Corina S. Păsăreanu (Ed.)

Model Checking Software

16th International SPIN Workshop
Grenoble, France, June 26-28, 2009
Proceedings
Preface

This volume contains the proceedings of the 16th International SPIN Workshop on Model Checking of Software (SPIN 2009), that was held at the Grenoble World Trade Center, in Grenoble, France, June 26–28, 2009. The workshop was co-located with the 21st International Conference on Computer-Aided Verification (CAV 2009).

The SPIN workshop is a forum for practitioners and researchers interested in the model checking-based analysis of software systems. The focus of the workshop is on theoretical advances and empirical evaluations related to state-space and path exploration techniques, as implemented in the SPIN model checker and other software verification tools. The workshop aims to encourage interactions and exchanges of ideas with all related areas in software engineering. SPIN 2009 was the 16th event in the workshop series, which started in 1995.

This year, we received 41 submissions (34 technical papers and 7 tool papers) out of which 18 papers were accepted (15 technical papers and 3 tool papers). Each submission was reviewed by three Program Committee members.

In addition to the refereed papers, the workshop featured four invited talks given by Patrice Godefroid, from Microsoft Research, USA, on “Software Model Checking Improving Security of a Billion Computers,” Marta Kwiatkowska, from Oxford University, UK, “On Quantitative Software Verification,” Joseph Sifakis (recipient of the Turing Award 2007), from VERIMAG, France, on “The Quest for Correctness - Beyond a posteriori Verification,” and Willem Visser, from the University of Stellenbosch, South Africa, on “Who Really Cares if the Program Crashes?”

We would like to thank the authors of submitted papers, the invited speakers, the Program Committee members, the external reviewers, and the Steering Committee, for their help in composing a strong program. Special thanks go to Stefan Leue for his guidance throughout the SPIN 2009 organization, to Saddek Ben Salem for the SPIN 2009 local organization, and to last year’s organizers, Klaus Havelund and Rupak Majumdar, for their advice and help with advertising the event. We also thank Springer for agreeing to publish these proceedings as a volume of Lecture Notes in Computer Science.

The EasyChair system was used for the submission and reviewing of the papers and also for the preparation of the proceedings.

April 2009

Corina S. Păsăreanu
Organization

Program Chair

Corina S. Păsăreanu

Program Committee

Christel Baier University Bonn, Germany
Dragan Bošnački Eindhoven University, The Netherlands
Patricia Bouyer ÉNS de Cachan, France
Lubos Brim Masaryk U, Czech Republic
Marsha Chechik University of Toronto, Canada
Matthew Dwyer University of Nebraska, USA
Stefan Edelkamp T.U. Dortmund, Germany
Jaco Geldenhuys University of Stellenbosch, South Africa
Susanne Graf VERIMAG, France
Klaus Havelund JPL, USA
Gerard Holzmann JPL, USA
Radu Iosif VERIMAG, France
Michael Jones Brigham Young U, USA
Sarfraz Khurshid University of Texas, Austin, USA
Orna Kupferman Hebrew University, Israel
Stefan Leue University of Konstanz, Germany
Rupak Majumdar University of California, Los Angeles, USA
Madan Musuvathi Microsoft Research, USA
Koushik Sen University of California, Berkeley, USA
Scott Stoller Stony Brook University, USA
Farn Wang National Taiwan University, Taiwan
Pierre Wolper University of Liege, Belgium

Steering Committee

Dragan Bošnački Eindhoven University, The Netherlands
Stefan Edelkamp T.U. Dortmund, Germany
Susanne Graf VERIMAG, France
Klaus Havelund JPL, USA
Stefan Leue (Chair) University of Konstanz, Germany
Rupak Majumdar University of California, Los Angeles, USA
Pierre Wolper, University of Liege, Belgium
Local Organization
Saddek Bensalem (CAV 2009 Local Organization, VERIMAG/UJF, France)

External Reviewers

Husain Aljazzar
Adam Antonik
Bahareh Badban
Jiri Barnat
Tobias Blechmann
Jacob Burnim
Franck Cassez
Ivana Cerna
Joel Galenson
Pallavi Joshi
Sudeep Juvekar
Shadi Abdul Khalek
Peter Kissmann
Joachim Klein
Filip Konecny
Laura Kovacs

Matthias Kuntz
Roman Manevich
Nicolas Markey
Eric Mercer
Chang-Seo Park
Polyvios Pratikakis
Neha Rungta
Roopsha Samanta
Christoph Scheben
Jiri Simacek
Jocilyn Simmonds
Christos Stergiou
Damian Sulewski
Faraz Torchizi
Wei Wei
Tim Willemse
# Table of Contents

## Invited Contributions

Software Model Checking Improving Security of a Billion Computers . . . 1  
*Patrice Godefroid*

On Quantitative Software Verification .............................. 2  
*Marta Kwiatkowska*

The Quest for Correctness-Beyond *a Posteriori* Verification ........ 4  
*Joseph Sifakis*

Who Really Cares If the Program Crashes? .......................... 5  
*Willem Visser*

## Regular Papers

Tool Presentation: Teaching Concurrency and Model Checking.......... 6  
*Mordechai (Moti) Ben-Ari*

Fast, All-Purpose State Storage ...................................... 12  
*Peter C. Dillinger and Panagiotis (Pete) Manolios*

Efficient Probabilistic Model Checking on General Purpose Graphics  32  
*Dragan Bošnački, Stefan Edelkamp, and Damian Sulewski*

Improving Non-Progress Cycle Checks ............................... 50  
*David Faragó and Peter H. Schmitt*

Reduction of Verification Conditions for Concurrent System Using  68  
*Malay K. Ganai and Sudipta Kundu*

Probabilistic Reachability for Parametric Markov Models ............. 88  
*Ernst Moritz Hahn, Holger Hermanns, and Lijun Zhang*

Extrapolation-Based Path Invariants for Abstraction Refinement of  107  
*Fifo Systems*  
*Alexander Heußner, Tristan Le Gall, and Grégoire Sutre*

A Decision Procedure for Detecting Atomicity Violations for  125  
*Communicating Processes with Locks*  
*Nicholas Kidd, Peter Lammich, Tayssir Touili, and Thomas Reps*
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eclipse Plug-In for Spin and st2msc Tools-Tool Presentation</td>
<td>143</td>
</tr>
<tr>
<td>Tim Kovše, Boštjan Vlaovič, Aleksander Vreže, and Zmago Brezočnik</td>
<td></td>
</tr>
<tr>
<td>Symbolic Analysis via Semantic Reinterpretation</td>
<td>148</td>
</tr>
<tr>
<td>Junghee Lim, Akash Lal, and Thomas Reps</td>
<td></td>
</tr>
<tr>
<td>EMMA: Explicit Model Checking Manager (Tool Presentation)</td>
<td>169</td>
</tr>
<tr>
<td>Radek Pelánek and Václav Rosecký</td>
<td></td>
</tr>
<tr>
<td>Efficient Testing of Concurrent Programs with Abstraction-Guided</td>
<td>174</td>
</tr>
<tr>
<td>Symbolic Execution</td>
<td></td>
</tr>
<tr>
<td>Neha Rungta, Eric G. Mercer, and Willem Visser</td>
<td></td>
</tr>
<tr>
<td>Subsumer-First: Steering Symbolic Reachability Analysis</td>
<td>192</td>
</tr>
<tr>
<td>Andrey Rybalchenko and Rishabh Singh</td>
<td></td>
</tr>
<tr>
<td>Identifying Modeling Errors in Signatures by Model Checking</td>
<td>205</td>
</tr>
<tr>
<td>Sebastian Schmerl, Michael Vogel, and Hartmut König</td>
<td></td>
</tr>
<tr>
<td>Towards Verifying Correctness of Wireless Sensor Network Applications</td>
<td>223</td>
</tr>
<tr>
<td>Using Insense and Spin</td>
<td></td>
</tr>
<tr>
<td>Oliver Sharma, Jonathan Lewis, Alice Miller, Al Dearle, Dharini Balasubramaniam, Ron Morrison, and Joe Sventek</td>
<td></td>
</tr>
<tr>
<td>Verification of GALS Systems by Combining Synchronous Languages</td>
<td>241</td>
</tr>
<tr>
<td>and Process Calculi</td>
<td></td>
</tr>
<tr>
<td>Hubert Garavel and Damien Thivolle</td>
<td></td>
</tr>
<tr>
<td>Experience with Model Checking Linearizability</td>
<td>261</td>
</tr>
<tr>
<td>Martin Vechev, Eran Yahav, and Greta Yorsh</td>
<td></td>
</tr>
<tr>
<td>Automatic Discovery of Transition Symmetry in Multithreaded Programs</td>
<td>279</td>
</tr>
<tr>
<td>Using Dynamic Analysis</td>
<td></td>
</tr>
<tr>
<td>Yu Yang, Xiaofang Chen, Ganesh Gopalakrishnan, and Chao Wang</td>
<td></td>
</tr>
<tr>
<td>Author Index</td>
<td>297</td>
</tr>
</tbody>
</table>