Lecture Notes in Computer Science 7322

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

Ioannis Askoxylakis Henrich C. Pöhls
Joachim Posegga (Eds.)

Information Security Theory and Practice

Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems

6th IFIP WG 11.2 International Workshop, WISTP 2012
Egham, UK, June 20-22, 2012
Proceedings

Springer

Volume Editors

Ioannis Askoxylakis
FORTH-ICS
Vassilika Vouton, P.O. Box 1385, 711 10 Heraklion, Crete, Greece
E-mail: asko@ics.forth.gr

Henrich C. Pöhls
Joachim Posegga
University of Passau, Innstrasse 43, 94032 Passau, Germany
E-mail:{hp, jp}@sec.uni-passau.de

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-30954-0 e-ISBN 978-3-642-30955-7
DOI 10.1007/978-3-642-30955-7
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012939067

CR Subject Classification (1998): E.3, C.2, D.4.6, K.6.5, C.5.3, H.4

LNCS Sublibrary: SL 4 – Security and Cryptology

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

Future ICT technologies, like the concepts of Ambient Intelligence and Internet of Things, provide a vision of the Information Society where the emphasis is on surrounding people by intelligent interactive interfaces and objects and on environments that are capable of recognizing and reacting to the presence of different individuals in a seamless, unobtrusive, and invisible manner. The success of such future ICT technologies will crucially depend on their security properties, how privacy and individuals' rights will be protected, and how much individuals will trust the intelligent world that will surround them and through which they will move.

The 6th Workshop in Information Security Theory and Practice (WISTP 2012) addressed the security, privacy, and trust issues in computing systems and ambient intelligence ecosystems along with evaluating their impact on business, individuals, and society. WISTP 2012 was organized by the Royal Holloway University of London during June 20–22, 2012, in Egham, United Kingdom. The workshop received 36 submissions. Each submission was reviewed by at least three reviewers.

This volume contains the nine full papers and six short papers that were selected for presentation at WISTP 2012. Furthermore, the proceedings include the three keynotes given by Dieter Gollmann, Paul Kearney and Frank Piessens, to whom we are grateful.

There is a long list of people who also devoted their energy and provided active support to the successful organization of the workshop. We are grateful to the members of the Program Committee and the external reviewers for reviewing all submissions and selecting the ones with substantial contribution to the thematic area of the workshop. We gratefully acknowledge everyone involved in the successful organization process: the members of the Steering Committee, Claudio Ardagna, Angelos Bilas, Konstantinos Markantonakis, Jean-Jacques Quisquater, Damien Sauveron and Jianying Zhou for their advice, the General Chairs Gerhard Hancke, Konstantinos Markantonakis and Keith Mayes for their invaluable support in the organization of the workshop, Sara Foresti and Taeshik Shon for their efforts as Publicity Chairs and Emma Dobson for her support in the local organization.

Last but not least we are grateful to the authors for submitting their excellent research results and to all attendees that honored us with their presence. We hope that the workshop proceedings will be helpful for future research in the area of Information Security.

June 2012

Ioannis Askoxylakis
Henrich C. Pöhls
Joachim Posegga

Organization

General Chairs

Konstantinos Markantonakis	ISG-SCC, Royal Holloway University of London, UK
Gerhard Hancke	ISG, Royal Holloway University of London, UK
Keith Mayes	ISG-SCC, Royal Holloway University of London, UK

Local Organizers

Emma Dobson	ISG, Royal Holloway University of London, UK

Workshop/Panel/Tutorial Chair

Damien Sauveron	XLIM, University of Limoges, France

Publicity Chairs

Sara Foresti	Universitá degli Studi di Milano, Italy
Taeshik Shon	Ajou University, Korea

Program Chairs

Ioannis Askoxylakis	FORTH-ICS, Greece
Joachim Posegga	Institute of IT Security and Security Law at the University of Passau, Germany

Program Committee

Claudio Ardagna	Universitá degli Studi di Milano, Italy
Lejla Batina	Radboud University Nijmegen, The Netherlands
Angelos Bilas	FORTH-ICS and University of Crete, Greece
Levente Buttyan	Budapest University of Technology and Economics, Hungary
Serge Chaumette	LaBRI and University of Bordeaux, France
Jorge Cueller	Siemens, Germany
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Catalan, Spain

Jaap-Henk Hoepman	TNO and Radboud University Nijmegen, The Netherlands
Michael Huth	Imperial College London, UK
Martin Johns	SAP Research, Germany
Cagatay Karabat	TUBITAK BILGEM (The Scientific and Technological Research Council of Turkey), Turkey
Angelos Keromytis	Columbia University, USA
Kwok Yan Lam	National University of Singapore, Singapore
Peter Lipp	Technische Universität Graz, Austria
Javier Lopez	University of Malaga, Spain
Emmanuel Magkos	Ionian University, Greece
Mark Manulis	Technische Universität Darmstadt, Germany
Louis Marinos	European Network and Information Security Agency (ENISA), EU
Fabio Martinelli	IIT-CNR, Italy
Aikaterini Mitrokosta	EPFL, Switzerland
Jose Onieva	University of Malaga, Spain
Gerardo Pelosi	University of Bergamo, Italy
Svetla Petkova-Nikova	Katholieke Universiteit Leuven, Belgium
Henrich C. Pöhls	Institute of IT Security and Security Law at the University of Passau, Germany
Ilia Polian	University of Passau, Germany
Axel Poschmann	National University of Singapore, Singapore
Jean-Jacques Quisquater	DICE, Catholic University of Louvain, Belgium
Bill Roscoe	Department of Computer Science, UK
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	Universitá degli Studi di Milano, Italy
Christos Siaterlis	Joint Research Centre, EU
George Spanoudakis	City University of London, UK
Theo Tryfonas	University of Bristol, UK
Michael Tunstall	University of Bristol, UK
Ingrid Verbauwhede	Katholieke Universiteit Leuven, Belgium
Heung-Youl Youm	Soonchunhyang University, Korea

WISTP Steering Committee

Claudio Ardagna	Universitá degli Studi di Milano, Italy
Angelos Bilas	FORTH-ICS, University of Crete, Greece
Konstantinos Markantonakis	ISG-SCC, Royal Holloway University of London, UK
Jean-Jacques Quisquater	DICE, Catholic University of Louvain, Belgium
Damien Sauveron	XLIM, University of Limoges, France
Jianying Zhou	Institute for Infocomm Research, Singapore

External Reviewers

Alcaraz, Cristina
Alpár, Gergely
Beslay, Laurent
Braun, Bastian
Chen, Bangdao
Dimitriou, Giorgos
Farras, Oriol
Fragkiadakis, Alexandros
Hanser, Christian
Huaqun, Wang
Jawurek, Marek
Karyotis, Vasileios
Kótyuk, Gergely
Lueks, Wouter
Moyano, Francisco
Naya-Plasencia, María
Nishide, Takashi
Ochoa, Martin
Palomba, Andrea
Petroulakis, Nikolaos
Poll, Erik
Roman, Rodrigo
Samelin, Kai
Schroepfer, Axel
Singelee, Dave
Su, Chunhua
Suzaki, Tomoyasu
Tragos, Elias
Trujillo-Rasua, Rolando
Uhsadel, Leif
Whitnall, Carolyn
Zhao, Laiping

Table of Contents

Policy and Access Control

Multi-Party Computation

Cryptography (Short Papers)

Mobile Security