

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, Zurich, 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>

Sara Foresti · Javier Lopez (Eds.)

Information Security Theory and Practice

10th IFIP WG 11.2 International Conference, WISTP 2016
Heraklion, Crete, Greece, September 26–27, 2016
Proceedings

Editors

Sara Foresti
Università degli Studi di Milano
Crema
Italy

Javier Lopez
University of Malaga
Malaga
Spain

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-45930-1 ISBN 978-3-319-45931-8 (eBook)
DOI 10.1007/978-3-319-45931-8

Library of Congress Control Number: 2016950232

LNCS Sublibrary: SL4 – Security and Cryptology

© IFIP International Federation for Information Processing 2016

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

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Preface

The widespread and fast development of ICT is changing the information society in which we live as well as our interactions with the surrounding environment and among each other. This evolution of ICT is bringing unprecedented advantages, but its success will depend on how secure ICT systems are and on the security and privacy guarantees that these systems offer.

These proceedings contain the papers selected for presentation at the 10th WISTP International Conference on Information Security Theory and Practice (WISTP 2016), held in Heraklion, Crete, Greece, on September 26–27, 2016, in conjunction with the 21st European Symposium On Research In Computer Security (ESORICS 2016).

In response to the call for papers, 29 papers were submitted to the conference from 14 different countries. Each paper was reviewed by at least three members of the Program Committee, and evaluated on the basis of its significance, novelty, and technical quality. As in previous years, reviewing was “double-blind”, that is, the identities of the authors were not revealed to the reviewers of the papers and the identities of the reviewers were not revealed to the authors. The Program Committee’s work was carried out electronically, yielding intensive discussions. Of the submitted papers, the Program Committee accepted 13 full papers (resulting in an acceptance rate of 44.8 %) and 5 short papers for presentation at the conference.

WISTP 2016 was organized in cooperation with the IFIP WG 11.2: Pervasive Systems Security and was sponsored by FORTH Institute of Computer Science.

The success of an event like this depends on the voluntary effort of many individuals. There is a long list of people who volunteered their time and energy to organize the conference, and who deserve special thanks. We would like to thank all the members of the Program Committee and all the external reviewers, for all their hard work in evaluating all the papers in a short time window, and for their active participation in the discussion and selection process. We would like to express our sincere gratitude to the WISTP Steering Committee, and its Chair Damien Sauveron in particular, for their support in the organization of the conference. Thanks to Ruggero Donida Labati for taking care of publicity. We are also very grateful to Ioannis Askoxylakis (WISTP General Chair) and to the local organizers for their support in the conference organization and logistics. We would also like to thank the keynote speakers for accepting our invitation and for their enlightening and interesting talks.

Last but certainly not least, our thanks goes to all the authors who submitted papers and to all the conference’s attendees. We hope you find the program of WISTP 2016 interesting, stimulating, and inspiring for your future research.

September 2016

Sara Foresti
Javier Lopez

Organization

General Chair

Ioannis Askoxylakis

FORTH-ICS, Greece

Program Chairs

Sara Foresti

Università degli Studi di Milano, Italy

Javier Lopez

University of Malaga, Spain

Publicity Chair

Ruggero Donida Labati

Università degli Studi di Milano, Italy

Steering Committee

Raja Naeem Akram

Royal Holloway University of London, UK

Angelos Bilas

FORTH-ICS, Greece

Sushil Jajodia

George Mason University, USA

Konstantinos

Royal Holloway University of London, UK

Markantonakis

Joachim Posegga

University of Passau, Germany

Jean-Jacques Quisquater

UCL, Belgium

Damien Sauveron (chair)

University of Limoges, France

Program Committee

Ioannis Askoxylakis

FORTH-ICS, Greece

Lejla Batina

Radboud University Nijmegen, The Netherlands

Kim-Kwang Raymond

University of Texas at San Antonio, USA

Choo

Jorge Cuellar

Siemens AG, Germany

Sabrina De Capitani di

Università degli Studi di Milano, Italy

Vimercati

Jose Fernandez

École Polytechnique de Montréal, Canada

Flavio Garcia

University of Birmingham, UK

Dieter Gollmann

Hamburg University of Technology, Germany

Stefanos Gritzalis

University of the Aegean, Greece

Dimitris Gritzalis

AUEB, Greece

Brahim Hamid

IRIT Research Laboratory, France

Xinyi Huang

Fujian Normal University, China

Michael Hutter	Cryptography Research, USA
Sushil Jajodia	George Mason University, USA
Vasilis Katos	Bournemouth University, UK
Sokratis Katsikas	NTNU, Norway
Florian Kerschbaum	SAP, Germany
Maryline Laurent	Institut Mines-Télécom, France
Giovanni Livraga	Università degli Studi di Milano, Italy
Evangelos Markatos	FORTH-ICS and University of Crete, Greece
Fabio Martinelli	CNR, Italy
Vashek Matyas	Masaryk University, Czech Republic
Sjouke Mauw	University of Luxembourg, Luxembourg
Alessio Merlo	University of Genoa, Italy
Haris Mouratidis	University of Brighton, UK
David Naccache	École Normale Supérieure, France
Rolf Oppliger	eSECURITY Technologies, Switzerland
Stefano Paraboschi	Università degli Studi di Bergamo, Italy
Gerardo Pelosi	Politecnico di Milano, Italy
Pedro Peris-Lopez	Carlos III University, Spain
Günther Pernul	Universität Regensburg, Germany
Milan Petkovic	TU Eindhoven, The Netherlands
Frank Piessens	Katholieke Universiteit Leuven, Belgium
Joachim Posegga	University of Passau, Germany
Jean-Jacques Quisquater	UCL, Belgium
Silvio Ranise	FBK, Italy
Kui Ren	State University of New York at Buffalo, USA
Rodrigo Roman	University of Malaga, Spain
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	Università degli Studi di Milano, Italy
Dave Singelée	Katholieke Universiteit Leuven, Belgium
Miguel Soriano	Universitat Politècnica de Catalunya, Spain
Willy Susilo	University of Wollongong, Australia
Guilin Wang	Huawei International Pte Ltd, Singapore
Meng Yu	University of Texas at San Antonio, USA

External Reviewers

Joonsang Baek	Jan Tobias Muehlberg	Zisis Tsitsikas
Boutheyna Belgacem	Theodore Ntouskas	Theodoros Tzouramanis
Antonio de La Piedra	Juan D. Parra Rodriguez	Yoshifumi Ueshige
Stelios Dritsas	Alexander Puchta	Ding Wang
Sigrid Guergens	Henrich C. Pöhls	Artsiom Yautsiukhin
Ravi Jhawar	Andreea-Ina Radu	Jiangshan Yu
Christos Kalloniatis	Giada Sciarretta	Yuexin Zhang
Eduard Marin	Raoul Strackx	
Pedro Maat Massolino	Johannes Säger	

Contents

Authentication and Key Management

- Securing Transactions with the eIDAS Protocols 3
Frank Morgner, Paul Bastian, and Marc Fischlin
- Novel Lightweight Signcryption-Based Key Distribution Mechanisms
for MIKEY 19
Kim Thuat Nguyen, Nouha Oualha, and Maryline Laurent
- Codes v. People: A Comparative Usability Study of Two Password
Recovery Mechanisms 35
Vlasta Stavova, Vashek Matyas, and Mike Just

Secure Hardware Systems

- An Implementation of a High Assurance Smart Meter Using Protected
Module Architectures. 53
*Jan Tobias Mühlberg, Sara Cleemput, Mustafa A. Mustafa,
Jo Van Bulck, Bart Preneel, and Frank Piessens*
- Security Challenges of Small Cell as a Service in Virtualized Mobile
Edge Computing Environments. 70
Vassilios Vassilakis, Emmanouil Panaousis, and Haralambos Mouratidis
- An HMM-Based Anomaly Detection Approach for SCADA Systems 85
Kyriakos Stefanidis and Artemios G. Voyiatzis

Attacks to Software and Network Systems

- Attacking and Defending Dynamic Analysis System-Calls Based IDS 103
Ishai Rosenberg and Ehud Gudes
- Towards Automatic Risk Analysis and Mitigation of Software Applications . . . 120
*Leonardo Regano, Daniele Canavese, Cataldo Basile, Alessio Viticchié,
and Antonio Lioy*
- Runtime Code Polymorphism as a Protection Against Side Channel Attacks. . . 136
*Damien Couroussé, Thierno Barry, Bruno Robisson, Philippe Jaillon,
Olivier Potin, and Jean-Louis Lanet*
- Analysis of a Code-Based Countermeasure Against Side-Channel
and Fault Attacks 153
Guillaume Barbu and Alberto Battistello

Access Control and Data Protection

LAMP - Label-Based Access-Control for More Privacy
in Online Social Networks 171
Leila Bahri, Barbara Carminati, Elena Ferrari, and William Lucia

Privacy-Preserving Two-Party Skyline Queries Over Horizontally
Partitioned Data 187
Ling Chen, Ting Yu, and Rada Chirkova

Fault-Channel Watermarks 204
Peter Samarin, Alexander Skripnik, and Kerstin Lemke-Rust

Short Papers

The Effect of Semantic Elaboration on the Perceived Security
and Privacy Risk of Privacy-ABCs — An Empirical Experiment 223
Ahmad Sabouri

Delegating Biometric Authentication with the Sumcheck Protocol 236
Hervé Chabanne, Julien Keuffer, and Roch Lescuyer

Password Generators: Old Ideas and New 245
Fatma Al Maqbali and Chris J. Mitchell

Provable Network Activity for Protecting Users Against False Accusation . . . 254
*Panagiotis Papadopoulos, Elias Athanasopoulos, Eleni Kosta,
George Siganos, Angelos D. Keromytis, and Evangelos P. Markatos*

Combining Third Party Components Securely in Automotive Systems 262
*Madeline Cheah, Siraj A. Shaikh, Jeremy Bryans,
and Hoang Nga Nguyen*

Author Index 271