Formal Aspects of Security and Trust

8th International Workshop, FAST 2011
Leuven, Belgium, September 12-14, 2011
Revised Selected Papers
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, Nataliai Jeffrey, Alan
Bursuc, Sergiu Koleini, Masoud
Clavel, Manuel Kordy, Barbara
Costa, Gabriele Koshutanski, Hristo
De Ruiter, Joeri Kunnemann, Robert
Dechesne, Francien Lee, Matías D.
Delaune, Stephanie Li, Ninghui
Gadyatskaya, Olga Manzano, Felipe
Garcia, Flavio D. Matteucci, Ilaria
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
Mihhail Aizatulin, François Dupressoir, Andrew D. Gordon, and Jan Jürjens

Better Security and Privacy for Web Browsers: A Survey of Techniques, and a New Implementation ........................................ 21
Willem De Groef, Dominique Devriese, and Frank Piessens

Differential Privacy: On the Trade-Off between Utility and Information Leakage ........................................... 39
Mário S. Alvim, Miguel E. Andrés, Konstantinos Chatzikokolakis, Pierpaolo Degano, and Catuscia Palamidessi

On-the-Fly Inlining of Dynamic Dependency Monitors for Secure Information Flow ........................................... 55
Luciano Bello and Eduardo Bonelli

Min-Entropy Leakage of Channels in Cascade ........................................... 70
Barbara Espinoza and Geoffrey Smith

Secure Recharge of Disposable RFID Tickets ........................................... 85
Riccardo Focardi and Flaminia L. Luccio

Avoiding Delegation Subterfuge Using Linked Local Permission Names ........................................... 100
Simon N. Foley and Samane Abdi

Verifiable Control Flow Policies for Java Bytecode ........................................... 115
Arnaud Fontaine, Samuel Hym, and Isabelle Simplot-Ryl

Concepts and Proofs for Configuring PKCS#11 ........................................... 131
Sibylle Fröschle and Nils Sommer

Service Automata ........................................... 148
Richard Gay, Heiko Mantel, and Barbara Sprick

Analysing Applications Layered on Unilaterally Authenticating Protocols ........................................... 164
Thomas Gibson-Robinson and Gavin Lowe

Type-Based Enforcement of Secure Programming Guidelines — Code Injection Prevention at SAP ........................................... 182
Robert Grabowski, Martin Hofmann, and Kebin Li
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBA: A Hybrid of Logic and Extensional Access Control Systems</td>
<td>198</td>
</tr>
<tr>
<td>Timothy L. Hinrichs, William C. Garrison III, Adam J. Lee, Skip Saunders, and John C. Mitchell</td>
<td></td>
</tr>
<tr>
<td>Diffie-Hellman without Difficulty</td>
<td>214</td>
</tr>
<tr>
<td>Sebastian Mödersheim</td>
<td></td>
</tr>
<tr>
<td>Is Cryptyc Able to Detect Insider Attacks?</td>
<td>230</td>
</tr>
<tr>
<td>Behnam Sattarzadeh and Mehran S. Fallah</td>
<td></td>
</tr>
<tr>
<td>Formal Analysis of Anonymity in ECC-Based Direct Anonymous Attestation Schemes</td>
<td>245</td>
</tr>
<tr>
<td>Ben Smyth, Mark Ryan, and Liqun Chen</td>
<td></td>
</tr>
<tr>
<td>Risk Balance in Optimistic Non-repudiation Protocols</td>
<td>263</td>
</tr>
<tr>
<td>Mohammad Torabi Dashti, Jan Cederquist, and Yanjing Wang</td>
<td></td>
</tr>
</tbody>
</table>

Author Index ........................................................................... 279