

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 for Informatics, Saarbruecken, Germany

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

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

© IFIP International Federation for Information Processing 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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	Università 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	Università 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

VIII Organization

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 Marinou	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	Università 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	Università 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
Jiaying 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

Keynotes

Recent Developments in Low-Level Software Security	1
<i>Pieter Agten, Nick Nikiforakis, Raoul Strackx, Willem De Groef, and Frank Piessens</i>	
Towards a C ² I Platform for Combating the Cyber-Threat (Extended Abstract)	17
<i>Paul Kearney</i>	
Veracity, Plausibility, and Reputation	20
<i>Dieter Gollmann</i>	

Protocols

Another Fallen Hash-Based RFID Authentication Protocol	29
<i>Julio Cesar Hernandez-Castro, Pedro Peris-Lopez, Masoumeh Safkhani, Nasour Bagheri, and Majid Naderi</i>	

Protocols (Short Papers)

HTTP Botnet Detection Using Adaptive Learning Rate Multilayer Feed-Forward Neural Network	38
<i>G. Kirubavathi Venkatesh and R. Anitha Nadarajan</i>	
How to Break EAP-MD5	49
<i>Fanbao Liu and Tao Xie</i>	

Privacy

Privacy Preserving Social Network Publication on Bipartite Graphs	58
<i>Jian Zhou, Jiwu Jing, Ji Xiang, and Lei Wang</i>	
Privacy Bubbles: User-Centered Privacy Control for Mobile Content Sharing Applications	71
<i>Delphine Christin, Pablo Sánchez López, Andreas Reinhardt, Matthias Hollick, and Michaela Kauer</i>	

Privacy (Short Paper)

Privacy Preservation of User History Graph	87
<i>Shinsaku Kiyomoto, Kazuhide Fukushima, and Yutaka Miyake</i>	

Policy and Access Control

HiPoLDS: A Security Policy Language for Distributed Systems 97
*Matteo Dell’Amico, Gabriel Serme, Muhammad Sabir Idrees,
 Anderson Santana de Olivera, and Yves Roudier*

ROAC: A Role-Oriented Access Control Model 113
Nezar Nassr and Eric Steegmans

Multi-Party Computation

Optimal Parameters for Efficient Two-Party Computation Protocols 128
Chaya Ganesh and C. Pandu Rangan

Assisting Server for Secure Multi-Party Computation 144
Jens-Matthias Bohli, Wenting Li, and Jan Seedorf

Cryptography (Short Papers)

An Efficient Lattice-Based Secret Sharing Construction 160
Rachid El Bansarkhani and Mohammed Meziani

On the Optimality of Correlation Power Attack on Embedded
 Cryptographic Systems 169
*Youssef Souissi, Nicolas Debande, Sami Mekki, Sylvain Guilley,
 Ali Maalaoui, and Jean-Luc Danger*

Impossible Differential Cryptanalysis of Reduced-Round LBlock 179
Ferhat Karakoç, Hüseyin Demirci, and A. Emre Harmancı

Mobile Security

Efficient Java Implementation of Elliptic Curve Cryptography for
 J2ME-Enabled Mobile Devices 189
Johann Großschädl, Dan Page, and Stefan Tillich

Kynoid: Real-Time Enforcement of Fine-Grained, User-Defined, and
 Data-Centric Security Policies for Android 208
*Daniel Schreckling, Joachim Posegga, Johannes Köstler, and
 Matthias Schaff*

Author Index 225