Lecture Notes in Computer Science 2057
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

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

http://www.springer.de

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 after 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
D. Bosnacki
J. Geldenhuys
D. Giannakopoulou
H. Hermanns
L. Holenderski
J. Katoen
R. Langerak
F. Lerda
S. Park
C. Pecheur
G. Rosu
T. Ruys
R. de Vries
B. Wolter

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

Technical Papers and Tool Reports

Invited Project Summaries