Lecture Notes in Computer Science 3866

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

Editorial Board

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

Formal Aspects in Security and Trust

Third International Workshop, FAST 2005
Newcastle upon Tyne, UK, July 18-19, 2005
Revised Selected Papers

Springer

Volume Editors

Theo Dimitrakos
Security Research Centre
BT Group Chief Technology Office
2A Rigel House, Adastral Park, Martlesham, Ipswich IP5 3RE, UK
E-mail: Theo.Dimitrakos@bt.com

Fabio Martinelli
Istituto di Informatica e Telematica - IIT
National Research Council - C.N.R.
Pisa Research Area, Via G. Moruzzi, Pisa, Italy
E-mail: fabio.martinelli@iit.cnr.it

Peter Y.A. Ryan
University of Newcastle upon Tyne
School of Computing Science
Newcastle upon Tyne, NE1 7RU, UK
E-mail: Peter.Ryan@newcastle.ac.uk

Steve Schneider
University of Surrey
Department of Computing
Guildford, Surrey, GU2 7XH, UK
E-mail: S.Schneider@surrey.ac.uk

Library of Congress Control Number: 2006921788

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 3-540-32628-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-32628-1 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11679219 06/3142 5 4 3 2 1 0

Preface

This volume contains the post-proceedings of the Third International Workshop on Formal Aspects in Security and Trust (FAST 2005), held in Newcastle upon Tyne, July 18-19, 2005. FAST is an event affiliated with the Formal Methods 2005 Congress (FM05).

FAST 2005 aimed at continuing the successful effort of the previous two 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 increase users' trust&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 which are not only effective but also easily comprehensible and manageable by users.

FAST sought 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 etc.

This volume contains revised versions of 17 papers selected out of 37 submissions and the extended abstract of one invited contribution. Each paper was reviewed by at least three members of the international Program Committee (PC).

We wish to thank the PC members for their valuable efforts in properly evaluating the submissions, and the FM05 organizers for accepting FAST as an affiliated event and for providing a perfect environment for running the workshop.

Thanks are also due to BCS-FACS and IIT-CNR for the financial support for FAST 2005.

October 2005

Theo Dimitrakos
Fabio Martinelli
Peter Y.A. Ryan
Steve Schneider
FAST 2005 Co-chairs

Workshop Organization

Workshop Organizers

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

Invited Speakers

Cédric Fournet, Microsoft Research (Cambridge), UK
Brian Randell, University of Newcastle, UK

Program Committee

Elisa Bertino, Purdue University, USA
John A. Clark, University of York, UK
Frédéric Cuppens, ENST Bretagne, France
Rino Falcone, ISTC-CNR, Italy
Simon Foley, University College Cork, Ireland
Roberto Gorrieri, University of Bologna, Italy
Masami Hagiya, University of Tokyo, Japan
Chris Hankin, Imperial College (London), UK
Valerie Issarny, INRIA, France
Christian Jensen, DTU, Denmark
Audun Jøsang, DSTC, Australia
Jan Jürjens, TU München, Germany
Yuecel Karabulut, SAP, Germany
Igor Kotenko, SPIIRAS, Russia
Heiko Krumm, University of Dortmund, Germany
Fabio Massacci, University of Trento, Italy
Stefan Poslad, Queen Mary College, UK
Catherine Meadows, Naval Research Lab, USA
Ron van der Meyden, University of New South Wales, Australia
Andrew Myers, Cornell University, USA
Mogens Nielsen, University of Aarhus, Denmark
Indrajit Ray, Colorado State University, USA
Babak Sadighi Firozabadi, SICS, Sweden
Pierangela Samarati, University of Milan, Italy
Ketil Stølen, SINTEF, Norway
Kymie Tan, Carnegie Mellon University, USA
William H. Winsborough, George Mason University, USA

Local Organization

Alessandro Falleni, IIT-CNR, Italy
Ilaria Matteucci, IIT-CNR, Italy

Table of Contents

Voting Technologies and Trust
Brian Randell, Peter Y.A. Ryan 1

On the Formal Analyses of the Zhou-Gollmann Non-repudiation Protocol
Susan Pancho-Festin, Dieter Gollmann 5

Formal Reasoning About a Specification-Based Intrusion Detection for Dynamic Auto-configuration Protocols in Ad Hoc Networks
Tao Song, Calvin Ko, Chinyang Henry Tseng, Poornima Balasubramanyam, Anant Chaudhary, Karl N. Levitt 16

A Formal Approach for Reasoning About a Class of Diffie-Hellman Protocols
Rob Delicata, Steve Schneider 34

Eliminating Implicit Information Leaks by Transformational Typing and Unification
Boris Köpf, Heiko Mantel 47

Abstract Interpretation to Check Secure Information Flow in Programs with Input-Output Security Annotations
N. De Francesco, L. Martini 63

Opacity Generalised to Transition Systems
Jeremy W. Bryans, Maciej Koutny, Laurent Mazaré, Peter Y.A. Ryan 81

Unifying Decidability Results on Protection Systems Using Simulations
Constantin Enea 96

Proof Obligations Preserving Compilation
Gilles Barthe, Tamara Rezk, Ando Saabas 112

A Logic for Analysing Subterfuge in Delegation Chains
Hongbin Zhou, Simon N. Foley 127

Probable Innocence Revisited
Konstantinos Chatzikokolakis, Catuscia Palamidessi 142

Relative Trustworthiness
Johan W. Klüwer, Arild Waaler 158

Secure Untrusted Binaries — Provably!
Simon Winwood, Manuel M.T. Chakravarty 171

Normative Specification: A Tool for Trust and Security
Olga Pacheco 187

Type-Based Distributed Access Control vs. Untyped Attackers
Tom Chothia, Dominic Duggan 203

A Security Management Information Model Derivation Framework: From Goals to Configurations
R. Laborde, F. Barrère, A. Benzekri 217

On Anonymity with Identity Escrow
Aybek Mukhamedov, Mark D. Ryan 235

Towards Verification of Timed Non-repudiation Protocols
Kun Wei, James Heather 244

Author Index 259