Lecture Notes in Computer Science 6561

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

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

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

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

Table of Contents

Quantifying and Qualifying Trust: Spectral Decomposition of Trust Networks (Invited Talk) 1
Dusko Pavlovic

Bounded Memory Dolev-Yao Adversaries in Collaborative Systems 18
Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, and Andre Scedrov

Efficient Decision Procedures for Message Deducibility and Static Equivalence 34
Bruno Conchinha, David Basin, and Carlos Caleiro

Understanding Abstractions of Secure Channels 50
Allaa Kamil and Gavin Lowe

Information Flow Analysis via Path Condition Refinement 65
Mana Taghdiri, Gregor Snelting, and Carsten Sinz

Foundations of Attack–Defense Trees 80
Barbara Kordy, Sjouke Mauw, Saša Radomirović, and Patrick Schweitzer

Reasoning with Past to Prove PKCS#11 Keys Secure 96
Sibylle Fröschle and Nils Sommer

A Formal Analysis of Authentication in the TPM 111
Stéphanie Delaune, Steve Kremer, Mark D. Ryan, and Graham Steel

Modeling Identity-Related Properties and Their Privacy Strength 126
Meilof Veeningen, Benne de Weger, and Nicola Zannone

Semantics of Trust 141
Tim Muller

Semi-automatic Synthesis of Security Policies by Invariant-Guided Abduction 157
Clément Hurlin and Hélène Kirchner

Corrective Enforcement of Security Policies 176
Raphael Khoury and Nadia Tawbi

Cryptographic Enforcement of Role-Based Access Control 191
Jason Crampton

A Calculus for the Analysis of Wireless Network Security Protocols 206
Francesco Ballardin and Massimo Merro

Analysis of a Receipt-Free Auction Protocol in the Applied Pi Calculus 223
Naipeng Dong, Hugo Jonker, and Jun Pang

Author Index 239