Lecture Notes in Computer Science 6993

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Sebastian Mödersheim
Catuscia Palamidessi (Eds.)

Theory of Security and Applications

Joint Workshop, TOSCA 2011
Saarbrücken, Germany, March 31 - April 1, 2011
Revised Selected Papers

Springer

Volume Editors

Sebastian A. Mödersheim
DTU Informatics
Richard Petersens Plads
2800 Kgs. Lyngby, Denmark
E-mail: samo@imm.dtu.dk

Catuscia Palamidessi
INRIA / Ecole Polytechnique
Rue de Saclay
91128 Palaiseau Cedex, France
E-mail: catuscia@lix.polytechnique.fr

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-27374-2 e-ISBN 978-3-642-27375-9
DOI 10.1007/978-3-642-27375-9
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011943626

CR Subject Classification (1998): D.4.6, K.6.5, C.2, E.3, D.2, F.3

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

It is our pleasure to welcome you to the proceedings of TOSCA 2011, a meeting on the Theory of SeCurity and Applications that was held in Saarbrücken from March 31 to April 1, 2011, in conjunction with ETAPS 2011.

TOSCA is the 2011 edition of an annual series of events formerly known as ARSPA-WITS. The aim of TOSCA is to provide a forum for continued activity in different areas of computer security, bringing computer security researchers in closer contact with the ETAPS community and giving ETAPS attendees an opportunity to talk to experts in computer security, on the one hand, and contribute to bridging the gap between logical methods and computer security foundations, on the other.

ARSPA (Automated Reasoning for Security Protocol Analysis) was a series of workshops aiming at bringing together researchers and practitioners from both the security and the formal methods communities, from academia and industry, interested in developing and applying automated reasoning techniques and tools for the formal specification and analysis of security protocols. The first two ARSPA workshops were held as satellite events of IJCAR 2004 and ICALP 2005, respectively. ARSPA then joined forces with the workshop FCS (Foundations of Computer Security): FCS-ARSPA 2006 was affiliated with LICS 2006, in the context of FLoC 2006, and FCS-ARSPA 2007 was affiliated with LICS 2007 and ICALP 2007.

WITS (Workshop on Issues in the Theory of Security) was the official annual event organized by the IFIP WG 1.7 on "Theoretical Foundations of Security Analysis and Design," established to encourage the investigation on the theoretical foundations of security, by discovering and promoting new areas of application of theoretical techniques in computer security and by supporting the systematic use of formal techniques in the development of security-related applications.

In 2008, ARSPA and WITS joined with FCS for a joint workshop – FCS-ARSPA-WITS 2008 – associated with LICS and CSF. In 2009, ARSPA and WITS merged in the joint workshop ARSPA-WITS which has been associated with ETAPS since then.

Starting from next year, TOSCA will also join forces with the workshops FAST (Formal Aspects of Security & Trust) and SecCo (Security Issues in Concurrency) to form the new sixth ETAPS conference *POST: Principles of Security and Trust*, and we wish this new conference great success.

In the 2011 edition of TOSCA there were 24 submissions. All the submissions were thoroughly evaluated on the basis of at least three referee reports, and an electronic Program Committee meeting was held by using the EasyChair on-line conference system. The committee decided to accept the nine papers included in this volume. The program was enriched with invited talks by Michael

Backes (ETAPS plenary speaker), Veronique Cortier, Ueli Maurer, Sjouke Mauw, and David Sands. We are delighted that Michael Backes and Ueli Maurer have presented novel results and have contributed full papers to this volume.

We would like to thank all the people who contributed to the organization of TOSCA. In particular, we are very grateful to the members of the Program Committee and the additional referees. Last but not least, warm thanks to the organizers of ETAPS 2011.

July 2011

Sebastian Mödersheim
Catuscia Palamidessi

Organization

Program Committee

Alessandro Armando	Università di Genova & Fondazione Bruno Kessler, Italy
Lujo Bauer	CMU, USA
Achim D. Brucker	SAP Research, Germany
Yannick Chevalier	Université de Toulouse, France
Luca Compagna	SAP Research, France
Cas Cremers	Siemens AG, Germany
Jorge Cuellar	ETH Zrich, Switzerland
Pierpaolo Degano	Università di Pisa, Italy
Riccardo Focardi	Università Ca' Foscari di Venezia
Dieter Gollman	Hamburg University of Technology, Germany
Joshua Guttman	Worcester Polytechnic Institute, USA
Jan Jürjens	TU Dortmund and Fraunhofer ISST, Germany
Gavin Lowe	Oxford University, UK
Catherine Meadows	Naval Research Laboratory, USA
John Mitchell	Stanford University, USA
Sebastian Alexander Mödersheim (Chair)	Technical University of Denmark
Catuscia Palamidessi (Chair)	INRIA and LIX, France
Michael Rusinowitch	INRIA-Lorraine, France
Mark Ryan	University of Birmingham, UK
Geoffrey Smith	Florida International University, USA
Graham Steel	LSV, INRIA & CNRS & ENS-Cachan, France
Luca Viganò	Università di Verona, Italy
Bogdan Warinschi	University of Bristol, UK

Additional Reviewers

Misha Aizatulin
Chiara Bodei
Mario Bravetti
Roberto Carbone
Matteo Centenaro
Morten Dahl
Gian-Luigi Ferrari
Martin Ochoa
Giancarlo Pellegrino
Serena Ponta
Silvio Ranise
Ben Smyth
Roberto Zunino

Table of Contents