Lecture Notes in Computer Science 4691

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

Springer

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

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: 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 Kotenko, 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