Lecture Notes in Computer Science 5746

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

Olivier Markowitch Angelos Bilas
Jaap-Henk Hoepman Chris J. Mitchell
Jean-Jacques Quisquater (Eds.)

Information Security Theory and Practice

Smart Devices, Pervasive Systems, and Ubiquitous Networks

Third IFIP WG 11.2 International Workshop, WISTP 2009
Brussels, Belgium, September 1-4, 2009
Proceedings

Springer

Volume Editors

Olivier Markowitch
Université Libre de Bruxelles
1050 Bruxelles, Belgium
E-mail: olivier.markowitch@ulb.ac.be

Angelos Bilas
Foundation for Research and Technology – Hellas
Institute of Computer Science
Vassilika Vouton, Heraklion 70013, Greece
E-mail: bilas@ics.forth.gr

Jaap-Henk Hoepman
TNO / Radboud University Nijmegen
9701 BK Groningen, The Netherlands
E-mail: jhh@cs.ru.nl

Chris J. Mitchell
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
E-mail: C.Mitchell@rhul.ac.uk

Jean-Jacques Quisquater
Université Catholique de Louvain
1348 Louvain-la-Neuve, Belgium
E-mail: quisquater@dice.ucl.ac.be

Library of Congress Control Number: 2009932597

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-03943-X Springer Berlin Heidelberg New York
ISBN-13 978-3-642-03943-0 Springer Berlin Heidelberg New York

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12738540 06/3180 5 4 3 2 1 0

Preface

This volume contains the 12 papers presented at the WISTP 2009 conference, held in Brussels, Belgium in September 2009. WISTP 2009 was the third international workshop devoted to information security theory and practice.

WISTP 2009 built on the successful WISTP 2007 and 2008 conferences, held in Heraklion, Crete, Greece and Seville, Spain in May 2007 and May 2008, respectively. The proceedings of WISTP 2007 and WISTP 2008 were published as volumes 4462 and 5019 of the *Lecture Notes in Computer Science* series.

This workshop received the following support:

- Co-sponsored by IFIP WG 11.2 Small System Security
- Co-sponsored by VDE ITG
- Technical sponsorship of the IEEE Systems, Man & Cybernetics Society
- Supported by the Technical Committee on Systems Safety and Security
- Organized in cooperation with the ACM SIGSAC
- Supported by ENISA
- Supported by the Institute for Systems and Technologies of Information, Control and Communication (INSTICC)

These proceedings contain 12 original papers covering a range of theoretical and practical topics in information security. For the purposes of the organization of the WISTP program, the papers were divided into four main categories, namely:

- Mobility
- Attacks and Secure Implementations
- Performance and Security
- Cryptography

The 12 papers included here were selected from a total of 27 submissions. The refereeing process was rigorous, involving at least three (and mostly four or five) independent reports being prepared for each submission. We are very grateful to our hard-working and distinguished Program Committee for doing such an excellent job in a timely fashion. We believe that the result is a high-quality set of papers, some of which have been significantly improved as a result of the refereeing process.

We are also happy to acknowledge the support and collaboration of the MASTER research project. MASTER is a collaborative project funded under the EU 7th Research Framework Program. It is aligned to Strategic Objective 1.4: Secure, dependable and trusted infrastructures, as defined by the European Commission in the 2007/08 FP7 ICT Work Program. The conference incorporates a session devoted to describing the work of this project.

We would like to thank the General Chairs, Angelos Bilas and Olivier Markowitch, the local organizers Jérôme Dossogne, Olivier Markowitch, and Naïm Qachri,

the Workshop Chair Jean-Jacques Quisquater and the Publicity Chairs Claudio Ardagna, Ioannis G. Askoxylakis, Joonsang Baek, and Gerhard Hancke. We would also like to thank Damien Sauveron for his tireless support during the whole process of organizing the workshop, setting up and maintaining the conference review website, and taking care of all kinds of behind-the-scenes arrangements.

Finally we would like to thank all the authors who submitted their papers to WISTP 2009, all external referees, all the attendees of the conference, and last, but by no means least, our five distinguished invited speakers, namely:

- Gildas Avoine, Université Catholique de Louvain, Belgium
- Jean-Pierre Delesse, Eurosmart, Brussels, Belgium
- Steve Purser, ENISA, Crete, Greece
- Vincent Rijmen, Katholieke Universiteit Leuven, Belgium
- Doug Tygar, UC Berkeley, USA

This conference was the third in an annual series of conferences devoted to the study of security and privacy of pervasive systems, and we look forward to WISTP 2010, due to take place in Passau, Germany in April 2010.

June 2009

Jaap-Henk Hoepman
Chris Mitchell

WISTP 2009

Third International Workshop on Information Security Theory and Practice

Brussels, Belgium
September 1–4, 2009

General Chairs

Angelos Bilas	FORTH-ICS and University of Crete, Greece
Olivier Markowitch	Université Libre de Bruxelles, Belgium

Local Organizers

Jérôme Dossogne	Université Libre de Bruxelles, Belgium
Olivier Markowitch	Université Libre de Bruxelles, Belgium (Chair)
Naïm Qachri	Université Libre de Bruxelles, Belgium

Workshop/Panel/Tutorial Chair

Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium

Publicity Chairs

Claudio Ardagna	University of Milan, Italy
Ioannis G. Askoxylakis	FORTH-ICS, Greece
Joonsang Baek	Institute for Infocomm Research (I2R), Singapore
Gerhard Hancke	Royal Holloway, University of London, UK

Program Chairs

Jaap-Henk Hoepman	TNO and Radboud University Nijmegen, The Netherlands
Chris J. Mitchell	Royal Holloway, University of London, UK

Program Committee

Rafael Accorsi	University of Freiburg, Germany
Manfred Aigner	Technical University Graz, Austria
François Arnault	University of Limoges, France
Ioannis G. Askoxylakis	FORTH-ICS, Greece
Christophe Bidan	Supélec, France
Pierre-François Bonnefoi	University of Limoges, France
Serge Chaumette	University Bordeaux 1, France
Estíbaliz Delgado	European Software Institute, Spain
Tassos Dimitriou	Athens Information Technology, Greece
Pierre Dusart	University of Limoges, France
Sara Foresti	University of Milan, Italy
Flavio Garcia	Radboud University Nijmegen, The Netherlands
Theodoulos Garefalakis	University of Crete, Greece
Dieter Gollmann	TU Hamburg-Harburg, Germany
Stefanos Gritzalis	University of the Aegean, Greece
Gerhard Hancke	Royal Holloway, University of London, UK
Olivier Heen	INRIA, France
Sotiris Ioannidis	FORTH-ICS and University of Crete, Greece
Sokratis Katsikas	University of Piraeus, Greece
Evangelos Kranakis	Carleton University, Canada
Deok-Gyu Lee	Electronics and Telecommunications Research Institute, Korea
Konstantinos Markantonakis	Royal Holloway, University of London, UK
Fabio Martinelli	IIT-CNR, Italy
Keith Mayes	Royal Holloway, University of London, UK
Jan de Meer	Brandenburg Technical University, Germany
Sjouke Mauw	University of Luxembourg, Luxembourg
Stefaan Motte	NXP Semiconductors, Belgium
Jose Onieva	University of Malaga, Spain
Rolf Oppliger	eSECURITY Technologies, Switzerland
Pierre Paradinas	INRIA and CNAM, France
Erik Poll	Radboud University Nijmegen, The Netherlands
Joachim Posegga	University of Passau, Germany
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
Kai Rannenberg	Goethe University Frankfurt, Germany
Konstantinos Rantos	Hellenic Ministry of Interior, Public Administration and Decentralisation, Greece
Damien Sauveron	University of Limoges, France

Frank Stajano	University of Cambridge, UK
Michael Tunstall	University of Bristol, UK
Paulo Jorge Esteves Veríssimo	University of Lisbon, Portugal
Erik Zenner	Technical University of Denmark, Denmark
Alf Zugenmaier	Docomo Research Labs, Germany

Steering Committee

Angelos Bilas	FORTH-ICS and University of Crete, Greece
Serge Chaumette	University Bordeaux 1, France
Dieter Gollmann	TU Hamburg-Harburg, Germany
Konstantinos Markantonakis	Royal Holloway, University of London, UK
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
Damien Sauveron	University of Limoges, France

External Reviewers

Samia Bouzefrane
Carlos Cid
Julien Cordry
Gabriele Costa
Ton van Deursen
David Galindo
Martin Johns
Aliksandr Lazouski
Marinella Petrocchi
Evgenia Pisko
Henrich C. Poehls
Saša Radomirović
Evangelos Rekleitis
Ruben Rios
Thomas Sirvent
Markus Tschersich
Harald Vogt
Christian Weber

Sponsoring Institution

Université Libre de Bruxelles, Belgium

Main Sponsors

Since the early stages of the inception of the workshop, the organizers have received positive feedback from a number of high-profile organizations. With the development of a strong Program and Organizing Committee, this developed into direct financial support. This has enabled the workshop organizers to strengthen

significantly their main objective of providing a high-standard academic workshop. The support has made a major contribution toward keeping the workshop registration costs as low as possible, and at the same time enabling us to offer a number of best paper awards. We would therefore like to express our gratitude to every single organization who has helped us financially, as listed below. We also look forward to working together with them on future WISTP events.

Table of Contents

Mobility

On the Unobservability of a Trust Relation in Mobile Ad Hoc Networks 1
Olivier Heen, Gilles Guette, and Thomas Genet

A Mechanism to Avoid Collusion Attacks Based on Code Passing in Mobile Agent Systems 12
Marc Jaimez, Oscar Esparza, Jose L. Muñoz, Juan J. Alins-Delgado, and Jorge Mata-Díaz

Privacy-Aware Location Database Service for Granular Queries 28
Shinsaku Kiyomoto, Keith M. Martin, and Kazuhide Fukushima

Attacks and Secure Implementations

Algebraic Attacks on RFID Protocols 38
Ton van Deursen and Saša Radomirović

Anti-counterfeiting Using Memory Spots 52
Helen Balinsky, Edward McDonnell, Liqun Chen, and Keith Harrison

On Second-Order Fault Analysis Resistance for CRT-RSA Implementations 68
Emmanuelle Dottax, Christophe Giraud, Matthieu Rivain, and Yannick Sierra

Performance and Security

Measurement Analysis When Benchmarking Java Card Platforms 84
Pierre Paradinas, Julien Cordry, and Samia Bouzefrane

Performance Issues of Selective Disclosure and Blinded Issuing Protocols on Java Card 95
Hendrik Tews and Bart Jacobs

Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks 112
Christian Lederer, Roland Mader, Manuel Koschuch, Johann Großschädl, Alexander Szekely, and Stefan Tillich

Cryptography

Key Management Schemes for Peer-to-Peer Multimedia Streaming Overlay Networks 128
J.A.M. Naranjo, J.A. López-Ramos, and L.G. Casado

Ultra-Lightweight Key Predistribution in Wireless Sensor Networks for Monitoring Linear Infrastructure 143
Keith M. Martin and Maura B. Paterson

PKIX Certificate Status in Hybrid MANETs 153
Jose L. Muñoz, Oscar Esparza, Carlos Gañán, and Javier Parra-Arnau

Author Index 167