Workshop on Trustworthy Software

May 18–19, 2006, Saarbrücken, Germany

Edited by

Serge Autexier
Stephan Merz
Leon van der Torre
Reinhard Wilhelm
Pierre Wolper

OASICS

Editors

Serge Autexier (DFKI Saarbrücken), autexier@dfki.de
Stephan Merz (INRIA Nancy & LORIA), Stephan.Merz@loria.fr
Leon van der Torre (University of Luxembourg), leon.vandertorre@uni.lu
Reinhard Wilhelm (Saarland University), wilhelm@cs.uni-saarland.de
Pierre Wolper (Université de Liege), pw@montefiore.ulg.ac.be

ACM Classification 1998
D.2.4 Software/Program Verification

ISBN 978-3-939897-02-6

Published online and open access by
Schloss Dagstuhl – Leibniz-Center for Informatics GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany.

Publication date
August, 2006.

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Digital Object Identifier: 10.4230/OASIcs.TrustworthySW.2006.i

ISBN 978-3-939897-02-6 **ISSN 2190-6807** **http://www.dagstuhl.de/oasics**

OASIcs – OpenAccess Series in Informatics

OASIcs aims at a suitable publication venue to publish peer-reviewed collections of papers emerging from a scientific event. OASIcs volumes are published according to the principle of Open Access, i.e., they are available online and free of charge.

ISSN 2190-6807

www.dagstuhl.de/oasics

Preface

The Interreg III C/E-Bird project "Recherches sans frontières/Forschen ohne Grenzen" aims at developing and strengthening the links between researchers in the SaarLorLuxWallonie region. Supporting actions initiated by the project were the documentation of shared and complementary research competences in that region as well as a series of thematic workshops held in 2006. The workshops were especially devoted to provide a forum for young scientists to present their research to a transnational audience from the SaarLorLuxWallonie region and to identify possible synergies and possibilities for cooperations.

The workshop on "Trustworthy Software" was the first workshop in that series and was held in Saarbrücken on 18-19th May 2006. It was organized by the Saarland University. As workshop theme the workshop chairs selected "Trustworthy Software" because a considerable concentration of research competence was found to exist in the SaarLorLuxWallonie region. The workshop aimed at presenting and fostering this research competence in the area of developing safe, secure and reliable software, computers and networks.

34 high-quality proposals were submitted for talks. In order to match the two-day format, the workshop chairs selected 21 for presentation at the workshop preferring contributions from young researchers.

The workshop consisted of the selected talks distributed into six sessions (one about Specification, three about Verification, one about Security and one about Privacy, Secrecy & Trust) and an invited talk by Christoph Weidenbach about "*From (Security) Protocol to Enterprise Network Infrastructure (Security) Analysis*". The detailed program is provided on the next page. These workshop proceedings incorporate a full paper or a short abstract for each talk.

We would like to thank several people who helped us in the organization of this workshop. First of all, many thanks to Wolfgang Lorenz and Signe Schelske, the coordinators for the project "Recherches sans frontières/Forschen ohne Grenzen", for their organizational and financial support. Many thanks also to Uta Merkle and their team for setting up the workshop environment and ensuring it to run smoothly. Last but not least, many thanks to all authors who submitted talks and to all active participants at the workshop.

Serge Autexier
Stephan Merz
Leon van der Torre
Reinhard Wilhelm
Pierre Wolper

INTERREG IIIC/e-Bird
Workshop "Trustworthy Software" 2006
http://drops.dagstuhl.de/opus/volltexte/2006/693

Program

Session 1: Specification

Ina Schaefer	*Semantic-Based Modeling of Embedded Adaptive System*
Arnaud Lanoix	*An Operator-based Approach to Incremental Development of Conform UML 2.0 Protocol State Machines*
Axel Legay	*On the Implementation of a Game-based Model for Specifying Open Systems*
Julien Schmaltz	*Formalizing On Chip Communications in a Functional Style*

Session 2: Verification I

Joerg Bauer	*Analysis of Dynamic Communicating Systems by Hierarchical Abstraction*
Sebastien Varrette	*Applicative Solutions for Safe Computations in Distributed Environments*
Klaus Dräger	*Generation of linear synchronization invariants*

Session 3: Verification II

Antoine Reilles	*Formal Validation of Pattern Matching Code*
Jan Schwinghammer	*Separation Logic for General Storage*
Jan Reineke	*Shape Analysis of Sets*
Björn Wachter	*Explaining Data Type Reduction in the Shape Analysis Framework*

Session 4: Invited Talk

Christoph Weidenbach	*From (Security) Protocol to Enterprise Network Infrastructure (Security) Analysis*

Session 5: Verification III

Jan Dörrenbächer	*Formal Model and Verification of a Microkernel*
Thomas Hillenbrand	*Processor Datapath Verification with SPASS*
Jean-François Couchot	*Superposition Based Verification of Invariants. Application to Parameterized Systems.*
Artem Starostin	*Formally Verified Data Structures Library for C. The String Data Structure.*

Session 6: Security

Stephan Neuhaus	*Isolating Intrusions by Automatic Experiments*
Michael Hilker	*Security Analysis in Internet Traffic through Artificial Immune Systems*
Stefan Mandel	*Heuristics-based Source Code Analysis for Security Vulnerabilities*

Session 7: Privacy, Secrecy & Trust

J. Paul Gibson	*Trust and security in e-voting systems: the verification problem*
Eugen Zalinescu	*When reachability-based secrecy implies equivalence-based secrecy in security protocols*
Mathieu Turuani	*The CL-Atse Protocol Analyser*