

*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*

Madhu Sudan

*Microsoft Research, Cambridge, MA, USA*

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*

Catherine Meadows  
Carmen Fernandez-Gago (Eds.)

# Security and Trust Management

7th International Workshop, STM 2011  
Copenhagen, Denmark, June 27-28, 2011  
Revised Selected Papers

Volume Editors

Catherine Meadows

Naval Research Laboratory, Code 5543  
4555 Overlook Ave, S. W., Washington DC 20375, USA  
E-mail: meadows@itd.nrl.navy.mil

Carmen Fernandez-Gago

University of Malaga, Department of Computer Science  
Campus de Teatinos, 29071 Málaga, Spain  
E-mail: mcgago@lcc.uma.es

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-29962-9

e-ISBN 978-3-642-29963-6

DOI 10.1007/978-3-642-29963-6

Springer Heidelberg Dordrecht London New York

Library of Congress Control: 2012936295

CR Subject Classification (1998): K.6.5, K.4.4, E.3, D.4.6, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2012

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. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, 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.

*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](http://www.springer.com))

# Preface

This volume contains the papers presented at STM 11: 7th International Workshop on Security and Trust Management held during June 27–28, 2011, in Copenhagen, Denmark.

There were 33 submissions. Each submission was reviewed by at least 3, and on average 3.9, Program Committee members. The Committee decided to accept 12 papers, yielding an acceptance rate of approximately 35%. The program also includes 4 invited papers from the two invited speakers and the participants on the panel.

STM is a working group of ERCIM (European Research Consortium in Informatics and Mathematics), and was established in 2005 to provide a platform for researchers in security and trust management to present and discuss their work and to foster cooperation. One of the means to achieve these goals is the organization of a yearly workshop.

There is a long list of people who volunteered their time and energy to put together this workshop and who deserve acknowledgement. We would like to thank the Program Committee and the external reviewers for all their hard work in evaluating and discussing papers, often under intense time pressure. We are also grateful to the STM Organizers, Christian Damsgaard Jensen and Aljosa Pasic, whose work made this meeting possible. We would also like to thank Javier Lopez, the head of the Security and Trust Management Working Group of the European Research Consortium for Informatics and Mathematics, which sponsors STM. He went out of his way to support the workshop and our work in attracting papers and dealing with publishers.

Last but not least, our thanks go to all the authors who submitted papers, and to all the attendees, without whom this workshop would not have taken place. We hope that you find the proceedings stimulating.

January 2012

Catherine Meadows  
Carmen Fernández-Gago

# Organization

## Program Committee

Rafael Accorsi	University of Freiburg, Germany
Isaac Agudo	University of Malaga, Spain
Alessandro Armando	DIST - University of Genova, Italy
Lujo Bauer	Carnegie Mellon University, USA
Jim Clarke	Waterford Institute of Technology, Ireland
Jason Crampton	Royal Holloway, University of London, UK
Jorge Cuellar	Siemens AG, CT IC 3, Germany
Christian Damsgaard Jensen	Technical University of Denmark
Sabrina De Capitani	Università degli Studi di Milano, Italy
Maribel Fernandez	King's College London, UK
Carmen Fernández-Gago	University of Malaga, Spain
Simone Fischer-Huebner	Karlstad University, Sweden
Simon Foley	University College Cork, Ireland
Michael Huth	Imperial College London, UK
Sushil Jajodia	George Mason University, USA
Martin Johns	SAP Research - CEC Karlsruhe, Germany
Aaron Johnson	Yale University, USA
Gunter Karjoth	IBM, Switzerland
Costas Lambrinoudakis	University of Piraeus, Greece
Ninghui Li	Purdue University, USA
Javier Lopez	University of Malaga, Spain
Volkmar Lotz	SAP AG, Germany
Fabio Martinelli	IIT-CNR, Italy
Sjouke Mauw	University of Luxembourg, Belgium
Catherine Meadows	NRL, USA
Stig F. Mjolsnes	Norwegian University of Science and Technology NTNU, Norway
Aljosa Pasic	Atos Origin, Spain
Dusko Pavlovic	Royal Holloway, Oxford, and Twente, UK / The Netherlands
Gunter Pernul	Universität Regensburg, Germany
Alex Pretschner	Karlsruhe Institute of Technology (KIT), Germany
Pierangela Samarati	Università degli Studi di Milano, Italy
Ketil Stoelen	SINTEF, Norway

## Additional Reviewers

Arnaud, Mathilde  
Berthold, Stefan  
Bier, Christoph  
Broser, Christian  
Brucker, Achim D.  
Carbone, Roberto  
Costa, Gabriele  
Darra, Eleni  
Dong, Naipeng  
Drogkaris, Prokopios  
Dürbeck, Stefan  
Erdogan, Gencer  
Havaldsrud, Tormod  
Kelbert, Florian  
Kumari, Prachi

Lehmann, Anja  
Ligaarden, Olav S.  
Lowis, Lutz  
Matteucci, Ilaria  
Merlo, Alessio  
Muller, Tim  
Nantes Sobrinho, Daniele  
Netter, Michael  
Neven, Gregory  
Ranise, Silvio  
Rekleitis, Evangelos  
Riesner, Moritz  
Wonnemann, Claus  
Zhang, Ge

# Table of Contents

Uncertainty, Subjectivity, Trust and Risk: How It All Fits together . . . . .	1
<i>Bjørnar Solhaug and Ketil Stølen</i>	
Trust Extortion on the Internet . . . . .	6
<i>Audun Jøsang</i>	
Trust Areas: A Security Paradigm for the Future Internet . . . . .	22
<i>Carsten Rudolph</i>	
Non-standards for Trust: Foreground Trust and Second Thoughts for Mobile Security . . . . .	28
<i>Stephen Marsh, Sylvie Noël, Tim Storer, Yao Wang, Pam Briggs, Lewis Robart, John Stewart, Babak Esfandiari, Khalil El-Khatib, Mehmet Vefa Bicakci, Manh Cuong Dao, Michael Cohen, and Daniel Da Silva</i>	
A Proof-Carrying File System with Revocable and Use-Once Certificates . . . . .	40
<i>Jamie Morgenstern, Deepak Garg, and Frank Pfenning</i>	
New Modalities for Access Control Logics: Permission, Control and Ratification . . . . .	56
<i>Valerio Genovese and Deepak Garg</i>	
Security Notions of Biometric Remote Authentication Revisited . . . . .	72
<i>Neyire Deniz Sarier</i>	
Hiding the Policy in Cryptographic Access Control . . . . .	90
<i>Sascha Müller and Stefan Katzenbeisser</i>	
Location Privacy in Relation to Trusted Peers . . . . .	106
<i>Klaus Rechert and Benjamin Greschbach</i>	
Fairness in Non-Repudiation Protocols . . . . .	122
<i>Wojciech Jamroga, Sjouke Maww, and Matthijs Melissen</i>	
Risk-Aware Role-Based Access Control . . . . .	140
<i>Liang Chen and Jason Crampton</i>	
Automated Analysis of Infinite State Workflows with Access Control Policies . . . . .	157
<i>Alessandro Armando and Silvio Ranise</i>	

The Role of Data Integrity in EU Digital Signature Legislation — Achieving Statutory Trust for Sanitizable Signature Schemes . . . . .	175
<i>Henrich C. Pöhls and Focke Höhne</i>	
Mutual Remote Attestation: Enabling System Cloning for TPM Based Platforms . . . . .	193
<i>Ulrich Greveler, Benjamin Justus, and Dennis Loehr</i>	
Secure Architecture for the Integration of RFID and Sensors in Personal Networks . . . . .	207
<i>Pablo Najera, Rodrigo Roman, and Javier Lopez</i>	
Accepting Information with a Pinch of Salt: Handling Untrusted Information Sources . . . . .	223
<i>Syed Sadiqur Rahman, Sadie Creese, and Michael Goldsmith</i>	
<b>Author Index</b> . . . . .	239