Lecture Notes in Computer Science 6033

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

Pierangela Samarati Michael Tunstall
Joachim Posegga Konstantinos Markantonakis
Damien Sauveron (Eds.)

Information Security Theory and Practices

Security and Privacy of Pervasive Systems and Smart Devices

4th IFIP WG 11.2 International Workshop, WISTP 2010
Passau, Germany, April 12-14, 2010
Proceedings

Springer

Volume Editors

Pierangela Samarati
Università degli Studi di Milano, Dipartimento di Tecnologie dell' Informazione
Via Bramante 65, 26013 Crema (CR), Italy
E-mail: pierangela.samarati@unimi.it

Michael Tunstall
University of Bristol, Department of Computer Science
Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB, UK
E-mail: tunstall@cs.bris.ac.uk

Joachim Posegga
Institute of IT Security and Security Law
94030 Passau, Germany
E-mail: jp@sec.uni-passau.de

Konstantinos Markantonakis
University of London, Information Security Group, Smart Card Centre
Royal Holloway, Egham, Surrey TW20 0EX, UK
E-mail: k.markantonakis@rhul.ac.uk

Damien Sauveron
University of Limoges, XLIM, UMR CNRS 6172
123 avenue Albert Thomas, 87060 Limoges, France
E-mail: damien.sauveron@unilim.fr

Library of Congress Control Number: 2010923798

CR Subject Classification (1998): E.3, C.2, D.4.6, K.6.5, J.1, H.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-12367-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-12367-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

These proceedings contain the papers selected for presentation at the 4th Workshop on Information Security Theory and Practice (WISTP 2010), held during April 12–14, 2010 in Passau, Germany.

In response to the call for papers, 69 papers were submitted to the workshop. These papers were evaluated on the basis of their significance, novelty, and technical quality. Each paper was reviewed by four members of the Program Committee. Reviewing was double-blind meaning that the Program Committee was not able to see the names and affiliations of the authors, and the authors were not told which committee members reviewed which papers. The Program Committee meeting was held electronically, holding intensive discussions over a period of two weeks. Of the papers submitted, 20 full papers and 10 short papers were selected for presentation at the workshop.

This workshop was sponsored by Vodaphone, who also provided a best paper award. We would like to thank this organization for their support, which helped make this workshop possible. Their continued support helps to reduce registration fees and make WISTP a continuing success.

WISTP 2010 was also organized in cooperation with the International Association for Cryptologic Research (IACR), the IFIP WG 11.2 Pervasive Systems Security, and ACM SIGSAC. Their support has significantly contributed to raising the profile of WISTP, which is reflected in the number of high-quality submissions that we received.

There is also a long list of people who volunteered their time and energy to put together the workshop and who deserve acknowledgment. Thanks to all the members of the Program Committee, and the external reviewers, for all their hard work in their evaluation of the submitted papers. We are also very grateful to everyone who gave their assistance and ensured a smooth organization process: the WISTP Steering Committee, Damien Sauveron in particular, for their advice; Joachim Posegga and Konstantinos Markantonakis, for their support in the overall organization as General Chairs; Claudio A. Ardagna, Ioannis G. Askoxylakis, and Gerhard Hancke, for taking care of the publicity for this workshop.

Last, but certainly not least, our thanks go to all the authors who submitted papers and all the attendees. We hope you find the proceedings stimulating.

February 2010

Pierangela Samarati
Michael Tunstall

WISTP 2010

4th International Workshop on Information Security Theory and Practice

Passau, Germany
April 12–14, 2010

General Chairs

Joachim Posegga	University of Passau, Germany
Konstantinos Markantonakis	Royal Holloway, University of London, UK

Local Organizer

Joachim Posegga	University of Passau, Germany

Workshop/Panel/Tutorial Chair

Damien Sauveron	University of Limoges, France

Publicity Chairs

Claudio Ardagna	University of Milan, Italy
Ioannis G. Askoxylakis	FORTH-ICS, Greece
Gerhard Hancke	Royal Holloway, University of London, UK

Program Chairs

Pierangela Samarati	University of Milan, Italy
Michael Tunstall	University of Bristol, UK

Program Committee

Rafael Accorsi	University of Freiburg, Germany
Claudio Ardagna	University of Milan, Italy
Franois Arnault	University of Limoges, France
Ioannis G. Askoxylakis	FORTH-ICS, Greece
Gildas Avoine	Catholic University of Louvain, Belgium

Angelos Bilas	FORTH-ICS & University of Crete, Greece
Carlo Blundo	University of Salerno, Italy
Marco Casassa	Mont. HP Labs, UK
Serge Chaumette	University Bordeaux 1, France
Sabrina De Capitani di Vimercati	University of Milan, Italy
Jan de Meer	Brandenburg Technical University, Germany
Estbaliz Delgado	European Software Institute, Spain
Tassos Dimitriou	Athens Information Technology, Greece
Sara Foresti	University of Milan, Italy
Flavio Garcia	Radboud University Nijmegen, The Netherlands
Stefanos Gritzalis	University of the Aegean, Greece
Yong Guan	Iowa State University, USA
Gerhard Hancke	Royal Holloway, University of London, UK
Ragib Hasan	University of Illinois, USA
Olivier Heen	INRIA, France
Jaap-Henk Hoepman	TNO & Radboud University Nijmegen, The Netherlands
Michael Huth	Imperial College London, UK
Sotiris Ioannidis	FORTH-ICS & University of Crete, Greece
Sokratis Katsikas	University of Piraeus, Greece
Evangelos Kranakis	Carleton University, Canada
Michiharu Kudo	IBM Research, Japan
Konstantinos Markantonakis	Royal Holloway University of London, UK
Olivier Markowitch	ULB, Belgium
Fabio Martinelli	IIT-CNR, Italy
Sjouke Mauw	University of Luxembourg, Luxembourg
Keith Mayes	Royal Holloway, University of London, UK
Carlos Maziero	Pontifical Catholic University of Parana, Brazil
Chris Mitchell	Royal Holloway University of London, UK
Stefaan Motte	NXP Semiconductors, Belgium
Jose Onieva	University of Malaga, Spain
Rolf Oppliger	eSECURITY Technologies, Switzerland
Dan Page	University of Bristol, UK
Stefano Paraboschi	University of Bergamo, Italy
Pierre Paradinas	INRIA & CNAM, France
Gerardo Pelosi	University of Bergamo, Italy
Erik Poll	Radboud University Nijmegen, The Netherlands
Konstantinos Rantos	Hellenic Ministry of Interior, Greece

Kui Ren	Illinois Institute of Technology, USA
Vincent Rijmen	Katholieke Universiteit Leuven, Belgium
Rei Safavi-Naini	University of Calgary, Canada
Damien Sauveron	University of Limoges, France
Daniel Schreckling	University of Passau, Germany
Byron Thomas	SiVenture, UK
Erik Zenner	Technical University of Denmark, Denmark
Bo Zhu	University of Concordia, Canada

Steering Committee

Angelos Bilas	FORTH-ICS & University of Crete, Greece
Jaap-Henk Hoepman	TNO and Radboud University Nijmegen, The Netherlands
Konstantinos Markantonakis	Royal Holloway, University of London, UK
Chris Mitchell	Royal Holloway, University of London, UK
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
Damien Sauveron	University of Limoges, France

External Reviewers

Naveed Ahmed
Efthimia Aivaloglou
Haitham Al-Sinani
Jérémie Albert
Mina Askari
Theodoros Balopoulos
Masoud Barati
Lejla Batina
Samia Bouzefrane
Lukasz Chmielewski
Gabriele Costa
Gerhard de Koning Gans
Damien Dubernet
David Galindo
Carl Gebhardt
Dimitris Geneiatakis
Simon Hoerder
Hugo Jonker
Ioanna Kantzavelou
Giorgos Karopoulos
Aliaksandr Lazouski
Hoi Le
Gregor Leander
Olivier Ly
Benjamin Martin
Tania Martin
Emmanuel Michailidis
Shivaramakrishnan Narayan
Svetla Nikova
Jonathan Ouoba
Vassilis Prevelakis
Sasa Radomirovic
Evangelos Rekleitis
Peipei Shi
Ton van Deursen
Pim Vullers
Artsiom Yautsiukhin

Table of Contents

Embedded Security

Protocols

Highly Constrained Embedded Systems

Security

Smart Card Security

Algorithms

Hardware Implementations

Embedded Systems

Anonymity/Database Security