Lecture Notes in Computer Science 5295

Natarajan Shankar   Jim Woodcock (Eds.)

Verified Software: Theories, Tools, Experiments

Second International Conference, VSTTE 2008
Toronto, Canada, October 6-9, 2008
Proceedings

Springer

Volume Editors

Natarajan Shankar
SRI International
Computer Science Laboratory
MS EL256, 333 Ravenswood Avenue
Menlo Park, CA 94025-3493, USA
E-mail: shankar@csl.sri.com

Jim Woodcock
University of York
Department of Computer Science
Heslington, York YO10 5DD, UK
E-mail: jim@cs.york.ac.uk

Library of Congress Control Number: 2008935491

CR Subject Classification (1998): B.6.3, B.2.2, D.2.4, D.4, F.3, G.4

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743
ISBN-10 3-540-87872-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-87872-8 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12532179 06/3180 5 4 3 2 1 0

Preface

This volume contains the papers presented at the Second Working Conference on Verified Software: Theories, Tools, and Experiments held in Toronto during October 6–9, 2008. This followed a successful working conference held in Zurich in 2005, also published in *Lecture Notes in Computer Science* as volume 4171 (DOI 10.1007/978-3-540-69149-5). The second conference formally inaugurated the Verified Software Initiative (VSI), a 15-year, co-operative, international project directed at the scientific challenges of large-scale software verification. The scope of the cooperative effort includes the sharing and interoperability of tools, the alignment of theory and practice, the identification of challenge problems, the construction of benchmark suites, and the execution of large-scale experiments. The conference was open to everyone interested in participating actively in the VSI effort.

The scope of the VSTTE conferences includes all aspects of verified software, covering theoretical as well as experimental work:

- requirements modelling
- specification languages
- specification case studies
- formal calculi
- programming languages
- language semantics
- software design methods
- software testing
- automatic code generation
- refinement methodologies
- type systems
- computer security
- static analyzers
- dynamic analyzers
- model checkers
- theorem provers
- satisfiability checkers
- benchmarks
- challenge problems
- integrated verification environments

The conference was addressed by four keynote speakers:

- John Reynolds (Carnegie Mellon University)
- Moshe Vardi (Rice University)
- Andreas Podelski (University of Freiburg)
- Sriram Rajamani (Microsoft Research)

Two invited tutorials were given by:

- Eric Hehner (University of Toronto) *Practical Predicative Programming Primer*
- Ernie Cohen (Microsoft Research) *The Hyper-V Project*
- Leonardo de Moura (Microsoft Research) *SMT@Microsoft*

The volume contains 16 rigorously refereed papers on different topics covering the spectrum from theoretical results to verification experience reports. The conference also included a session of short presentations of ongoing work.

The main VSTTE 2008 conference hosted three specialized workshops on Theories, Tools, and Experiments for Verified Software.

VS-THEORY: Workshop on Theory for Verified Software

Dave Naumann (Stevens Institute)
Peter O'Hearn (Queen Mary, University of London)

Summary: Program verification has seen a worldwide renaissance, with many ongoing practical tool projects and experimental verification efforts. The current state of the field builds on fundamental theoretical advances of the past. Similarly, future advances on software verification will depend on developments in theory. This can range from the difficult and essential study of soundness of delicate proof methods, to the discovery of new specification techniques and proof methods, to dramatic simplification or unification of existing methods, to as yet unknown breakthroughs. The Verified Software Initiative (VSI) is envisaged as a 15-year Grand Challenge project to advance the state of software verification. Specific milestones and challenges of the VSI should often be concrete in nature, but advances beyond immediate progress will again depend on theoretical insights. The purpose of this workshop was to bring together theory and programming language researchers to discuss scientific challenges posed by software verification.

VS-TOOLS: Workshop on Tools in Verified Software

Daniel Kroening (University of Oxford)
Tiziana Margaria (University of Potsdam)

Summary: The scope of the workshop included submissions of technical and position papers on all aspects of tools conducted relating to verified software. Paper-and-pencil proofs are error-prone and expensive. Program verification provides better value if proofs are checked by machine, and preferably generated automatically. The properties checked can range from light-weight control-flow properties to full specification. In order to demonstrate that machine reasoning can improve the quality and cost of artifacts of industrial software engineers, a substantial tool-building effort is required. This workshop brought tool-builders together in order to learn about

- Interfaces between tools (e.g., decision procedures and program verifiers)
- Tool integration platforms
- Case studies that particularly excite the tool aspect

VS-EXPERIMENTS: Workshop on Experiments in Verified Software

Rajeev Joshi (NASA/JPL Laboratory for Reliable Software)
Joseph Kiniry (University College Dublin)

Summary: The scope of the workshop included technical and position papers on all aspects of experiments conducted relating to verified software. The organizers are especially interested in the reflective results of past challenges and ongoing experiments. Such projects include:

- The Mondex Case Study: `vsr.sourceforge.net/mondex.htm`
- The Verified File System: `www.cs.york.ac.uk/circus/mc/abz`
- Medical devices: `www.cas.mcmaster.ca/sqrl/pacemaker.htm`

- Verifying Free andOpen Source Software, e.g., the Apache webserver and the KOA e-voting platform

This workshop was meant to be a *working* workshop. Participants were responsible for formulating action plans, based upon current experiences and best-practices, for tackling the challenges inherent in identifying, defining, promoting, executing, sharing, maintaining, and publishing the results of scientific experiments in verified software.

We would like to thank the following: the keynote speakers and tutors; the authors of all submissions; the members of the Programme Committee (95% of all reviews were received on time!); the workshop organizers and participants; Rick Hehner and his team for the local arrangements for the entire event; Richard Paige for conference and workshop publicity; and last—but not least—our Steering Committee, Jay Misra and Tony Hoare. We are also pleased to acknowledge financial support for VSTTE 2008 from US and UK funding agencies: the US National Science Foundation (NSF) (as part of Grant CNS-0627284) and EPSRC (as part of grant EP/D506735/1), and from Microsoft Research. The proceedings were assembled using EasyChair.

July 2008

Natarajan Shankar
Jim Woodcock

Conference Organization

Steering Committee

Tony Hoare	Microsoft Research Cambridge
Jay Misra	University of Texas at Austin

Programme Chairs

Natarajan Shankar	SRI International
Jim Woodcock	University of York

Programme Committee

Egon Börger	University of Pisa
Supratik Chakraborty	Indian Institute of Technology, Bombay
Patrick Cousot	École Normale Supérieure, Paris
Jin Song Dong	National University of Singapore
José-Luiz Fiadeiro	University of Leicester
Kokichi Futatsugi	JAIST
Chris George	UNU-IIST
Ian Hayes	University of Queensland
Eric Hehner	University of Toronto
Rajeev Joshi	Jet Propulsion Laboratory
Joseph Kiniry	University College Dublin
Yassine Lakhnech	Université Joseph Fourier
Gary Leavens	University of Central Florida
Zhiming Liu	UNU-IIST
Peter Manolios	Northeastern University
Tiziana Margaria	University of Potsdam
David Naumann	Stevens Institute
Peter O'Hearn	Queen Mary, University of London
Ernst-Rüdiger Olderog	University of Oldenburg
Wolfgang Paul	Saarland University
Augusto Sampaio	Federal University of Pernambuco
Mark Utting	Waikato University
Jian Zhang	Chinese Academy of Sciences

Local Organization

Eric Hehner	University of Toronto

Publicity Chair

Richard Paige	University of York

External Reviewers

Oliver R. Athing
Stephen Bloom
Ben Chambers
Chunqing Chen
Zhenbang Chen
Yuki Chiba
Antonio Cisternino
Dermot Cochran
Robert Colvin
Márcio Cornélio
Jed Davis
Peter Dillinger
Brijesh Dongol
Fintan Fairmichael
Yuzhang Feng
Sibylle Fröschle
Daniel Gaina
Radu Grigore
Bhargav Gulavani
Yu Guo
Mark Hillebrand
Viliam Holub
Georg Jung
E.-Y. Kang
Ioannis Kassios
Weiqiang Kong
Yang Liu
Charles Morisset
Masaki Nakamura
Zhaozhong Ni
Kazuhiro Ogata
Stan Rosenberg
Andreas Roth
Joseph Ruskiewicz
Gerhard Schellhorn
Norbert Schirmer
Zhong Shao
Leila Silva
Graeme Smith
Volker Stolz
Jun Sun
Aaron Turon
Kapil Vaswani
Xian Zhang

Table of Contents

Keynote Talks (Abstracts)

Logics

Tools

Case Studies

Methodology

Verisoft

Paper from VSTTE 2005