

## ICT Systems Security and Privacy Protection

Lech Jan Janczewski, Mirosław Kutylowski

► **To cite this version:**

Lech Jan Janczewski, Mirosław Kutylowski. ICT Systems Security and Privacy Protection: 33rd IFIP TC 11 International Conference, SEC 2018, Held at the 24th IFIP World Computer Congress, WCC 2018, Poznan, Poland, September 18-20, 2018, Proceedings. Springer International Publishing, AICT-529, 2018, IFIP Advances in Information and Communication Technology, 978-3-319-99827-5. 10.1007/978-3-319-99828-2 . hal-02023737

**HAL Id: hal-02023737**

**<https://hal.inria.fr/hal-02023737>**

Submitted on 21 Feb 2019

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



## Editor-in-Chief

*Kai Rannenberg, Goethe University Frankfurt, Germany*

## Editorial Board

TC 1 – Foundations of Computer Science

*Jacques Sakarovitch, Télécom ParisTech, France*

TC 2 – Software: Theory and Practice

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

TC 3 – Education

*Arthur Tatnall, Victoria University, Melbourne, Australia*

TC 5 – Information Technology Applications

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

TC 6 – Communication Systems

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

TC 7 – System Modeling and Optimization

*Fredi Tröltzsch, TU Berlin, Germany*

TC 8 – Information Systems

*Jan Pries-Heje, Roskilde University, Denmark*

TC 9 – ICT and Society

*David Kreps, University of Salford, Greater Manchester, UK*

TC 10 – Computer Systems Technology

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

TC 11 – Security and Privacy Protection in Information Processing Systems

*Steven Furnell, Plymouth University, UK*

TC 12 – Artificial Intelligence

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

TC 13 – Human-Computer Interaction

*Marco Winckler, University Paul Sabatier, Toulouse, France*

TC 14 – 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>


Lech Jan Janczewski · Mirosław Kutylowski (Eds.)

# ICT Systems Security and Privacy Protection

33rd IFIP TC 11 International Conference, SEC 2018  
Held at the 24th IFIP World Computer Congress, WCC 2018  
Poznan, Poland, September 18–20, 2018  
Proceedings

*Editors*

Lech Jan Janczewski   
University of Auckland  
Auckland  
New Zealand

Mirosław Kutylowski   
Wrocław University of Technology  
Wrocław  
Poland

ISSN 1868-4238 ISSN 1868-422X (electronic)  
IFIP Advances in Information and Communication Technology  
ISBN 978-3-319-99827-5 ISBN 978-3-319-99828-2 (eBook)  
<https://doi.org/10.1007/978-3-319-99828-2>

Library of Congress Control Number: 2018952247

© IFIP International Federation for Information Processing 2018

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. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

This year, the annual IFIP TC-11 (International Federation for Information Processing Technical Committee) Sec 2018 conference was the 33rd in the series. This conference is part of the World Computer Congress (WCC) organized by the IFIP. Major IFIP partners in the Congress are: the Committee on Informatics of the Polish Academy of Sciences, the Polish Information Processing Society Wielkopolska Branch, Poznan University of Technology, The Polish Ministry of Digital Affairs, and the Polish Ministry of Science and Higher Education; the Mayor of Poznan provided WCC Honorary Patronage. The conference was held in the Lecture and Conference Centre of the Poznan University of Technology in the city of Poznan, Poland.

The Program Committee, consisting of 100 members, considered 89 papers. These proceedings include the revised versions of the 27 papers presented at the conference. Therefore, the overall acceptance rate for this conference is 30%. These papers were selected on the basis of originality, quality, and relevance to security and privacy. As a result, they give an accurate picture of how the field is evolving.

The selection of papers was a difficult and challenging task. Each submission was refereed usually by at least four reviewers. We used the single-blind review principle. We wish to thank the Program Committee members for their great effort. In addition, we gratefully acknowledge the help of a large number of external reviewers. All reviewers are listed in the section following this preface. We apologize for any inadvertent omission.

Many thanks to the creators of EasyChair without which the management of submissions for this conference would have been a nightmare. It would be difficult to imagine organizing and administering a conference without this valuable tool. Special thanks to Prof. Jacek Cichoń and the Department of Computer Science of Wrocław University of Science and Technology for technical support in Web communication.

Finally, we wish to thank the all authors who submitted papers for making this conference possible by providing the scientific material, and especially the authors of accepted papers. We would also like to thank the publisher, Springer, for working within a tight schedule to produce these proceedings in due time.

July 2018

Lech Jan Janczewski  
Mirośław Kutylowski

# IFIP TC-11 SEC 2018

September 18–20, 2018, Poznan, Poland

Sponsored by the

*International Federation for Information Processing (IFIP)*

## General Chairs

Kai Rannenberg  
Yuko Murayama

Goethe University, Frankfurt a. Main, Germany  
Iwate Prefectural University, Japan

## Program Chairs

Mirosław Kutylowski

Wrocław University of Science  
and Technology – Wrocław, Poland

Lech Janczewski

The University of Auckland, Auckland, New Zealand

## Program Committee

Adnan Ahmad

Government College University Lahore, Pakistan

Vijay Atluri

Rutgers University, USA

Man Ho Au

The Hong Kong Polytechnic University, Hong Kong

Gildas Avoine

IRISA, Rennes, France

Gergei Bana

Inria, France

Amel Bennaceur

The Open University, UK

Jan Camenisch

IBM Research - Zurich, Switzerland

Herve Chabanne

Morpho, France

Michal Choras

ITTI Ltd., Poland

K P Chow

The University of Hong Kong, Hong Kong

Nathan Clarke

Centre for Security, Communication & Network  
Research, University of Plymouth, UK

Nora Cuppens

IMT Atlantique, France

Brian Cusack

AUT University, New Zealand

Paolo D'Arco

University of Salerno, Italy

Ed Dawson

Queensland University of Technology, Australia

Sabrina De Capitani di  
Vimercati

University of Milan, Italy

Bart De Decker

Katholieke Universiteit Leuven, Belgium

Roberto De Prisco

University of Salerno, Italy

Vesna Dimitrova

Ss. Cyril and Methodius University of Skopje,  
Macedonia

Itai Dinur

Ben Gurion University, Israel

Shlomi Dolev

Ben Gurion University of the Negev, Israel

Hannes Federrath	University of Hamburg, Germany
Simone Fischer-Hübner	Karlstad University, Sweden
Sara Foresti	Politecnico di Milano, Italy
Felix Freiling	Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany
Steven Furnell	Plymouth University, UK
Chaya Ganesh	Aarhus University, Denmark
Niv Gilboa	Ben Gurion University, Israel
Lucjan Hanzlik	CISPA, Poland
Karin Hedström	Swedish Business School, Örebro University, Sweden
Julio Hernandez-Castro	University of Kent, UK
Dominik Herrmann	University of Bamberg, Germany
Marko Hölbl	University of Maribor, Faculty of Electrical Engineering and Computer Science, Slovenia
Xinyi Huang	Fujian Normal University, China
Dieter Hutter	DFKI GmbH, Germany
Pedro Inácio	Universidade da Beira Interior, Portugal
Martin Gilje Jaatun	SINTEF Digital, Norway
Wojciech Jamroga	Polish Academy of Sciences, Poland
Audun Jøsang	University of Oslo, Norway
Jan Jürjens	Fraunhofer Institute for Software & Systems Engineering ISST and University of Koblenz-Landau, Germany
Georgios Kambourakis	University of the Aegean, Greece
Dogan Kesdogan	Universität Regensburg, Germany
Dong Seong Kim	University of Canterbury, New Zealand
Kamil Kluczniak	Hong Kong Polytechnic, Hong Kong
Zbigniew Kotulski	Warsaw University of Technology, Poland
Matthias Krause	University of Mannheim, Germany
Lukasz Krzywiecki	Wroclaw University of Technology, Poland
Lam For Kwok	City University of Hong Kong, Hong Kong
Heejo Lee	Korea University, South Korea
Yingjiu Li	Singapore Management University, Singapore
Maciej Liskiewicz	Institut für Theoretische Informatik, University Luebeck, Germany
Luigi Logrippo	Université du Québec en Outaouais, Canada
Javier Lopez	NICS Lab, Spain
Marian Margraf	Freie Universität Berlin, Germany
Konstantinos Markantonakis	ISG-Smart Card Centre, Founded by Vodafone, G&D and the Information Security Group of Royal Holloway, University of London, UK
Vashek Matyas	Masaryk University, Switzerland
Gert Læssøe Mikkelsen	The Alexandra Institute, Denmark
Pawel Morawiecki	IPI PAN, Poland
Yuko Murayama	Tsuda University, Japan
Maurizio Naldi	Università di Roma Tor Vergata, Italy



Jetzabel Maritza Serna Olvera	Universitat Politècnica de Catalunya, Spain
Brajendra Nath Panda	University of Arkansas, USA
Sebastian Pape	Goethe University Frankfurt, Germany
Stefano Paraboschi	Universita di Bergamo, Italy
Ludovic Perret	UPMC/LIP6 INRIA/SALSA, France
Gibert Peterson	US Air Force Institute of Technology, USA
Raphael C.-W. Phan	Loughborough University, UK
Alexander Pretschner	Technical University of Munich, Germany
Rami Puzis	Ben Gurion University of the Negev, Israel
Rui Qiao	Virginia Polytechnic Institute and State University, Roanoke, USA
Kai Rannenber	Goethe University Frankfurt, Germany
Indrajit Ray	Colorado State University, USA
Akram Rn	ISG-Smart Card Centre, Royal Holloway, University of London, UK
Juha Rönig	University of Oulu, Finland
Reyhaneh Safavi-Naini	University of Calgary, Canada
Pierangela Samarati	University of Milan, Italy
Ingrid Schaumueller - Bichl	Upper Austrian University of Applied Sciences Campus Hagenberg, Austria
Annikken Seip	Finanstilsynet, Norway
Jun Shao	Hangzhou Gongshang University, China
Nicolas Sklavos	University of Patras, Greece
Daniel Slamanig	AIT Austrian Institute of Technology, Austria
Agusti Solanas	Universitat Rovira i Virgili, Spain
Gene Spafford	Purdue University, USA
Chunhua Su	Osaka University, Japan
Shamik Sural	IIT, Kharagpur, India
Neeraj Suri	TU Darmstadt, Germany
Willy Susilo	University of Wollongong, Australia
Theo Tryfonas	University of Bristol, UK
Ding Wang	Peking University, China
Jianfeng Wang	Xidian University, China
Edgar Weippl	SBA Research, Austria
Tatjana Welzer Družovec	University of Maribor, Slovenia
Henry Wolfe	University of Otago, New Zealand
Qianhong Wu	Beihang University, China
Filip Zagorski	Wroclaw University of Technology, Poland
Yuexin Zhang	Deakin University, Australia

**Additional Reviewers**

Mayank Agarwal

Mohsen Ahmadvand

Marios Anagnostopoulos

Yusuf Baha

Przemyslaw Blaskiewicz

Haibo Cheng

Anastasia Douma

Jürgen Dürwang

Maciej Gebala

Amjad Ibrahim

Michał Knapik

Stephan Krenn

Damian Kurpiewski

Laurens Lemaire

Wenting Li

Jens Lindemann

Matthias Marx

Mevludin Memedi

Tilo Müller

Ralph Palutke

Dimitrios Papamartzivanos

Andreas Put

Marcin Slowik

Witold Waligora

Marcin Zawada

# Contents

## Authentication

Design Weaknesses in Recent Ultralightweight RFID Authentication Protocols . . . . .	3
<i>P. D'Arco and R. De Prisco</i>	
CPMap: Design of Click-Points Map-Based Graphical Password Authentication . . . . .	18
<i>Weizhi Meng, Fei Fei, Lijun Jiang, Zhe Liu, Chunhua Su, and Jinguang Han</i>	
The Influence of Native Language on Password Composition and Security: A Socioculture Theoretical View . . . . .	33
<i>Pardon Blessings Maoneke, Stephen Flowerday, and Naomi Isabirye</i>	
A Hypergame Analysis for ErsatzPasswords . . . . .	47
<i>Christopher N. Gutierrez, Mohammed H. Almeshekah, Saurabh Bagchi, and Eugene H. Spafford</i>	
Walking Through the Deep: Gait Analysis for User Authentication Through Deep Learning . . . . .	62
<i>Giacomo Giorgi, Fabio Martinelli, Andrea Saracino, and Mina Sheikhalishahi</i>	

## Failures of Security Management

Practical Cryptographic Data Integrity Protection with Full Disk Encryption . . . . .	79
<i>Milan Brož, Mikuláš Patočka, and Vashek Matyáš</i>	
When Your Browser Becomes the Paper Boy: An Anonymous Browser Network . . . . .	94
<i>Juan D. Parra Rodriguez, Eduard Brehm, and Joachim Posegga</i>	
EMPower: Detecting Malicious Power Line Networks from EM Emissions . . . . .	108
<i>Richard Baker and Ivan Martinovic</i>	
Attacking RO-PUFs with Enhanced Challenge-Response Pairs . . . . .	122
<i>Nils Wisiol and Marian Margraf</i>	

A Security Analysis of FirstCoin. . . . . 127  
*Alexander Marsalek, Christian Kollmann, and Thomas Zefferer*

PRETT: Protocol Reverse Engineering Using Binary Tokens  
and Network Traces . . . . . 141  
*Choongin Lee, Jeonghan Bae, and Heejo Lee*

Assessing Privacy Policies of Internet of Things Services. . . . . 156  
*Niklas Paul, Welderufael B. Tesfay, Dennis-Kenji Kipker,  
Mattea Stelter, and Sebastian Pape*

JonDonym Users' Information Privacy Concerns. . . . . 170  
*David Harborth and Sebastian Pape*

**Security Management / Forensic**

Optimal Security Configuration for Cyber Insurance . . . . . 187  
*Fabio Martinelli, Ganbayar Uuganbayar, and Artsiom Yautsiukhin*

The Tweet Advantage: An Empirical Analysis of 0-Day Vulnerability  
Information Shared on Twitter . . . . . 201  
*Clemens Sauerwein, Christian Sillaber, Michael M. Huber,  
Andrea Mussmann, and Ruth Breu*

Anti-forensic = Suspicious: Detection of Stealthy Malware that Hides  
Its Network Traffic . . . . . 216  
*Mayank Agarwal, Rami Puzis, Jawad Haj-Yahya, Polina Zilberman,  
and Yuval Elovici*

Usability Characteristics of Security and Privacy Tools:  
The User's Perspective . . . . . 231  
*Ioanna Topa and Maria Karyda*

Efficient Identification of Applications in Co-resident VMs via a  
Memory Side-Channel . . . . . 245  
*Jens Lindemann and Mathias Fischer*

**Software Security / Attacks**

Follow the WhiteRabbit: Towards Consolidation of On-the-Fly  
Virtualization and Virtual Machine Introspection. . . . . 263  
*Sergej Proskurin, Julian Kirsch, and Apostolis Zarras*

Hunting Password Leaks in Android Applications. . . . . 278  
*Johannes Feichtner*

Smashing the Stack Protector for Fun and Profit . . . . . 293  
*Bruno Bierbaumer, Julian Kirsch, Thomas Kittel, Aurélien Francillon,  
and Apostolis Zarras*

Formal Analysis of Sneak-Peek: A Data Centre Attack and Its Mitigations. . . 307  
*Wei Chen, Yuhui Lin, Vashti Galpin, Vivek Nigam, Myungjin Lee,  
and David Aspinall*

An Evaluation of Bucketing in Systems with Non-deterministic  
Timing Behavior . . . . . 323  
*Yuri Gil Dantas, Richard Gay, Tobias Hamann, Heiko Mantel,  
and Johannes Schickel*

Detection and Response to Data Exfiltration from Internet of Things  
Android Devices . . . . . 339  
*Mariem Graa, Ivan Marco Lobe Kome, Nora Cuppens-Boulahia,  
Frédéric Cuppens, and Vincent Frey*

When George Clooney Is Not George Clooney: Using *GenAttack*  
to Deceive Amazon’s and Naver’s Celebrity Recognition APIs. . . . . 355  
*Keyoung Kim and Simon S. Woo*

Performance Improvements in Behavior Based Malware  
Detection Solutions . . . . . 370  
*Gheorghe Hăjmășan, Alexandra Mondoc, Radu Portase,  
and Octavian Creț*

On the Integrity of Cross-Origin JavaScripts . . . . . 385  
*Jukka Ruohonen, Joonas Salovaara, and Ville Leppänen*

**Author Index** . . . . . 399