

*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*

Gilles Barthe Anupam Datta  
Sandro Etalle (Eds.)

# Formal Aspects of Security and Trust

8th International Workshop, FAST 2011  
Leuven, Belgium, September 12-14, 2011  
Revised Selected Papers

Volume Editors

Gilles Barthe  
Universidad Politecnica de Madrid  
IMDEA Software Institute  
Campus Montegancedo  
28660 Boadilla del Monte, Madrid, Spain  
E-mail: gilles.barthe@imdea.org

Anupam Datta  
Carnegie Mellon University  
NASA Research Park, Bldg. 23 (MS 23-11)  
P.O. Box 1  
Moffet Field, CA 94035-0001, USA  
E-mail: danupam@cmu.edu

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

ISSN 0302-9743 e-ISSN 1611-3349  
ISBN 978-3-642-29419-8 e-ISBN 978-3-642-29420-4  
DOI 10.1007/978-3-642-29420-4  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012934839

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

# Preface

The present volume contains the proceedings of the 8th International Workshop on Formal Aspects of Security and Trust (FAST 2011), held in Leuven, Belgium, September 12–14, 2011, in co-location with the 16th European Symposium on Research in Computer Security (ESORICS).

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 Program Committee of FAST 2011 received 42 submissions in response to the Call for Papers. Our warmest thanks go to all the authors of submitted papers for sending their work to the conference. Each paper was reviewed by three members of the Program Committee; we thank all the external reviewers for their valuable efforts. Based on the review reports and electronic discussions, the Program Committee selected 15 papers for inclusion in the proceedings.

The proceedings contain revised versions of these 15 accepted papers, and two papers that accompany invited lectures by Andrew D. Gordon (Microsoft Research and University of Edinburgh), and Frank Piessens (Katholieke Universiteit Leuven).

We are grateful to the invited speakers for accepting to address the conference, and to the members of the Program Committee for their assistance in the paper selection. We are also grateful to the local organizers of ESORICS 2011 for providing a perfect environment for running the workshop, and to Andrei Voronkov for his EasyChair system.

November 2011

Gilles Barthe  
Anupam Datta  
Sandro Etalle

# Organization

## Program Committee

Gilles Barthe	IMDEA Software Institute, Spain
Konstantinos Chatzikokolakis	CNRS and Ecole Polytechnique, France
Stephen Chong	Harvard University, USA
Michael Clarkson	George Washington University, USA
Ricardo Corin	Universidad Nacional de Córdoba, Argentina
Cas Cremers	ETH Zurich, Switzerland
Anupam Datta	Carnegie Mellon University, USA
Sandro Etalle	T.U. Eindhoven and University of Twente, The Netherlands
Cédric Fournet	Microsoft Research, USA
Deepak Garg	Carnegie Mellon University, USA
Peter Herrmann	NTNU Trondheim, Norway
Bart Jacobs	Radboud University Nijmegen, The Netherlands
Christian Damsgaard Jensen	Technical University of Denmark, Denmark
Steve Kremer	LSV, ENS Cachan, CNRS, INRIA, France
Fabio Martinelli	IIT-CNR, Italy
Fabio Massacci	University of Trento, Italy
Sjouke Mauw	University of Luxembourg, Luxembourg
Ron van der Meyden	University of New South Wales, Australia
Mogens Nielsen	BRICS, University of Aarhus, Denmark
Mark Ryan	University of Birmingham, UK
Luca Viganò	University of Verona, Italy

## Additional Reviewers

Alvim, Mario S.	Harvan, Matus
Barletta, Michele	Huisman, Marieke
Bielova, Nataliia	Jeffrey, Alan
Bursuc, Sergiu	Koleini, Masoud
Clavel, Manuel	Kordy, Barbara
Costa, Gabriele	Koshutanski, Hristo
De Ruiter, Joeri	Kunemann, Robert
Dechesne, Francien	Lee, Matías D.
Delaune, Stephanie	Li, Ninghui
Gadyatskaya, Olga	Manzano, Felipe
Garcia, Flavio D.	Matteucci, Ilaria

VIII Organization

Melissen, Matthijs  
Mödersheim, Sebastian  
Paci, Federica  
Pagano, Miguel  
Pang, Jun  
Radomirović, Saša  
Ramanujam, R.  
Samardjiska, Simona

Schmidt, Benedikt  
Shkaravska, Olha  
Su, Kaile  
Torabi Dashti, Mohammad  
Ullman, Jonathan  
Van Deursen, Ton  
Verdult, Roel  
Yautsiukhin, Artsiom

# Table of Contents

Verifying Cryptographic Code in C: Some Experience and the Csec Challenge . . . . .	1
<i>Mihhail Aizatulin, François Dupressoir, Andrew D. Gordon, and Jan Jürjens</i>	
Better Security and Privacy for Web Browsers: A Survey of Techniques, and a New Implementation . . . . .	21
<i>Willem De Groef, Dominique Devriese, and Frank Piessens</i>	
Differential Privacy: On the Trade-Off between Utility and Information Leakage . . . . .	39
<i>Mário S. Alvim, Miguel E. Andrés, Konstantinos Chatzikokolakis, Pierpaolo Degano, and Catuscia Palamidessi</i>	
On-the-Fly Inlining of Dynamic Dependency Monitors for Secure Information Flow . . . . .	55
<i>Luciano Bello and Eduardo Bonelli</i>	
Min-Entropy Leakage of Channels in Cascade . . . . .	70
<i>Barbara Espinoza and Geoffrey Smith</i>	
Secure Recharge of Disposable RFID Tickets . . . . .	85
<i>Riccardo Focardi and Flaminia L. Luccio</i>	
Avoiding Delegation Subterfuge Using Linked Local Permission Names . . . . .	100
<i>Simon N. Foley and Samane Abdi</i>	
Verifiable Control Flow Policies for Java Bytecode . . . . .	115
<i>Arnaud Fontaine, Samuel Hym, and Isabelle Simplot-Ryl</i>	
Concepts and Proofs for Configuring PKCS#11 . . . . .	131
<i>Sibylle Fröschle and Nils Sommer</i>	
Service Automata . . . . .	148
<i>Richard Gay, Heiko Mantel, and Barbara Sprick</i>	
Analysing Applications Layered on Unilaterally Authenticating Protocols . . . . .	164
<i>Thomas Gibson-Robinson and Gavin Lowe</i>	
Type-Based Enforcement of Secure Programming Guidelines — Code Injection Prevention at SAP . . . . .	182
<i>Robert Grabowski, Martin Hofmann, and Keqin Li</i>	

TBA : A Hybrid of Logic and Extensional Access Control Systems . . . . .	198
<i>Timothy L. Hinrichs, William C. Garrison III, Adam J. Lee, Skip Saunders, and John C. Mitchell</i>	
Diffie-Hellman without Difficulty . . . . .	214
<i>Sebastian Mödersheim</i>	
Is Cryptoc Able to Detect Insider Attacks? . . . . .	230
<i>Behnam Sattarzadeh and Mehran S. Fallah</i>	
Formal Analysis of Anonymity in ECC-Based Direct Anonymous Attestation Schemes . . . . .	245
<i>Ben Smyth, Mark Ryan, and Liqun Chen</i>	
Risk Balance in Optimistic Non-repudiation Protocols . . . . .	263
<i>Mohammad Torabi Dashti, Jan Cederquist, and Yanjing Wang</i>	
<b>Author Index</b> . . . . .	279