

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7410>

Raja Naeem Akram · Sushil Jajodia (Eds.)

Information Security Theory and Practice

9th IFIP WG 11.2 International Conference, WISTP 2015
Heraklion, Crete, Greece, August 24–25, 2015
Proceedings

Editors

Raja Naeem Akram
ISG-SCC
University of London
Egham
UK

Sushil Jajodia
George Mason University
Fairfax, VI
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-24017-6 ISBN 978-3-319-24018-3 (eBook)
DOI 10.1007/978-3-319-24018-3

Library of Congress Control Number: 2015948704

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Cham Heidelberg New York Dordrecht London
© Springer International Publishing Switzerland 2015

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, 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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media
(www.springer.com)

Preface

Future ICT technologies, such as the concepts of Ambient Intelligence, Cyber-physical Systems, and Internet of Things provide a vision of the Information Society in which a) people and physical systems are surrounded with intelligent interactive interfaces and objects, and b) environments are capable of recognizing and reacting to the presence of different individuals or events in a seamless, unobtrusive, and invisible manner. The success of future ICT technologies will depend on how secure these systems are and to what extent they protect the privacy of individuals and individuals trust them.

In 2007, the Workshop on Information Security Theory and Practice (WISTP) was created as a forum for bringing together researchers and practitioners in related areas and to encourage interchange and cooperation between the research community and the industrial/consumer community. Due to the growing number of participants, the 2015 event became a conference – The 9th WISTP International Conference on Information Security Theory and Practice (WISTP 2015).

WISTP 2015 sought original submissions from academia and industry presenting novel research on all theoretical and practical aspects of security and privacy, as well as experimental studies of fielded systems, the application of security technology, the implementation of systems, and lessons learned. We encouraged submissions from other communities such as law, business, and policy that present these communities' perspectives on technological issues.

These proceedings contain the papers selected for presentation at the 9th WISTP International Conference on Information Security Theory and Practice (WISTP 2015), held August 24–25 in Heraklion, Crete, Greece.

In response to the call for papers 52 papers were submitted to the conference. These papers were evaluated on the basis of their significance, novelty, and technical quality. Each paper was reviewed by at least three members of the Program Committee. Of the papers submitted, 14 full papers and 4 short papers were selected for presentation at the conference.

There is a long list of people who volunteered their time and energy to put together the conference and who deserve acknowledgment. Thanks to all the members of the Program Committee and the external reviewers for all their hard work in evaluating and discussing papers. We are also very grateful to Damien Sauveron, Chair of the WISTP Steering Committee, for his guidance through all stages of the conference. Last, but certainly not least, our thanks go to all the authors who submitted papers and all the attendees.

We hope that you will find the proceedings stimulating and a source of inspiration for future research.

July 2015

Raja Naeem Akram
Sushil Jajodia

Organization

WISTP 2015 was organized by FORTH-ICS, Greece

General Chair

Ioannis Askoxylakis FORTH- ICS, Greece

Local Organizer

Nikolaos Petroulakis FORTH-ICS, Greece

Workshop/Panel/Tutorial Chair

Damien Sauveron XLIM, University of Limoges, France

Publicity Chair

Ruggero Donida Labati Università degli Studi di Milano, Italy

Program Chairs

Raja Naeem Akram Royal Holloway, University of London, UK
Sushil Jajodia George Mason University, USA

Program Committee

Mohamed Ahmed Abdelraheem	The Technical University of Denmark/DTU Compute, Denmark
Claudio A. Ardagna	Università degli Studi di Milano, Italy
Ioannis Askoxylakis	FORTH-ICS, Greece
Selcuk Baktir	Bahcesehir University, Turkey
Lejla Batina	Radboud University Nijmegen, The Netherlands
Samia Bouzefrane	CEDRIC, Conservatoire National des Arts et Métiers, France
Lorenzo Cavallaro	Royal Holloway, University of London, UK
Hervé Chabanne	Morpho, France
Serge Chaumette	LaBRI, University of Bordeaux, France
Delphine Christin	University of Bonn, Fraunhofer FKIE, Germany
Mauro Conti	University of Padua, Italy
Kurt Dietrich	NXP, Austria
Sara Foresti	Università degli Studi di Milano, Italy
José María De Fuentes	Carlos III University of Madrid, Spain
Flavio Garcia	University of Birmingham, UK

Yong Guan	Iowa State University, USA
Gerhard Hancke	City University of Hong Kong, Hong Kong
Julio Hernandez-Castro	University of Kent, UK
Michael Hutter	IAIK, Graz University of Technology, Austria
Süleyman Kardas	TBITAK-BILGEM, Turkey
Mehmet Sabir Kiraz	TBITAK-BILGEM, Turkey
Andrea Lanzi	University of Milan, Italy
Maryline Laurent	SAMOVAR UMR CNRS 5157, Télécom SudParis, France
Albert Levi	Sabancı University, Turkey
Peng Liu	Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
Federico Maggi	Politecnico di Milano, Italy
Vashek Matyas	Masaryk University, Czech Republic
Sjouke Mauw	University of Luxembourg, Luxembourg
Nele Mentens	KU Leuven, Belgium
Alessio Merlo	University of Genoa, Italy
Vladimir A. Oleshchuk	University of Agder, Norway
Jonathan P. Chapman	University of Bonn, Germany
Milan Petkovic	Eindhoven University of Technology, The Netherlands
Wolter Pieters	TU Delft and University of Twente, The Netherlands
Joachim Posegga	Institute of IT-Security and Security Law, Germany
Kai Rannenber	Goethe University Frankfurt, Deutsche Telekom, Germany
Kui Ren	State University of New York at Buffalo, USA
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	Università degli Studi di Milano, Italy
Siraj Ahmed Shaikh	Coventry University, UK
Dave Singelée	KU Leuven, iMinds, COSIC, Belgium
Willy Susilo	University of Wollongong, Australia
Ulrich Tamm	TU Chemnitz, Germany
Li Tiejian	Huawei Technologies, Singapore
Denis Trcek	University of Ljubljana, Slovenia
Michael Tunstall	Cryptography Research Inc, USA
Umut Uludag	TBITAK-BILGEM UEKAE, Turkey
Omair Uthmani	West Lothian College, Livingston, UK
Stefano Zanero	Politecnico di Milano, Italy

Additional Reviewers

Ambrosin, Moreno	Anada, Hiroaki
Bilzhause, Arne	Carminati, Michele
Continella, Andrea	Dargahi, Tooska
Fukushima, Kazuhide	Garcia-Perez, Alexeis
González Manzano, Lorena	Jayasinghe, Danushka
Jonker, Hugo	Kalutarage, Harsha Kumara
Karaođlan Altop, Duygu	Kasi, Mumraiz Khan

Le Vinh, Thinh	Marktscheffel, Tobias
Ordean, Mihai	Polian, Iliia
Quarta, Davide	Radu, Andreea-Ina
Roman, Rodrigo	Spolaor, Riccardo
Tatli, Emin	Tschersich, Markus
Yang, Shuzhe	Yesuf, Ahmed Seid
Yoshida, Hirotaka	Zeng, Qiang

Steering Committee

Angelos Bilas	FORTH-ICS & University of Crete, Greece
Konstantinos Markantonakis	ISG-SCC, Royal Holloway, University of London, UK
David Naccache	Ecole Normale Supérieure, France
Joachim Posegga	Institute of IT-Security and Security Law at the University of Passau, Germany
Jean-Jacques Quisquater	DICE, Catholic University of Louvain, Belgium
Damien Sauveron	XLIM, University of Limoges, France

Scientific Support

IFIP WG 11.2 Pervasive Systems Security

Main Sponsors

The development of a strong program and Organizing Committee, and the WISTP relationship with high profile organizations, has further capitalized into direct financial support. This enabled the conference organizers to strengthen significantly their main objective for proposing a high standard academic event. The support helped significantly to keep the conference registration costs as low as possible and, at the same time, offer a number of best paper awards. Therefore, we would like to express our gratitude and thank Huawei for their support. We are also looking forward to working together for future WISTP events.



Contents

Security and Privacy Services

On Secrecy Amplification Protocols	3
<i>Radim Ošřádal, Petr Švenda, and Vashek Matyáš</i>	
Privacy-Respecting Auctions as Incentive Mechanisms in Mobile Crowd Sensing	20
<i>Tassos Dimitriou and Ioannis Krontiris</i>	
Electrical Heart Signals can be Monitored from the Moon: Security Implications for IPI-Based Protocols	36
<i>Alejandro Calleja, Pedro Peris-Lopez, and Juan E. Tapiador</i>	
Private Minutia-Based Fingerprint Matching	52
<i>Neyire Deniz Sarier</i>	

Secure Resource Sharing and Access Control

Secure Resource Sharing for Embedded Protected Module Architectures	71
<i>Jo Van Bulck, Job Noorman, Jan Tobias Mühlberg, and Frank Piessens</i>	
Secure Obfuscation of Authoring Style	88
<i>Hoi Le, Reihaneh Safavi-Naini, and Asadullah Galib</i>	
DET-ABE: A Java API for Data Confidentiality and Fine-Grained Access Control from Attribute Based Encryption	104
<i>Miguel Morales-Sandoval and Arturo Diaz-Perez</i>	
WSACd - A Usable Access Control Framework for Smart Home Devices . . .	120
<i>Konstantinos Fysarakis, Charalampos Konstantourakis, Konstantinos Rantos, Charalampos Manifavas, and Ioannis Papaefstathiou</i>	

Secure Devices and Execution Environment

Automatic Top-Down Role Engineering Framework Using Natural Language Processing Techniques	137
<i>Masoud Narouei and Hassan Takabi</i>	
Practical and Privacy-Preserving TEE Migration	153
<i>Ghada Arfaoui, Saïd Gharout, Jean-François Lalande, and Jacques Traoré</i>	

Randomizing the Montgomery Powering Ladder 169
Duc-Phong Le, Chik How Tan, and Michael Tunstall

Challenges of Security and Reliability

How Current Android Malware Seeks to Evade Automated Code Analysis. 187
Siegfried Rasthofer, Irfan Asrar, Stephan Huber, and Eric Bodden

On Linkability and Malleability in Self-blindable Credentials 203
Jaap-Henk Hoepman, Wouter Lueks, and Sietse Ringers

Device Synchronisation: A Practical Limitation on Reader Assisted
Jamming Methods for RFID Confidentiality 219
Qiao Hu, Lavinia Mihaela Dinca, and Gerhard Hancke

Short Papers

Normalizing Security Events with a Hierarchical Knowledge Base 237
David Jaeger, Amir Azodi, Feng Cheng, and Christoph Meinel

Attack Tree Generation by Policy Invalidation 249
*Marieta Georgieva Ivanova, Christian W. Probst, René Rydhof Hansen,
and Florian Kammüller*

Lightweight Password Hashing Scheme for Embedded Systems 260
*George Hatzivasilis, Ioannis Papaefstathiou, Charalampos Manifavas,
and Ioannis Askoxylakis*

Secure and Authenticated Access to LLN Resources Through Policy
Constraints 271
*Konstantinos Rantos, Konstantinos Fysarakis, Othonas Soultatos,
and Ioannis Askoxylakis*

Author Index 281