

**Editor-in-Chief**

*Kai Rannenber, Goethe University Frankfurt, Germany*

**Editorial Board**

Foundation of Computer Science

*Jacques Sakarovitch, Télécom ParisTech, France*

Software: Theory and Practice

*Michael Goedicke, University of Duisburg-Essen, Germany*

Education

*Arthur Tatmall, Victoria University, Melbourne, Australia*

Information Technology Applications

*Erich J. Neuhold, University of Vienna, Austria*

Communication Systems

*Aiko Pras, University of Twente, Enschede, The Netherlands*

System Modeling and Optimization

*Fredi Tröltzsch, TU Berlin, Germany*

Information Systems

*Jan Pries-Heje, Roskilde University, Denmark*

ICT and Society

*Diane Whitehouse, The Castlegate Consultancy, Malton, UK*

Computer Systems Technology

*Ricardo Reis, Federal University of Rio Grande do Sul, Porto Alegre, Brazil*

Security and Privacy Protection in Information Processing Systems

*Yuko Murayama, Iwate Prefectural University, Japan*

Artificial Intelligence

*Ulrich Furbach, University of Koblenz-Landau, Germany*

Human-Computer Interaction

*Jan Gulliksen, KTH Royal Institute of Technology, Stockholm, Sweden*

Entertainment Computing

*Matthias Rauterberg, Eindhoven University of Technology, The Netherlands*

## **IFIP – The International Federation for Information Processing**

IFIP was founded in 1960 under the auspices of UNESCO, following the first World Computer Congress held in Paris the previous year. A federation for societies working in information processing, IFIP's aim is two-fold: to support information processing in the countries of its members and to encourage technology transfer to developing nations. As its mission statement clearly states:

*IFIP is the global non-profit federation of societies of ICT professionals that aims at achieving a worldwide professional and socially responsible development and application of information and communication technologies.*

IFIP is a non-profit-making organization, run almost solely by 2500 volunteers. It operates through a number of technical committees and working groups, which organize events and publications. IFIP's events range from large international open conferences to working conferences and local seminars.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is generally smaller and occasionally by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is also rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

IFIP distinguishes three types of institutional membership: Country Representative Members, Members at Large, and Associate Members. The type of organization that can apply for membership is a wide variety and includes national or international societies of individual computer scientists/ICT professionals, associations or federations of such societies, government institutions/government related organizations, national or international research institutes or consortia, universities, academies of sciences, companies, national or international associations or federations of companies.

More information about this series at <http://www.springer.com/series/6102>

Jaap-Henk Hoepman · Stefan Katzenbeisser (Eds.)

# ICT Systems Security and Privacy Protection

31st IFIP TC 11 International Conference, SEC 2016  
Ghent, Belgium, May 30 – June 1, 2016  
Proceedings

 Springer

*Editors*

Jaap-Henk Hoepman  
Institute for Computing and Information  
Sciences  
Radboud University Nijmegen  
Nijmegen  
The Netherlands

Stefan Katzenbeisser  
Security Engineering Group  
Technische Universität Darmstadt  
Darmstadt  
Germany

ISSN 1868-4238                      ISSN 1868-422X (electronic)  
IFIP Advances in Information and Communication Technology  
ISBN 978-3-319-33629-9              ISBN 978-3-319-33630-5 (eBook)  
DOI 10.1007/978-3-319-33630-5

Library of Congress Control Number: 2016937373

© 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

It is our great pleasure to present the proceedings of the 31st IFIP International Conference on ICT Systems Security and Privacy Protection, which was held in Ghent, Belgium, between May 30 and June 1, 2016. IFIP SEC conferences are the flagship events of the International Federation for Information Processing (IFIP) Technical Committee 11 on Information Security and Privacy Protection in Information Processing Systems (TC-11).

Continuing the tradition of previous years, we sought for a balanced program that covers all significant aspects of information security, ranging from software security over platform security to human factors. The selection of papers was a highly challenging task. We received 145 submissions in response to our call for papers, of which six were withdrawn before the reviewing process started. From these 139 submissions we selected 27 full papers to be presented at the conference, based on their significance, novelty, and technical quality. Each paper received at least three reviews by members of the Program Committee.

We wish to thank all contributors who helped make IFIP SEC 2016 a success: the authors who submitted their latest research results to the conference, as well as the members of the Program Committee who devoted significant amounts of their time to evaluate all submissions. We would like in particular to thank the organizing chair Vincent Naessens and the general chair Bart de Decker for their support and their efforts to organize the conference in beautiful Ghent.

We hope that this proceedings volume provides inspirations for future research in the area of information security!

March 2016

Stefan Katzenbeisser  
Jaap-Henk Hoepman

## Organization

### Program Committee

Gunes Acar	KU Leuven, Belgium
Luca Allodi	University of Trento, Italy
Frederik Armknecht	Universität Mannheim, Germany
Vijay Atluri	Rutgers University, USA
Matt Bishop	University of California at Davis, USA
Rainer Boehme	University of Innsbruck, Austria
Joan Borrell	Universitat Autònoma de Barcelona, Spain
Joppe Bos	NXP Semiconductors, Leuven, Belgium
Dagmar Brechlerova	Euromise Prague, Czech Republic
Christina Brzuska	Hamburg University of Technology, Germany
William Caelli	IISEC Pty Ltd., Australia
Jan Camenisch	IBM Research — Zurich, Switzerland
Iliano Cervesato	Carnegie Mellon University, USA
Eric Chan-Tin	Oklahoma State University, USA
Nathan Clarke	Centre for Security, Communication and Network Research, University of Plymouth, UK
Frédéric Cuppens	Telecom Bretagne, France
Nora Cuppens-Bouahia	Telecom Bretagne, France
Ernesto Damiani	University of Milan, Italy
Sabrina De Capitani di Vimercati	University of Milan, Italy
Mourad Debbabi	Concordia University, Canada
Andreas Dewald	University of Mannheim, Germany
Gurpreet Dhillon	Virginia Commonwealth University, USA
Theo Dimitrakos	Security Research Centre, BT Group CTO, UK
Jana Dittmann	University of Magdeburg, Germany
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Paul Dowland	Plymouth University, UK
Hannes Federrath	University of Hamburg, Germany
Simone Fischer-Hübner	Karlstad University, Sweden
William Michael Fitzgerald	United Technologies Research Centre Ireland, Ltd., Ireland
Sara Foresti	University of Milan, Italy
Felix Freiling	Friedrich-Alexander-Universität, Germany
Lothar Fritsch	Norsk Regnesentral — Norwegian Computing Center, Norway
Steven Furnell	Plymouth University, UK

VIII Organization

Lynn Fitcher	IFIP WG 11.8 (Vice-chair), South Africa
Dieter Gollmann	Hamburg University of Technology, Germany
Stefanos Gritzalis	University of the Aegean, Greece
Seda Gürses	NYU, USA
Marit Hansen	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Germany
Karin Hedström	Swedish Business School, Örebro University, Sweden
Andreas Heinemann	Hochschule Darmstadt — University of Applied Sciences, Germany
Dominik Herrmann	University of Hamburg, Germany
Michael Herrmann	KU Leuven ESAT/COSIC, iMinds, Belgium
Alejandro Hevia	University of Chile, Chile
Jaap-Henk Hoepman	Radboud University Nijmegen, The Netherlands
Ralph Holz	NICTA, Australia
Xinyi Huang	Fujian Normal University, China
Sushil Jajodia	George Mason University, USA
Lech Janczewski	The University of Auckland, New Zealand
Christian Damsgaard Jensen	Technical University of Denmark
Thomas Jensen	Inria, France
Martin Johns	SAP Research, Germany
Wouter Joosen	Katholieke Universiteit Leuven, Belgium
Audun Josang	University of Oslo, Norway
Sokratis Katsikas	University of Piraeus, Greece
Stefan Katzenbeisser	TU Darmstadt, Germany
Florian Kerschbaum	SAP, Germany
Dogan Kesdogan	Universität Regensburg, Germany
Kwangjo Kim	KAIST, South Korea
Valentin Kisimov	UNWE, Bulgaria
Zbigniew Kotulski	Warsaw University of Technology, Poland
Stefan Köpsell	TU Dresden, Germany
Ronald Leenes	Tilburg University – TILT, The Netherlands
Luigi Logrippo	Université du Québec en Outaouais, Canada
Javier Lopez	University of Malaga, Spain
Emil Lupu	Imperial College, UK
Stephen Marsh	UOIT, UK
Fabio Martinelli	IIT-CNR, Italy
Michael Meier	University of Bonn, Fraunhofer FKIE, Germany
Martin Mulazzani	SBA Research, Austria
Yuko Murayama	Iwate Prefectural University, Japan
Eiji Okamoto	University of Tsukuba, Japan
Daniel Olejar	Comenius University, Slovakia
Federica Paci	University of Southampton, UK
Jakob Illeborg Pagter	Centre for IT Security, The Alexandra Institute Ltd., Denmark
Sebastian Pape	Goethe University Frankfurt, Germany
Philipp Peleties	Cyprus Computer Society, Cyprus

Günther Pernul	Universität Regensburg, Germany
Andreas Peter	University of Twente, The Netherlands
Gilbert Peterson	US Air Force Institute of Technology, USA
Wolter Pieters	TBM-ESS, Delft University of Technology, The Netherlands
Joachim Posegga	University of Passau, Germany
Sihan Qing	Peking University, China
Kai Rannenberg	Goethe University Frankfurt, Germany
Indrajit Ray	Colorado State University, USA
Indrakshi Ray	Colorado State University, USA
Konrad Rieck	University of Göttingen, Germany
Carlos Rieder	ISEC AG, Switzerland
Yves Roudier	EURECOM, France
Mark Ryan	University of Birmingham, UK
Peter Ryan	University of Luxembourg, Luxembourg
Pierangela Samarati	Università degli Studi di Milano, Italy
Thierry Sans	Carnegie Mellon University in Qatar
Damien Sauveron	University of Limoges, France
Ingrid Schaumüller-Bichl	Upper Austrian University of Applied Sciences Campus Hagenberg, Austria
Björn Scheuermann	Humboldt University of Berlin, Germany
Sebastian Schinzel	Münster University of Applied Sciences, Germany
Joerg Schwenk	Ruhr-Universität Bochum, Germany
Anne Karen Seip	Finanstilsynet, Norway
Jetzabel Maritza Serna Olvera	Universidad Politecnica de Cataluña, Spain
Abbas Shahim	VU University Amsterdam, The Netherlands
Haya Shulman	Technische Universität Darmstadt, Germany
Adesina S. Sodiya	Federal University of Agric, Abeokuta, Nigeria
Radu State	University of Luxembourg, Luxembourg
Jakub Szefer	Yale University, USA
Kerry-Lynn Thomson	Nelson Mandela Metropolitan University, South Africa
Nils Ole Tippenhauer	Singapore University of Technology and Design, Singapore
Carmela Troncoso	Gradiant, Spain
Markus Tschersich	Goethe University Frankfurt, Germany
Pedro Veiga	University of Lisbon, Portugal
Michael Vielhaber	Hochschule Bremerhaven, Germany
Melanie Volkamer	Technische Universität Darmstadt, Germany
Rossouw Von Solms	Nelson Mandela Metropolitan University, South Africa
Jozef Vyskoc	VaF, Slovak Republic
Lingyu Wang	Concordia University, Canada
Christian Weber	Ostfalia University of Applied Sciences, Germany
Edgar Weippl	SBA Research, Austria
Tatjana Welzer	University of Maribor, Slovenia
Steffen Wendzel	Fraunhofer FKIE, Germany



X      Organization

Gunnar Wenngren

Jeff Yan

Zhenxin Zhan

André Zúquete

AB Wenngrens i Linköping, Sweden

Newcastle University, UK

University of Texas at San Antonio, USA

IEETA, University of Aveiro, Portugal

# Contents

## Cryptographic Protocols

Coercion-Resistant Proxy Voting. . . . .	3
<i>Oksana Kulyk, Stephan Neumann, Karola Marky, Jurlind Budurushi, and Melanie Volkamer</i>	
A Posteriori Openable Public Key Encryption. . . . .	17
<i>Xavier Bultel and Pascal Lafourcade</i>	
Multicast Delayed Authentication for Streaming Synchronphasor Data in the Smart Grid. . . . .	32
<i>Sérgio Câmara, Dhananjay Anand, Victoria Pillitteri, and Luiz Carmo</i>	

## Human Aspects of Security

Developing a Human Activity Model for Insider IS Security Breaches Using Action Design Research . . . . .	49
<i>Gurpreet Dhillon, Spyridon Samonas, and Ugo Etudo</i>	
Evaluating CVSS Base Score Using Vulnerability Rewards Programs . . . . .	62
<i>Awad Younis, Yashwant K. Malaiya, and Indrajit Ray</i>	
Defining Objectives for Preventing Cyberstalking . . . . .	76
<i>Gurpreet Dhillon, Chandrashekar Challa, and Kane Smith</i>	

## Cyber Infrastructure

Using Process Invariants to Detect Cyber Attacks on a Water Treatment System . . . . .	91
<i>Sridhar Adepu and Aditya Mathur</i>	
Expression and Enforcement of Security Policy for Virtual Resource Allocation in IaaS Cloud . . . . .	105
<i>Yanhuang Li, Nora Cuppens-Boulahia, Jean-Michel Crom, Frédéric Cuppens, and Vincent Frey</i>	
Software Defined Networking Reactive Stateful Firewall . . . . .	119
<i>Salaheddine Zerkane, David Espes, Philippe Le Parc, and Frederic Cuppens</i>	

**Phishing and Data Sharing**

Teaching Phishing-Security: Which Way is Best? . . . . . 135  
*Simon Stockhardt, Benjamin Reinheimer, Melanie Volkamer,  
 Peter Mayer, Alexandra Kunz, Philipp Rack, and Daniel Lehmann*

On Gender Specific Perception of Data Sharing in Japan . . . . . 150  
*Markus Tschersich, Shinsaku Kiyomoto, Sebastian Pape,  
 Toru Nakamura, Gökhan Bal, Haruo Takasaki, and Kai Rannenber*

TORPEDO: TOoltip-poweRed Phishing Email DetectiOn. . . . . 161  
*Melanie Volkamer, Karen Renaud, and Benjamin Reinheimer*

**Social Networks**

SybilRadar: A Graph-Structure Based Framework for Sybil Detection  
 in On-line Social Networks . . . . . 179  
*Dieudonné Mulamba, Indrajit Ray, and Indrakshi Ray*

Collateral Damage of Facebook Apps: Friends, Providers,  
 and Privacy Interdependence . . . . . 194  
*Iraklis Symeonidis, Fatemeh Shirazi, Gergely Biczók,  
 Cristina Pérez-Solà, and Bart Preneel*

**Software Vulnerabilities**

Automated Source Code Instrumentation for Verifying Potential  
 Vulnerabilities . . . . . 211  
*Hongzhe Li, Jaesang Oh, Hakjoo Oh, and Heejo Lee*

An Information Flow-Based Taxonomy to Understand the Nature  
 of Software Vulnerabilities . . . . . 227  
*Daniela Oliveira, Jedidiah Crandall, Harry Kalodner, Nicole Morin,  
 Megan Maher, Jesus Navarro, and Felix Emiliano*

XSS PEEKER: Dissecting the XSS Exploitation Techniques and Fuzzing  
 Mechanisms of Blackbox Web Application Scanners . . . . . 243  
*Enrico Bazzoli, Claudio Criscione, Federico Maggi, and Stefano Zanero*

**TPM and Internet of Things**

A Utility-Based Reputation Model for the Internet of Things . . . . . 261  
*Benjamin Aziz, Paul Fremantle, Rui Wei, and Alvaro Arenas*

Advanced Remote Firmware Upgrades Using TPM 2.0 . . . . . 276  
*Andreas Fuchs, Christoph Krauß, and Jürgen Repp*

**Sidechannel Analysis**

RegRSA: Using Registers as Buffers to Resist Memory Disclosure Attacks. . . 293  
*Yuan Zhao, Jingqiang Lin, Wuqiong Pan, Cong Xue, Fangyu Zheng,  
and Ziqiang Ma*

Uncertain? No, It’s Very Certain!: Recovering the Key from Guessing  
Entropy Enhanced CPA . . . . . 308  
*Changhai Ou, Zhu Wang, Degang Sun, Xinping Zhou, and Juan Ai*

**Software Security**

Advanced or Not? A Comparative Study of the Use of Anti-debugging  
and Anti-VM Techniques in Generic and Targeted Malware. . . . . 323  
*Ping Chen, Christophe Huygens, Lieven Desmet, and Wouter Joosen*

NativeProtector: Protecting Android Applications by Isolating  
and Intercepting Third-Party Native Libraries . . . . . 337  
*Yu-Yang Hong, Yu-Ping Wang, and Jie Yin*

A Progress-Sensitive Flow-Sensitive Inlined Information-Flow  
Control Monitor . . . . . 352  
*Andrew Bedford, Stephen Chong, Josée Desharnais, and Nadia Tawbi*

**Privacy**

Deducing User Presence from Inter-Message Intervals in Home  
Automation Systems . . . . . 369  
*Frederik Möllers and Christoph Sorge*

Privacy by Design Principles in Design of New Generation Cognitive  
Assistive Technologies. . . . . 384  
*Ella Kolkowska and Annica Kristofferson*

A Trustless Privacy-Preserving Reputation System . . . . . 398  
*Alexander Schaub, Rémi Bazin, Omar Hasan, and Lionel Brunie*

**Author Index** . . . . . 413