

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

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

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Theo Dimitrakos Fabio Martinelli
Peter Y. A. Ryan Steve Schneider (Eds.)

Formal Aspects in Security and Trust

Fourth International Workshop, FAST 2006
Hamilton, Ontario, Canada, August 26-27, 2006
Revised Selected Papers

Volume Editors

Theo Dimitrakos

BT Group Chief Technology Office, Ipswich IP5 3RE, UK

E-mail: Theo.Dimitrakos@bt.com

Fabio Martinelli

National Research Council - C.N.R., Pisa, Italy

E-mail: fabio.martinelli@iit.cnr.it

Peter Y. A. Ryan

University of Newcastle, UK

E-mail: peter.ryan@ncl.ac.uk

Steve Schneider

University of Surrey, UK

E-mail: S.Schneider@surrey.ac.uk

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 3-540-75226-9 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-75226-4 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 is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12164677 06/3180 5 4 3 2 1 0

Preface

The present volume contains the post-proceedings of the 4th International Workshop on Formal Aspects in Security and Trust (FAST2006), held in Hamilton, Ontario, Canada, August 26–27, 2006. FAST is an event affiliated with the Formal Methods 2006 Congress (FM06). FAST 2006 was held under the auspices of the IFIP WG 1.7 on Foundations of Security Analysis and Design.

FAST2006 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. The new challenges offered by the so-called ambient intelligence space, as a future paradigm in the information society, demand for a coherent and rigorous framework of concepts, tools and methodologies to provide users with trust and confidence in the underlying communication/interaction infrastructure. It is necessary to address issues relating to both guaranteeing security of the infrastructure and the perception of the infrastructure being secure. In addition, user confidence in what is happening must be enhanced by developing trust models effectively but that are also easily comprehensible and manageable by users.

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; and case studies.

The FAST2006 post-proceedings collect the revised versions of 18 papers, selected out of 47 submissions. Each paper was reviewed by at least three members of the Program Committee.

We wish to thank the the Program Committee members for their valuable efforts in properly evaluating the submissions, and the FM06 organizers for accepting FAST as an affiliated event and for providing a perfect environment for running the workshop.

Thanks are also due to the Center for Software Reliability (CSR) of Newcastle University and IIT-CNR for sponsoring FAST2006.

February 2007

Theo Dimitrakos
Fabio Martinelli
Peter Y.A. Ryan
Steve Schneider

Organization

Workshop Organizers

Theo Dimitrakos, BT
Fabio Martinelli, IIT-CNR
Peter Y.A. Ryan, University of Newcastle
Steve Schneider, University of Surrey

Invited Speakers

Joshua D. Guttman, MITRE, USA

Program Committee

Gilles Barthe, INRIA Sophia-Antipolis, France
Stefano Bistarelli, University of Pescara, Italy
Gregor v. Bochmann, University of Ottawa, Canada
John A. Clark, University of York, UK
Frédéric Cuppens, ENST Bretagne, France
Roberto Gorrieri, University of Bologna, Italy
Joshua D. Guttman, MITRE, USA
Masami Hagiya, University of Tokyo, Japan
Chris Hankin, Imperial College (London), UK
Christian Jensen, DTU, Denmark
Audun Jøsang, DSTC, Australia
Jan Jürjens, TU München, Germany
Yuecel Karabulut, SAP, Germany
Igor Kottenko, SPIIRAS, Russia
Heiko Krumm, University of Dortmund, Germany
Ninghui Li, Purdue University, USA
Steve Marsh, Institute for Information Technology, NRC, Canada
Catherine Meadows, Naval Research Lab, USA
Ron van der Meyden, University of New South Wales, Australia
Mogens Nielsen, University of Aarhus, Denmark
Flemming Nielson, Danish Technical University, Denmark
Indrajit Ray, Colorado State University, USA
Babak Sadighi Firozabadi, SICS, Sweden
Pierangela Samarati, University of Milan, Italy
Jean-Marc Seigneur, University of Geneva, Switzerland
Paul Syverson, Naval Research Laboratory, USA
Ketil Stolen, SINTEF, Norway
William H. Winsborough, George Mason University, USA

Local Organization

Alessandro Falleni, IIT-CNR

Table of Contents

Strategic Games on Defense Trees	1
<i>Stefano Bistarelli, Marco Dall’Aglio, and Pamela Peretti</i>	
Timed Calculus of Cryptographic Communication	16
<i>Johannes Borgström, Olga Grinchtein, and Simon Kramer</i>	
A Semantic Paradigm for Component-Based Specification Integrating a Notion of Security Risk	31
<i>Gyrd Brændeland and Ketil Stølen</i>	
Game-Based Criterion Partition Applied to Computational Soundness of Adaptive Security	47
<i>M. Daubignard, R. Janvier, Y. Lakhnech, and L. Mazaré</i>	
Measuring Anonymity with Relative Entropy	65
<i>Yuzin Deng, Jun Pang, and Peng Wu</i>	
Formalizing and Analyzing Sender Invariance	80
<i>Paul Hankes Drielsma, Sebastian Mödersheim, Luca Viganò, and David Basin</i>	
From Simulations to Theorems: A Position Paper on Research in the Field of Computational Trust	96
<i>Karl Krukow and Mogens Nielsen</i>	
A Tool for the Synthesis of Controller Programs	112
<i>Ilaria Matteucci</i>	
Where Can an Insider Attack?	127
<i>Christian W. Probst, René Rydhof Hansen, and Flemming Nielson</i>	
Maintaining Information Flow Security Under Refinement and Transformation	143
<i>Fredrik Seehusen and Ketil Stølen</i>	
A Classification of Delegation Schemes for Attribute Authority	158
<i>Ludwig Seitz, Erik Rissanen, and Babak Sadighi</i>	
Program Partitioning Using Dynamic Trust Models	170
<i>Dan Søndergaard, Christian W. Probst, Christian Damsgaard Jensen, and René Rydhof Hansen</i>	
Locality-Based Security Policies	185
<i>Terkel K. Tolstrup, Flemming Nielson, and René Rydhof Hansen</i>	

A Theorem-Proving Approach to Verification of Fair Non-repudiation Protocols	202
<i>Kun Wei and James Heather</i>	
A Formal Specification of the MIDP 2.0 Security Model.....	220
<i>Santiago Zanella Béguelin, Gustavo Betarte, and Carlos Luna</i>	
A Comparison of Semantic Models for Noninterference.....	235
<i>Ron van der Meyden and Chenyi Zhang</i>	
Hiding Information in Multi Level Security Systems	250
<i>Danièle Beauquier and Ruggero Lanotte</i>	
A New Trust Model Based on Advanced D-S Evidence Theory for P2P Networks	270
<i>Chunqi Tian, Shihong Zou, Wendong Wang, and Shiduan Cheng</i>	
Author Index	285