

*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*

Pierpaolo Degano Sandro Etalle  
Joshua Guttman (Eds.)

# Formal Aspects of Security and Trust

7th International Workshop, FAST 2010  
Pisa, Italy, September 16-17, 2010  
Revised Selected Papers



Springer

## Volume Editors

Pierpaolo Degano  
Università di Pisa, Dipartimento di Informatica  
Largo Bruno Pontecorvo, 3, 56127 Pisa, Italy  
E-mail: degano@di.unipi.it

Sandro Etalle  
Technical University of Eindhoven  
Faculty of Mathematics and Computer Science  
P.O. Box 513, 5600 MB Eindhoven, The Netherlands  
E-mail: s.etalle@tue.nl

Joshua Guttman  
Worcester Polytechnic Institute, Computer Science  
100 Institute Road, Worcester, MA 01609, USA  
E-mail: guttman@wpi.edu

ISSN 0302-9743                                    e-ISSN 1611-3349  
ISBN 978-3-642-19750-5                            e-ISBN 978-3-642-19751-2  
DOI 10.1007/978-3-642-19751-2  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011922329

CR Subject Classification (1998): C.2.0, K.6.5, D.4.6, E.3, K.4.4, H.3-4

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011

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

The present volume contains the proceedings of the seventh international workshop on Formal Aspects of Security and Trust (FAST 2010), held in Pisa, Italy, 16–17 September 2010, as part of the 8th IEEE International Conference on Software Engineering and Formal Methods (SEFM 2010).

FAST aims to foster cooperation among researchers in the areas of security and trust. As computing and network infrastructures become increasingly pervasive, and as they carry increasing economic activity, society needs well-matched security and trust mechanisms. These interactions increasingly span several enterprises and involve loosely structured communities of individuals. Participants involved in these activities must control interactions with their partners based on trust policies and business logic. Trust-based decisions effectively determine the security goals for shared information and for access to sensitive or valuable resources.

FAST sought original papers focusing on formal aspects of the following topics: security and trust policy models; security protocol design and analysis; formal models of trust and reputation; logics for security and trust; distributed trust management systems; trust-based reasoning; digital assets protection; data protection; privacy and ID issues; information flow analysis; language-based security; security and trust aspects of ubiquitous computing; validation/analysis tools; web service security/trust/privacy; GRID security; security risk assessment; and case studies.

The proceedings of this, the seventh FAST workshop, contains a paper by Dusko Pavlovic based on his invited talk. It also comprises 14 revised papers selected out of 42 submissions. Each paper was reviewed by at least three members of the Program Committee, whom we wish to thank for their valuable efforts. We are also grateful to the organizers of SEFM 2010 for having accepted FAST 2010 as an affiliated event and for providing a perfect environment for running the workshop. Last but not least, many thanks to Andrei Voronkov, who allowed us to use the free conference software system EasyChair, which greatly simplified the work of the Program Committee.

December 2010

Pierpaolo Degano  
Sandro Etalle  
Joshua Guttman

# Conference Organization

## Program Chairs

Pierpaolo Degano  
Sandro Etalle  
Joshua Guttman

## Program Committee

Gilles Barthe	IMDEA Software, Spain
Massimo Bartoletti	University of Cagliari, Italy
Lujo Bauer	CMU, USA
Cas Cremers	ETH Zurich, Switzerland
Frédéric Cuppens	Télécom Bretagne, France
Pierpaolo Degano	University of Pisa, Italy (Program Co-chair)
Sandro Etalle, Eindhoven	The Netherlands (Program Co-chair)
Joshua Guttman	Worcester Polytechnic Institute, USA (Program Co-chair)
Chris Hankin	Imperial College London, UK
Bart Jacobs	Radboud University Nijmegen, The Netherlands
Christian Damsgaard Jensen	DTU, Denmark
Fabio Martinelli	CNR, Italy
Sjouke Mauw	University of Luxembourg, Luxembourg
Catherine Meadows	Naval Research Lab, USA
Ron van der Meyden	University of New South Wales, Australia
Mogens Nielsen	Aarhus, Denmark
Dusko Pavlovic	Kestrel Institute, USA, and Oxford, UK
Riccardo Pucella	Northeastern, USA
Peter Ryan	Luxembourg
Steve Schneider	Surrey, UK
Jean-Marc Seigneur	University of Geneva, Switzerland
Luca Viganò	University of Verona, Italy

## Local Organization

Ilaria Matteucci

## External Reviewers

Maurizio Atzori	Wojciech Mostowski
Tom Chothia	Catuscia Palamidessi
David Clark	Alessandra Di Pierro
Gabriele Costa	Jun Pang
Nora Cuppens-Boulahia	Marc Pouly
Stephanie Delaune	Mark Ryan
Hugo Jonker	Wolter Pieters
Gerhard de Koning Gans	Sjaak Smetsers
Pierre Ganty	Xavier Titi
Daniel Hedin	Jan Willemson
Leanid Krautsevich	Simon Winwood
Pascal Lafourcade	Damiano Zanardini
Gabriele Lenzini	Chenyi Zhang
Ilaria Matteucci	Roberto Zunino

# Table of Contents

Quantifying and Qualifying Trust: Spectral Decomposition of Trust Networks (Invited Talk) .... <i>Dusko Pavlovic</i>	1
Bounded Memory Dolev-Yao Adversaries in Collaborative Systems .... <i>Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, and Andre Scedrov</i>	18
Efficient Decision Procedures for Message Deducibility and Static Equivalence .... <i>Bruno Conchinha, David Basin, and Carlos Caleiro</i>	34
Understanding Abstractions of Secure Channels .... <i>Allaa Kamil and Gavin Lowe</i>	50
Information Flow Analysis via Path Condition Refinement .... <i>Mana Taghdiri, Gregor Snelting, and Carsten Sinz</i>	65
Foundations of Attack–Defense Trees .... <i>Barbara Kordy, Sjouke Mauw, Saša Radomirović, and Patrick Schweitzer</i>	80
Reasoning with Past to Prove PKCS#11 Keys Secure .... <i>Sibylle Fröschle and Nils Sommer</i>	96
A Formal Analysis of Authentication in the TPM .... <i>Stéphanie Delaune, Steve Kremer, Mark D. Ryan, and Graham Steel</i>	111
Modeling Identity-Related Properties and Their Privacy Strength .... <i>Meilof Veeningen, Benne de Weger, and Nicola Zannone</i>	126
Semantics of Trust .... <i>Tim Muller</i>	141
Semi-automatic Synthesis of Security Policies by Invariant-Guided Abduction .... <i>Clément Hurlin and Hélène Kirchner</i>	157
Corrective Enforcement of Security Policies.... <i>Raphael Khoury and Nadia Tawbi</i>	176
Cryptographic Enforcement of Role-Based Access Control .... <i>Jason Crampton</i>	191

X        Table of Contents

A Calculus for the Analysis of Wireless Network Security Protocols ....	206
<i>Francesco Ballardin and Massimo Merro</i>	
Analysis of a Receipt-Free Auction Protocol in the Applied Pi Calculus .....	223
<i>Naipeng Dong, Hugo Jonker, and Jun Pang</i>	
<b>Author Index .....</b>	<b>239</b>