

Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

2057

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Matthew Dwyer (Ed.)

Model Checking Software

8th International SPIN Workshop
Toronto, Canada, May 19–20, 2001
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Matthew Dwyer
Kansas State University, Department of Computing and Information Sciences
234 Nichols Hall, Manhattan, KS 66506-2302, USA
E-mail: dwyer@cis.ksu.edu

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Model checking software : proceedings / 8th International SPIN
Workshop, Toronto, Canada, May 19 - 20, 2001. Matthew Dwyer (ed.). -
Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ;
Milan ; Paris ; Singapore ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2057)
ISBN 3-540-42124-6

CR Subject Classification (1998): F.3, D.2.4, D.3.1

ISSN 0302-9743

ISBN 3-540-42124-6 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2001
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna
Printed on acid-free paper SPIN: 10781569 06/3142 5 4 3 2 1 0

Preface

Research on model checking has matured from a purely theoretical topic to encompass tool development and applications, in addition to more foundational topics. This diversity of model checking research is driving the area onward as foundational developments enable automation, development of robust tool support enables increasingly sophisticated applications, and feedback from applications spurs further work on the underlying theory and tools. The program of the eighth SPIN workshop reflected this diversity; it included three contributions on foundational topics, eight contributions on model checking tools, and eight contributions describing applications of model checking.

Continuing a trend begun in the seventh SPIN workshop, the eighth SPIN workshop emphasized the connections between model checking and program analysis. Research on static program analysis has a long history in both the compiler and software engineering communities. In an effort to establish a dialog between researchers in model checking and software analysis, this year's workshop was co-located with the 23rd International Conference on Software Engineering in Toronto. The workshop program contained several contributions that were clearly targeted at analyzing programs. Three contributions addressed tools for model checking of program source code, implemented in C and Java, and one contribution described model checking of a popular software component architecture.

The workshop featured 13 refereed technical papers selected from 26 submissions and two refereed descriptions of model checking tools selected from four submissions. Each submitted paper was reviewed by at least three members of the program committee; additional reviewers were used for several papers. The program committee discussed the merits of the submitted papers to arrive at the final 15 refereed contributions. In addition to refereed contributions, two leading experts in model checking technology and three groups that are applying model checking techniques in an industrial setting were invited to give presentations. The invited presentations were given by: Doron Peled (Bell Laboratories), Rob Gerth (Intel Corporation), Leszek Holenderski (Philips Research), Erik Engstrom (Honeywell Laboratories), and Bernhard Steffen (Metaframe Technologies). This proceedings issue contains four contributions detailing the content of the invited presentations. A panel session on the topic of "Prospects for and impediments to practical model checking" was organized to generate a dialog between those working on applying model checking and researchers working on extending model checking technologies.

Historically, the SPIN workshop has served as a forum for researchers interested in the subject of automata-based, explicit-state model checking technologies for the analysis and verification of asynchronous concurrent and distributed systems. In recent years, the scope of the workshop has broadened to encompass applications of model checking to software analysis. The workshop is named af-

ter the SPIN model checker, developed by Gerard Holzmann, which is one of the best known and most widely used model checking tools. The first SPIN workshop was held in October 1995 in Montréal. Subsequent workshops were held in New Brunswick (August 1996), Enschede (April 1997), Paris (November 1998), Trento (July 1999), Toulouse (September 1999), and at Stanford University (August 2000).

Acknowledgments. The editor wishes to thank the program committee members, and the referees, for their help in in organizing the workshop. Committee members volunteered many valuable suggestions as well as a significant amount of time for refereeing and discussing papers. The workshop organizers wish to thank the ICSE'2001 organizing committee for facilitating the co-location of the SPIN workshop and ACM SIGSOFT, Lucent Technologies, Microsoft Research, and the Office of Naval Research for their sponsorship and support of the SPIN workshop.

March 2001

Matthew B. Dwyer

Organization

Organizing Committee

General Chair: Moshe Y. Vardi (Rice University, USA)

Program Chair: Matthew B. Dwyer (Kansas State University, USA)

Local Arrangements Chair: Marsha Chechik (University of Toronto, Canada)

Program Committee

George Avrunin (University of Massachusetts, USA)

Thomas Ball (Microsoft Research, USA)

Ed Brinksma (University of Twente, The Netherlands)

Marsha Chechik (University of Toronto, Canada)

Dennis R. Dams (Eindhoven University, The Netherlands)

Klaus Havelund (QSS/Recom at NASA Ames Research Center, USA)

Connie Heitmeyer (Naval Research Laboratory, USA)

Gerard J. Holzmann (Bell Laboratories, USA)

Fabio Somenzi (University of Colorado, USA)

Willem Visser (RIACS at NASA Ames Research Center, USA)

Pierre Wolper (Université de Liege, Belgium)

Referees

R. Bloem

J. Katoen

T. Ruys

D. Bosnacki

R. Langerak

R. de Vries

J. Geldenhuys

F. Lerda

B. Wolter

D. Giannakopoulou

S. Park

H. Hermanns

C. Pecheur

L. Holenderski

G. Rosu

Sponsoring Organizations

The eighth SPIN Workshop was sponsored by the ACM SIGSOFT (Special Interest Group on Software Engineering). Additional support was provided by: Bell Laboratories, Lucent Technologies, USA, Microsoft Research, Microsoft Inc., USA, and The Office of Naval Research, USA.

Table of Contents

Invited Keynotes

From Model Checking to a Temporal Proof.....	1
<i>Doron Peled (Bell Laboratories), Lenore Zuck (New York University)</i>	
Model Checking if Your Life Depends on It: A View from Intel's Trenches	15
<i>Rob Gerth (Intel corp.)</i>	

Technical Papers and Tool Reports

Model-Checking Infinite State-Space Systems with Fine-Grained Abstractions Using SPIN	16
<i>Marsha Chechik, Benet Devereux, Arie Gurfinkel (University of Toronto)</i>	
Implementing LTL Model Checking with Net Unfoldings	37
<i>Javier Esparza (Technische Universität München), Keijo Heljanko (Helsinki University of Technology)</i>	
Directed Explicit Model Checking with HSF-SPIN	57
<i>Stefan Edelkamp, Alberto Lluch Lafuente, Stefan Leue (Albert-Ludwigs-Universität)</i>	
Addressing Dynamic Issues of Program Model Checking	80
<i>Flavio Lerda, Willem Visser (NASA Ames Research Center)</i>	
Automatically Validating Temporal Safety Properties of Interfaces	103
<i>Thomas Ball, Sriram K. Rajamani (Microsoft Research)</i>	
Verification Experiments on the MASCARA Protocol	123
<i>Guoping Jia, Susanne Graf (VERIMAG)</i>	
Using SPIN for Feature Interaction Analysis – A Case Study	143
<i>Muffy Calder, Alice Miller (University of Glasgow)</i>	
Behavioural Analysis of the Enterprise JavaBeans TM Component Architecture.....	163
<i>Shin Nakajima (NEC Corporation), Tetsuo Tamai (University of Tokyo)</i>	
p2b: A Translation Utility for Linking Promela and Symbolic Model Checking (Tool Paper).....	183
<i>Michael Baldamus, Jochen Schröder-Babo (University of Karlsruhe)</i>	

Transformations for Model Checking Distributed Java Programs	192
<i>Scott D. Stoller, Yanhong A. Liu (SUNY at Stony Brook)</i>	
Distributed LTL Model-Checking in SPIN	200
<i>Jiri Barnat, Lubos Brim (Masaryk University Brno), Jitka Stříbrná (University of Pennsylvania)</i>	
Parallel State Space Construction for Model-Checking	217
<i>Hubert Garavel, Radu Mateescu, Irina Smarandache (INRIA Rhône-Alpes)</i>	
Model Checking Systems of Replicated Processes with Spin	235
<i>Fabrice Derepas (Nortel Networks), Paul Gastin (Université Paris)</i>	
A SPIN-Based Model Checker for Telecommunication Protocols	252
<i>Vivek K. Shanbhag, K. Gopinath (Indian Institute of Science)</i>	
Modeling and Verifying a Price Model for Congestion Control in Computer Networks Using Promela/Spin	272
<i>Clement Yuen, Wei Tjioe (University of Toronto)</i>	
Invited Project Summaries	
A Model Checking Project at Philips Research	288
<i>Leszek Holenderski (Philips Research)</i>	
Applications of Model Checking at Honeywell Laboratories	296
<i>Darren Cofer, Eric Engstrom, Robert Goldman, David Musliner, Steve Vestal (Honeywell Laboratories)</i>	
Coarse-Granular Model Checking in Practice	304
<i>Bernhard Steffen, Tiziana Margaria, Volker Braun (METAFrame Technologies, Universität Dortmund)</i>	
Author Index	313