

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

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Pierpaolo Degano Joshua Guttman
Fabio Martinelli (Eds.)

Formal Aspects in Security and Trust

5th International Workshop, FAST 2008
Malaga, Spain, October 9-10, 2008
Revised Selected Papers

Volume Editors

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

Joshua Guttman
The MITRE Corporation
202 Burlington Road, Bedford, MA 01730-1420, USA
E-mail: guttman@mitre.org

Fabio Martinelli
Istituto di Informatica e Telematica (IIT)
Consiglio Nazionale delle Ricerche (CNR)
Pisa Research Area, Via G. Moruzzi 1, 56125 Pisa, Italy
E-mail: fabio.martinelli@iit.cnr.it

Library of Congress Control Number: Applied for

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-642-01464-X Springer Berlin Heidelberg New York
ISBN-13	978-3-642-01464-2 Springer Berlin Heidelberg New York

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.

springer.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12654567 06/3180 5 4 3 2 1 0

Preface

The present volume contains the proceedings of the 5th International Workshop on Formal Aspects in Security and Trust (FAST 2008), held in Malaga, Spain, October 9-10, 2008. FAST is an event affiliated with the 13th European Symposium on Research in Computer Security (ESORICS 2008). FAST 2008 was held under the auspices of the IFIP WG 1.7 on Foundations of Security Analysis and Design.

The 5th International Workshop on Formal Aspects in Security and Trust (FAST 2008) aimed at continuing the successful effort of the previous three FAST workshop editions for fostering the 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 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 for original papers focusing on formal aspects in: 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 in ubiquitous computing; validation/analysis tools; Web service security/trust/privacy; GRID security; security risk assessment; case studies.

The proceedings consist of an invited paper by Gilles Barthe and 20 revised papers selected out of 59 submissions. Each paper was reviewed by at least three members of the Program Committee (PC).

We wish to thank the the PC members for their valuable efforts in properly evaluating the submissions, and the ESORICS 2008 organizers for accepting FAST as an affiliated event and for providing a perfect environment for running the workshop.

October 2008

Pierpaolo Degano
Joshua Guttman
Fabio Martinelli

Organization

Program Chairs

Pierpaolo Degano
Joshua Guttman
Fabio Martinelli

Program Committee

Gilles Barthe
Frederic Cuppens
Theo Dimitrakos
Roberto Gorrieri
Masami Hagiya
Chris Hankin
Christian Jensen
Audun Josang
Yuecel Karabulut
Igor Kotenko
Ninghui Li
Javier Lopez
Steve Marsh
Catherine Meadows
Mogens Nielsen
Flemming Nielson
Indrajit Ray
Peter Ryan
Steve Schneider
Jean-Marc Seigneur
Vitaly Shmatikov
Ketil Stoelen
William Winsborough
Ron van der Meyden

External Reviewers

Aldini, Alessandro
Autrel, Fabien
Ben Ghorbel, Meriam
Bodei, Chiara
Bouzida, Yacine
Bravetti, Mario
Bucur, Doina
Cederquist, Jan
Costa, Gabriele
Crafa, Silvia
Cuppens, Nora
Durante, Luca
Garcia-Alfaro, Joaquin
Guidi, Claudio
Hoa, Feng
Kawamoto, Yusuke
Koutny, Maciej
Liu, Alex
Lund, Mass Soldal
Luo, Zhengqin
Maillé, Patrick
Matos, Ana
Matteucci, Ilaria
Mazzara, Manuel
Nadales, Damian
Pacalet, Anne
Petri, Gustavo
Piazza, Carla
Refsdal, Atle
Riis Nielson, Hanne
Rossi, Sabina
Sakurada, Hideki
Seehusen, Fredrik
Takahashi, Koichi
Tishkov, Artem
Toahchoodee, Manachai
Xia, Zhe
Zanella Beguelin, Santiago

Table of Contents

Formal Certification of ElGamal Encryption: A Gentle Introduction to CertiCrypt	1
<i>Gilles Barthe, Benjamin Grégoire, Sylvain Heraud, and Santiago Zanella Béguelin</i>	
Secure Information Flow as a Safety Property	20
<i>Gérard Boudol</i>	
Who Can Declassify?	35
<i>Alexander Lux and Heiko Mantel</i>	
Non-Interference for Deterministic Interactive Programs	50
<i>David Clark and Sebastian Hunt</i>	
Information-Theoretic Modeling and Analysis of Interrupt-Related Covert Channels	67
<i>Heiko Mantel and Henning Sudbrock</i>	
Causality and Accountability	82
<i>Dominic Duggan and Ye Wu</i>	
Dynamics, Robustness and Fragility of Trust	97
<i>Dusko Pavlovic</i>	
Trust within the Context of Organizations: A Formal Approach	114
<i>Emiliano Lorini, Rino Falcone, and Cristiano Castelfranchi</i>	
Know What You Trust: Analyzing and Designing Trust Policies with Scoll	129
<i>Fred Spiessens, Jerry den Hartog, and Sandro Etalle</i>	
Privacy-Friendly Electronic Traffic Pricing via Commits	143
<i>Wiebren de Jonge and Bart Jacobs</i>	
A Formal Privacy Management Framework	162
<i>Daniel Le Métayer</i>	
Parameterised Anonymity	177
<i>Jan Friso Groote and Simona Orzan</i>	
Automatic Methods for Analyzing Non-repudiation Protocols with an Active Intruder	192
<i>Francis Klay and Laurent Vigneron</i>	

Petri Net Security Checker: Structural Non-interference at Work	210
<i>Simone Frau, Roberto Gorrieri, and Carlo Ferigato</i>	
Verifying Multi-party Authentication Using Rank Functions and PVS.	226
<i>Rob Verhoeven and Francien Dechesne</i>	
The Append-Only Web Bulletin Board	242
<i>James Heather and David Lundin</i>	
Secure Broadcast Ambients	257
<i>Elsa L. Gunter and Ayesha Yasmeeen</i>	
Extending Anticipation Games with Location, Penalty and Timeline . . .	272
<i>Elie Bursztein</i>	
Do You Really Mean What You Actually Enforced? Edit Automata Revisited	287
<i>Nataliia Bielova and Fabio Massacci</i>	
Delegating Privileges over Finite Resources: A Quota Based Delegation Approach	302
<i>Isaac Agudo, Carmen Fernandez-Gago, and Javier Lopez</i>	
Access Control and Information Flow in Transactional Memory	316
<i>Ariel Cohen, Ron van der Meyden, and Lenore D. Zuck</i>	
Author Index	331