

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Sjouke Mauw
Christian Damsgaard Jensen (Eds.)

Security and Trust Management

10th International Workshop, STM 2014
Wroclaw, Poland, September 10-11, 2014
Proceedings

Volume Editors

Sjouke Mauw
University of Luxembourg
Luxembourg
E-mail: sjouke.mauw@uni.lu

Christian Damsgaard Jensen
Technical University of Denmark
Lyngby, Denmark
E-mail: christian.jensen@imm.dtu.dk

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-319-11850-5

e-ISBN 978-3-319-11851-2

DOI 10.1007/978-3-319-11851-2

Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014949608

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer International Publishing Switzerland 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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

These are the proceedings of the 10th International Workshop on Security and Trust Management (STM 2014). They mark the second lustrum of a workshop series that started in 2005 with the foundation of the ERCIM Security and Trust Management group. This is a Working Group of the European Research Consortium in Informatics and Mathematics (ERCIM) with the aim of providing a platform for researchers to present and discuss their ideas and foster cooperation. One of the means to achieve these goals is the organization of the annual STM workshop. This year's workshop was held during September 10–11, 2014, in conjunction with the 19th European Symposium on Research in Computer Security (ESORICS 2014) in Wrocław, Poland.

The STM 2014 workshop received 29 submissions that were evaluated on the basis of their significance, novelty, technical quality, and appropriateness to the STM audience. After intensive reviewing and electronic discussions, 11 papers were selected for presentation at the workshop, giving an acceptance rate of less than 38%. In addition, the Program Committee selected six short papers, based on their potential to initiate interesting discussions or to highlight novel research directions.

As in previous editions, the program of the STM 2014 workshop also featured a talk by the winner of the ERCIM-STM best PhD thesis award, Juraj Somorovsky, for his thesis entitled “On the Insecurity of XML Security.”

We would like to thank all the people who volunteered their time and energy to make this year's workshop happen. In particular, we thank the authors for submitting their manuscripts to the workshop and all the attendees for contributing to the workshop discussions. We are also grateful to the members of the Program Committee and the external reviewers for their work in reviewing and discussing the submissions, and their commitment to meeting the strict deadlines. Last but not least, our thanks also go to all the people who played a role in the organization of the event: Pierangela Samarati (chair of the STM working group) for her energy, support, and the many useful pieces of advice; Mirosław Kutylowski, Jaideep Vaidya, and Giovanni Livraga (co-chairs and publicity chair of ESORICS 2014) for their support; Piotr Kordy for managing the STM 2014 website; and Rolando Trujillo Rasua for taking care of the publicity of the workshop.

August 2014

Sjouke Mauw
Christian Damsgaard Jensen

Organization

STM (Security and Trust Management) is a working group of ERCIM (European Research Consortium in Informatics and Mathematics).

Program Chairs

Sjouke Mauw	University of Luxembourg, Luxembourg
Christian Damsgaard Jensen	Technical University of Denmark, Denmark

Publicity Chair

Rolando Trujillo Rasua	University of Luxembourg, Luxembourg
------------------------	--------------------------------------

Web Chair

Piotr Kordy	University of Luxembourg, Luxembourg
-------------	--------------------------------------

STM Steering Committee

Theo Dimitrakos	British Telecom, UK
Javier Lopez	University of Malaga, Spain
Fabio Martinelli	IIT - CNR, Italy
Sjouke Mauw	University of Luxembourg, Luxembourg
Stig F. Mjølnsnes	Norwegian University of Science and Technology, Norway
Pierangela Samarati (Chair)	Università degli Studi di Milano, Italy
Babak Sadighi	Axiomatics AB, Sweden
Ulrich Ultes-Nitsche	University of Fribourg, Switzerland

Program Committee

Rafael Accorsi	University of Freiburg, Germany
Gildas Avoine	IRISA Rennes, France
Cas Cremers	University of Oxford, UK
Jorge Cuellar	Siemens AG, Germany
Christian Damsgaard Jensen	Technical University of Denmark, Denmark
Sabrina De Capitani Di Vimercati	Università degli Studi di Milano, Italy
Roberto Di Pietro	Bell Labs, France
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain

VIII Organization

Carmen Fernández-Gago	University of Malaga, Spain
Simone Fischer-Hübner	Karlstad University, Sweden
Sara Foresti	Università degli Studi di Milano, Italy
Sascha Hauke	Technische Universität Darmstadt, Germany
Michael Huth	Imperial College London, UK
Bart Jacobs	Radboud University Nijmegen, The Netherlands
Martin Johns	SAP Research, UK
Günter Karjoth	Lucerne University of Applied Sciences and Arts, Switzerland
Dogan Kesdogan	Universität Regensburg, Germany
Marek Klonowski	Wroclaw University of Technology, Poland
Yang Liu	Nanyang Technological University, Singapore
Giovanni Livraga	Università degli Studi di Milano, Italy
Javier Lopez	University of Malaga, Spain
Fabio Martinelli	IIT-CNR, Italy
Sjouke Mauw	University of Luxembourg, Luxembourg
Catherine Meadows	Naval Research Laboratory, USA
Silvio Ranise	Fondazione Bruno Kessler, Italy
Michael Rusinowitch	Inria Nancy-Grand Est, France
Pierangela Samarati	Università degli Studi di Milano, Italy
Jan-Philipp Steghöfer	Augsburg University, Germany
Rolando Trujillo Rasua	University of Luxembourg, Luxembourg
Jie Zhang	Nanyang Technological University, Singapore

Additional Reviewers

Cristina Alcaraz	Leanid Krautsevich
Clara Bertolissi	Aliaksandr Lazouski
Vincent Cheval	Francisco Moyano
Yannick Chevalier	Simone Mutti
Alessio Coletta	Tobias Müller
Florian Hahn	Saša Radomirović
Sara Hajian	Albert Sabaté
Roger Jardí	Giada Sciarretta
Ravi Jhawar	Santiago Suppan
Markus Karwe	Mathieu Turuani
Barbara Kordy	

Table of Contents

Integrating Trust and Economic Theories with Knowledge Science for Dependable Service Automation	1
<i>Vangalur Alagar and Kaiyu Wan</i>	
Privacy Architectures: Reasoning about Data Minimisation and Integrity	17
<i>Thibaud Antignac and Daniel Le Métayer</i>	
Monotonicity and Completeness in Attribute-Based Access Control	33
<i>Jason Crampton and Charles Morisset</i>	
Caching and Auditing in the RPPM Model	49
<i>Jason Crampton and James Sellwood</i>	
BlueWallet: The Secure Bitcoin Wallet	65
<i>Tobias Bamert, Christian Decker, Roger Wattenhofer, and Samuel Welten</i>	
Ensuring Secure Non-interference of Programs by Game Semantics	81
<i>Aleksandar S. Dimovski</i>	
Stateful Usage Control for Android Mobile Devices	97
<i>Aliaksandr Lazouski, Fabio Martinelli, Paolo Mori, and Andrea Saracino</i>	
A Formal Model for Soft Enforcement: Influencing the Decision-Maker	113
<i>Charles Morisset, Iryna Yevseyeva, Thomas Groß, and Aad van Moorsel</i>	
Using Prediction Markets to Hedge Information Security Risks	129
<i>Pankaj Pandey and Einar Arthur Snekkenes</i>	
ALPS: An Action Language for Policy Specification and Automated Safety Analysis	146
<i>Silvio Ranise and Riccardo Traverso</i>	
A Formal Definition of Protocol Indistinguishability and Its Verification Using Maude-NPA	162
<i>Sonia Santiago, Santiago Escobar, Catherine Meadows, and José Meseguer</i>	

Short Papers

Hybrid Enforcement of Category-Based Access Control	178
<i>Asad Ali and Maribel Fernández</i>	
Lime: Data Lineage in the Malicious Environment	183
<i>Michael Backes, Niklas Grimm, and Aniket Kate</i>	
NoPhish: An Anti-Phishing Education App	188
<i>Gamze Canova, Melanie Volkamer, Clemens Bergmann, and Roland Borza</i>	
ROMEo: ReputatiOn Model Enhancing OpenID Simulator	193
<i>Ginés Dólera Tormo, Félix Gómez Mármol, and Gregorio Martínez Pérez</i>	
Evaluation of Key Management Schemes in Wireless Sensor Networks	198
<i>Filip Jurnečka, Martin Stehlík, and Vashek Matyáš</i>	
Efficient Java Code Generation of Security Protocols Specified in <i>AnB/AnBx</i>	204
<i>Paolo Modesti</i>	
Author Index	209