University of California, Davis, USA
Bow-Yaw Wang	Academia Sinica, People's Republic of China (Taiwan)
Valentin Wüstholz	ConsenSys Diligence, Germany

Additional Reviewers

Hajdu, Akos
Maghareh, Rasool
Mukherjee, Suvam
Noetzli, Andres
Reynolds, Andrew

Abstract of Invited Talks

Combinations of Reusable Abstract Domains for a Multilingual Static Analyzer

Matthieu Journault[1], Antoine Miné[1,2], Raphaël Monat[1], and Abdelraouf Ouadjaout[1]

[1] Sorbonne Université, CNRS, LIP6, 75005 Paris, France
{matthieu.journault,antoine.mine,raphael.monat, abdelraouf.ouadjaout}@lip6.fr
[2] Institut Universitaire de France, 75005 Paris, France

Abstract. We discuss the design of MOPSA, an ongoing effort to design a novel semantic static analyzer by abstract interpretation. MOPSA strives to achieve a high degree of modularity and extensibility by considering value abstractions for numeric, pointer, objects, arrays, etc. as well as syntax-driven iterators and control-flow abstractions uniformly as domain modules, which offer a unified signature and loose coupling, so that they can be combined and reused at will. Moreover, domains can dynamically rewrite expressions, which simplifies the design of relational abstractions, encourages a design based on layered semantics, and enables domain reuse across different analyses and different languages. We present preliminary applications of MOPSA analyzing simple programs in subsets of the C and Python programming languages, checking them for run-time errors and uncaught exceptions.

Uncertainty, Modeling and Safety Assurance: Towards a Unified Framework

Marsha Chechik, Sahar Kokaly, Mona Rahimi, Rick Salay, and Torin Viger

University of Toronto, Toronto, Canada
{chechik,skokaly,mrahimi,
rsalay,torinviger}@cs.toronto.edu

Abstract. Uncertainty occurs naturally in software systems, including those that are model-based. When such systems are safety-critical, they need to be assured, e.g., by arguing that the system satisfies its safety goals. But how can we rigorously reason about assurance in the presence of uncertainty? In this paper, we propose a vision for a framework for managing uncertainty in assurance cases for software systems, and in particular, for *model-based* software systems, by systematically *identifying*, *assessing* and *addressing* it. We also discuss a set of challenges that need to be addressed to realize this framework.

Verifying Network Control Planes

Aarti Gupta

Princeton University, Princeton, USA
aartig@cs.princeton.edu

Abstract. The last decade has seen tremendous advances in applying formal methods to verification of computer networks. In this talk, I will describe two recent efforts that target network control planes, i.e., the complex distributed systems comprising various protocols for exchanging messages between routers and selecting paths for routing traffic. In the first effort, we develop a general-purpose, symbolic model of the network control and data planes that encodes the stable states of a network as a satisfying assignment to an SMT formula. Using this model, we show how to verify a wide variety of properties including reachability, fault-tolerance, router equivalence, and load balancing. Our second effort focuses on leveraging symmetry in control planes to find network abstractions that achieve compression in size while preserving many properties of interest.

This is joint work with Ryan Beckett, Ratul Mahajan, and David Walker.

Quantifying Information Leakage Using Model Counting Constraint Solvers

Tevfik Bultan

University of California, Santa Barbara, USA
bultan@cs.ucsb.edu

Abstract. This paper provides a brief overview of recent results in quantitative information flow analysis, model counting constraints solvers, side-channel analysis and attack synthesis. By combining model counting constraints solvers with symbolic execution it is possible to quantify the amount of information that a program leaks about a secret input. As discussed below, this type of analysis is crucial for detection and analysis of side channel vulnerabilities.

This material is based on research supported by an Amazon Research Award, by NSF under Grant CCF-1817242, and by DARPA under the 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.

Contents