

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Alfred Kobsa

*University of California, Irvine, CA, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Germany*

Madhu Sudan

*Microsoft Research, Cambridge, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

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

## 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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

springer.com

© IFIP International Federation for Information Processing 2010

Printed in Germany

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 Vodafone, 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

VIII Organization

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

# Table of Contents

## Embedded Security

Efficient and Effective Buffer Overflow Protection on ARM Processors .....	1
<i>Raoul Strackx, Yves Younan, Pieter Philippaerts, and Frank Piessens</i>	
Efficient Entropy Estimation for Mutual Information Analysis Using B-Splines .....	17
<i>Alexandre Venelli</i>	
A Probabilistic Diffusion Scheme for Anomaly Detection on Smartphones .....	31
<i>Tansu Alpcan, Christian Bauckhage, and Aubrey-Derrick Schmidt</i>	
A Smart Card Implementation of the McEliece PKC .....	47
<i>Falko Strenzke</i>	
Evaluation Metrics of Physical Non-invasive Security .....	60
<i>Huiyun Li, Keke Wu, Fengqi Yu, and Hai Yuan</i>	

## Protocols

Trust in Peer-to-Peer Content Distribution Protocols .....	76
<i>Nicolai Kuntze, Carsten Rudolph, and Andreas Fuchs</i>	
Generic Constructions of Biometric Identity Based Encryption Systems .....	90
<i>Neyire Deniz Sarier</i>	
Design and Analysis of a Generalized Canvas Protocol .....	106
<i>Marián Novotný</i>	

## Highly Constrained Embedded Systems

Efficient Mutual Authentication for Multi-domain RFID Systems Using Distributed Signatures .....	122
<i>Michael Braun, Ulrike Meyer, and Susanne Wetzel</i>	
Practical Schemes for Privacy and Security Enhanced RFID (Extended Abstract) .....	138
<i>Jaap-Henk Hoepman and Rieks Joosten</i>	
MoteAODV – An AODV Implementation for TinyOS 2.0 .....	154
<i>Werner Backes and Jared Cordasco</i>	



## Security

Random Number Generation Based on Fingerprints . . . . .	170
<i>Shkodran Gerguri, Václav Matyáš, Zdeněk Říha, and Luděk Smolík</i>	
Improvements of pan-European IDM Architecture to Enable Identity Delegation Based on X.509 Proxy Certificates and SAML . . . . .	183
<i>Sergio Sánchez García and Ana Gómez Oliva</i>	
Fraud Detection for Voice over IP Services on Next-Generation Networks . . . . .	199
<i>Igor Ruiz-Agundez, Yoseba K. Penya, and Pablo Garcia Bringas</i>	

## Smart Card Security

Proxy Smart Card Systems . . . . .	213
<i>Giuseppe Cattaneo, Pompeo Faruolo, Vincenzo Palazzo, and Ivan Visconti</i>	
Can We Support Applications' Evolution in Multi-application Smart Cards by Security-by-Contract? . . . . .	221
<i>Nicola Dragoni, Olga Gadyatskaya, and Fabio Massacci</i>	
Website Credential Storage and Two-Factor Web Authentication with a Java SIM . . . . .	229
<i>Jonathan Hart, Konstantinos Markantonakis, and Keith Mayes</i>	

## Algorithms

Attribute-Based Encryption with Break-Glass . . . . .	237
<i>Achim D. Brucker, Helmut Petritsch, and Stefan G. Weber</i>	
On the Security of a Two-Factor Authentication Scheme . . . . .	245
<i>Luigi Catuogno and Clemente Galdi</i>	
The Design of Secure and Efficient P2PSIP Communication Systems . . .	253
<i>Xianghan Zheng and Vladimir Oleshchuk</i>	

## Hardware Implementations

Novel FPGA-Based Signature Matching for Deep Packet Inspection . . . .	261
<i>Nitesh B. Guinde and Sotirios G. Ziavras</i>	
Towards Electrical, Integrated Implementations of SIMPL Systems . . . .	277
<i>Ulrich Rührmair, Qingqing Chen, Martin Stutzmann, Paolo Lugli, Ulf Schlichtmann, and György Csaba</i>	

A Very Compact Hardware Implementation of the KASUMI Block Cipher .....	293
<i>Dai Yamamoto, Kouichi Itoh, and Jun Yajima</i>	

## Embedded Systems

Secure and Usable Out-Of-Band Channels for <i>Ad Hoc</i> Mobile Device Interactions .....	308
<i>Ronald Kainda, Ivan Flechais, and A.W. Roscoe</i>	
Identification and Verification of Security Relevant Functions in Embedded Systems Based on Source Code Annotations and Assertions .....	316
<i>Johannes Loinig, Christian Steger, Reinhold Weiss, and Ernst Haselsteiner</i>	
Security Analysis of Mobile Phones Used as OTP Generators .....	324
<i>Håvard Raddum, Lars Hopland Nestås, and Kjell Jørgen Hole</i>	
An Energy-Efficient Symmetric Cryptography Based Authentication Scheme for Wireless Sensor Networks .....	332
<i>Oscar Delgado-Mohatar, José M. Sierra, Ljiljana Brankovic, and Amparo Fúster-Sabater</i>	

## Anonymity/Database Security

The Market Failure of Anonymity Services .....	340
<i>Heiko Rossnagel</i>	
Exploiting Node Mobility for Coordinating Data Usage in Crisis Scenarios .....	355
<i>Giovanni Russello and Enrico Scalavino</i>	
Predicting and Preventing Insider Threat in Relational Database Systems .....	368
<i>Qussai Yaseen and Brajendra Panda</i>	
<b>Author Index</b> .....	385