


Editor-in-Chief

Kai Rannenberg, Goethe University Frankfurt, Germany

Editorial Board Members

TC 1 – Foundations of Computer Science

Luis Soares Barbosa , University of Minho, Braga, Portugal

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

Burkhard Stiller, University of Zurich, Zürich, Switzerland

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

Eunika Mercier-Laurent , University of Reims Champagne-Ardenne, Reims, France

TC 13 – Human-Computer Interaction

Marco Winckler , University of Nice Sophia Antipolis, France

TC 14 – Entertainment Computing

Rainer Malaka, University of Bremen, Germany

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>

Marko Hölbl · Kai Rannenberg ·
Tatjana Welzer (Eds.)

ICT Systems Security and Privacy Protection

35th IFIP TC 11 International Conference, SEC 2020
Maribor, Slovenia, September 21–23, 2020
Proceedings

Editors

Marko Hölbl 
University of Maribor
Maribor, Slovenia

Tatjana Welzer
University of Maribor
Maribor, Slovenia

Kai Rannenberg
Goethe University Frankfurt
Frankfurt, Germany

ISSN 1868-4238 ISSN 1868-422X (electronic)
IFIP Advances in Information and Communication Technology
ISBN 978-3-030-58200-5 ISBN 978-3-030-58201-2 (eBook)
<https://doi.org/10.1007/978-3-030-58201-2>

© IFIP International Federation for Information Processing 2020

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, expressed 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

In these challenging times caused by the COVID-19 situation, we are honored to bring you this collection of the best papers submitted to the 35th IFIP International Conference on ICT Systems Security and Privacy Protection, which was held in Maribor, Slovenia, September 21–23, 2020. 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).

The 2020 edition of the IFIP SEC proceedings includes 29 high-quality papers covering a wide range of research areas in the information security field. They were authored by researchers from 19 different countries. The selection of papers was a highly challenging task: 149 received submissions were evaluated based on their significance, novelty, and technical quality. Each paper received at least three, but most of them four reviews by members of the Program Committee. The Program Committee meetings were held electronically, with intensive discussions over a period of three weeks. Of the papers submitted, 29 were selected for presentation at the conference, leading to an acceptance rate of 19.5%.

We want to express our appreciation to all the contributors who helped to make IFIP SEC 2020 a success. There is a long list of people who volunteered their time and energy to put together the conference and who deserve acknowledgement. We want to thank the members of the Program Committee and the external reviewers, who devoted significant amounts of their time to evaluate all the submissions. Special thanks go to the keynote speakers Elisa Bertino from Purdue University West Lafayette, USA, and Stanka Šalamun and Mitja Kolšek from Opatch by ACROS Security, Slovenia, who accepted our invitation to present their insights at the conference.

Further individuals who deserve special thanks and without whom the current program and success of the conference would not have been possible include: the organizing chair Lili Nemeč Zlatolas and the members of the Organizing Committee Borut Zlatolas, Luka Hrgarek, and Marko Kompara, all from the University of Maribor, Faculty of Electrical Engineering and Computer Science. They kept all things smooth and flowing, even after the delays caused by the pandemic. The IFIP SEC and WISE had to be postponed without clear information on when public events like it could be safely held again. The IFIP Summer School, which was being organized separately, also got postponed and found a new home at IFIP SEC 2020. Due to the constant changes in local regulation, the questionable safety of international travel and uncertainty regarding the future spread of the disease, the decision was made to hold the conference virtually, despite the best efforts to have it in Maribor, Slovenia. Special recognition goes to Hotel City Maribor and the Maribor Convention Bureau, who were very accommodating and understanding regardless of the economic impact of the unfortunate situation, and we express our regret to the participants, for missing the opportunity to see the beauty Slovenia has to offer.

We also acknowledge the institutional support for IFIP SEC 2020, which came from the University of Maribor, Faculty of Electrical Engineering and Computer Science, Institute of Informatics. Without this support, it would not have been possible to organize the conference.

Last but certainly not least, we thank all the authors who submitted papers and all the conference's attendees who coped with the changing circumstances in a kind and flexible manner.

We hope you find the proceedings of IFIP SEC 2020 interesting, stimulating, and inspiring for your future research regardless of the challenging times in which the conference took place.

July 2020

Marko Hölbl
Kai Rannenberg
Tatjana Welzer

Organization

General Chair

Tatjana Welzer University of Maribor, Slovenia

Program Committee Chairs

Marko Hölbl University of Maribor, Slovenia
Kai Rannenberg Goethe University Frankfurt, Germany

Organizing Chair

Lili Nemeč Zlatolas University of Maribor, Slovenia

Program Committee

Rose-Mharie Åhlfeldt University of Skövde, Sweden
Raja Naeem Akram Royal Holloway, University of London, UK
Vijay Atluri Rutgers University, USA
Man Ho Au The University of Hong Kong, China
Gergei Bana University of Missouri, USA
Joao Paulo Barraca University of Aveiro, Portugal
Pedro Brandão University of Porto, Portugal
Dagmar Brechlerova EuroMISE Prague, Czech Republic
Ricardo Chaves IST, INESC-ID, Portugal
Michal Choras ITTI Ltd., Poland
K. P. Chow The University of Hong Kong, China
Nathan Clarke University of Plymouth, UK
Miguel Correia Universidade de Lisboa, Portugal
Nora Cuppens-Boulahia Polytechnique Montréal, Canada
Paolo D'Arco Università di Salerno, Italy
Ed Dawson QUT, Australia
Sabrina De Capitani di Università degli Studi di Milano, Italy
 Vimercati
Bart De Decker Katholieke Universiteit Leuven, Belgium
Nicola Dragoni Technical University of Denmark, Denmark
Nicolás Emilio Daz Ferreyra University of Duisburg-Essen, Germany
Isao Echizen National Institute of Informatics, Japan
Simone Fischer-Hübner Karlstad University, Sweden
Sara Foresti Università degli Studi di Milano, Italy
Steven Furnell University of Plymouth, UK
Chaya Ganesh Aarhus University, Denmark

Hélder Gomes	Universidade de Aveiro, Portugal
Jonas Hallberg	Swedish Defence Research Agency (FOI), Sweden
Lucjan Hanzlik	Stanford University, USA
Paul Haskell-Dowland	Edith Cowan University, Australia
Karin Hedström	Örebro University, Sweden
Dominik Herrmann	University of Bamberg, Germany
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	University of Luxembourg, Luxembourg
Lech Janczewski	The University of Auckland, New Zealand
Christian Damsgaard Jensen	Technical University of Denmark, Denmark
Allen Johnston	University of Alabama, USA
Audun Josang	University of Oslo, Norway
Jan Jürjens	Fraunhofer Institute and University of Koblenz-Landau, Germany
Georgios Kambourakis	University of the Aegean, Greece
Fredrik Karlsson	Örebro University, Sweden
Dogan Kesdogan	Universität Regensburg, Germany
Dongseong Kim	The University of Queensland, Australia
Kamil Kluczniak	Helmholtz Center for Information Security - CISPA, Germany
Andrea Kolberger	University of Applied Sciences Upper Austria, Austria
Marko Kompara	University of Maribor, Slovenia
Zbigniew Kotulski	Warsaw University of Technology, Poland
Lukasz Krzywiecki	Wrocław University of Science and Technology, Poland
Mirosław Kutylowski	Wrocław University of Science and Technology, Poland
Kwangjo Kim	Korea Advanced Institute of Science and Technology, South Korea
Heejo Lee	Korea University, South Korea
Yingjiu Li	University of Oregon, USA
Maciej Liskiewicz	University of Luebeck, Germany
Luigi Logrippo	Université du Québec en Outaouais, Canada
Javier Lopez	University of Malaga, Spain
Suryadipta Majumdar	University at Albany, SUNY, USA
Marian Margraf	FU Berlin, Germany
Fabio Martinelli	IIT-CNR, Italy
Vashek Matyas	Masaryk University, Czech Republic
Zlatogor Minchev	Bulgarian Academy of Sciences, Bulgaria
Yuko Murayama	Tsuda College, Japan
Maurizio Naldi	LUMSA Università Maria SS. Assunta di Roma, Italy
Lili Nemeč Zlatolas	University of Maribor, Slovenia

Sergio Nunes	ISEG - School of Economics and Management, Portugal
Balaji Palanisamy	University of Pittsburgh, USA
Brajendra Panda	University of Arkansas, USA
Sebastian Pape	Goethe University Frankfurt, Germany
Stefano Paraboschi	Università di Bergamo, Italy
Miguel Pardal	Universidade de Lisboa, Portugal
Gilbert Peterson	US Air Force Institute of Technology, USA
António Pinto	ESTG, P.Porto, Portugal
Rami Puzis	Ben-Gurion University of the Negev, Israel
Arun Raghuramu	Forescout Technologies Inc., USA
Carlos Rieder	Isec AG, Switzerland
Juha Rönning	University of Oulu, Finland
Elham Rostami	Örebro University, Sweden
Reyhaneh Safavi-Naini	University of Calgary, Canada
Pierangela Samarati	Università degli Studi di Milano, Italy
Damien Sauveron	Université de Limoges, France
Ingrid Schaumüller-Bichl	Upper Austrian University of Applied Sciences Campus Hagenberg, Austria
Jetzabel Maritza Serna Olvera	Universitat Politècnica de Catalunya, Spain
Paria Shirani	Concordia University, Canada
Nicolas Sklavos	University of Patras, Greece
Daniel Slamanig	AIT Austrian Institute of Technology, Austria
Kane Smith	University of North Carolina at Greensboro, USA
Agusti Solanas	Rovira i Virgili University, Spain
Teodor Sommestad	Swedish Defence Research Agency (FOI), Sweden
Chunhua Su	Osaka University, Japan
Shamik Sural	Indian Institute of Technology, India
Kerry-Lynn Thomson	Nelson Mandela University, South Africa
Muhamed Turkanović	University of Maribor, Slovenia
Rossouw Vonsolms	Nelson Mandela University, South Africa
Jozef Vyskoc	VaF, Slovakia
Ding Wang	Peking University, China
Lingyu Wang	Concordia University, Canada
Edgar Weippl	University of Vienna, SBA Research, Austria
Vladimir Zadorozhny	University of Pittsburgh, USA
Filip Zagorski	Wroclaw University of Technology, Poland
Yuexin Zhang	Swinburne University of Technology, Australia
André Zúquete	University of Aveiro, Portugal

Additional Reviewers

Mohiuddin Ahmed
Marios Anagnostopoulos
Arash Atashpendar
Sebastian Berndt
Olivier Blazy
Rohit Chadha
Aveek Kumar Das
Tiago Dias
Rong Huang
Vincenzo Iovino
Andreas Jakoby
Manfred Jeusfeld
Jan Kalbantner
Kallol Krishna Karmakar
Joakim Kävrestad
Mathieu Klingler
Vasileios Kouliaridis
Chengjun Lin
Chao Lin
Chang Liu
Francesco Mercaldo
Louis Moreau
Hong-Huy Nguyen
Wojciech Niewolski
Fahad Nife
Jianting Ning
Marcus Nohlberg

Tomasz Nowak
Tomás Oliveira E Silva
Oleksii Osliak
Ali Padyab
Bernardo Portela
Nektaria Potha
Andreas Put
Sebastian Ramacher
Musa Samaila
Benjamin Semal
Mariusz Sepczuk
Bernardo Sequeiros
Mina Sheikhalishahi
João Marco Silva
Tiago Simões
Marjan Skrobot
Eva Söderström
Ptryk Szewczyk
Florian Thaeter
Ngoc Dung Tieu
Ganbayar Uuganbayar
Benito van der Zander
Weizheng Wang
S. J. Yang
Wenjie Yang
Xu Yang
Kai Zhu

Contents

Channel Attacks

Leaky Controller: Cross-VM Memory Controller Covert Channel on Multi-core Systems	3
<i>Benjamin Semal, Konstantinos Markantonakis, Raja Naeem Akram, and Jan Kalbantner</i>	
Evaluation of Statistical Tests for Detecting Storage-Based Covert Channels	17
<i>Thomas A. V. Sattolo and Jason Jaskolka</i>	
IE-Cache: Counteracting Eviction-Based Cache Side-Channel Attacks Through Indirect Eviction	32
<i>Muhammad Asim Mukhtar, Muhammad Khurram Bhatti, and Guy Gogniat</i>	

Connection Security

Refined Detection of SSH Brute-Force Attackers Using Machine Learning. . .	49
<i>Karel Hynek, Tomáš Beneš, Tomáš Čejka, and Hana Kubátová</i>	
MULTITLS: Secure Communication Channels with Cipher Suite Diversity . . .	64
<i>Ricardo Moura, David R. Matos, Miguel L. Pardal, and Miguel Correia</i>	
Improving Big Data Clustering for Jamming Detection in Smart Mobility . . .	78
<i>Hind Bangui, Mouzhi Ge, and Barbora Buhnova</i>	

Human Aspects of Security and Privacy

Assisting Users to Create Stronger Passwords Using ContextBased MicroTraining	95
<i>Joakim Kävrestad and Marcus Nohlberg</i>	
Facilitating Privacy Attitudes and Behaviors with Affective Visual Design . . .	109
<i>Agnieszka Kitkowska, Yefim Shulman, Leonardo A. Martucci, and Erik Wästlund</i>	
Privacy CURE: Consent Comprehension Made Easy	124
<i>Olha Drozd and Sabrina Kirrane</i>	

Detecting Malware and Software Weaknesses

JavaScript Malware Detection Using Locality Sensitive Hashing 143
Stefan Carl Peiser, Ludwig Friborg, and Riccardo Scandariato

RouAlign: Cross-Version Function Alignment and Routine Recovery
with Graphlet Edge Embedding 155
Can Yang, Jian Liu, Mengxia Luo, Xiaorui Gong, and Baoxu Liu

Code Between the Lines: Semantic Analysis of Android Applications 171
Johannes Feichtner and Stefan Gruber

System Security

IMShell-Dec: Pay More Attention to External Links in PowerShell 189
*RuiDong Han, Chao Yang, JianFeng Ma, Siqi Ma, YunBo Wang,
and Feng Li*

Secure Attestation of Virtualized Environments. 203
Michael Eckel, Andreas Fuchs, Jürgen Repp, and Markus Springer

Network Security and Privacy

Security and Performance Implications of BGP Rerouting-Resistant Guard
Selection Algorithms for Tor 219
*Asya Mitseva, Marharyta Aleksandrova, Thomas Engel,
and Andriy Panchenko*

Actively Probing Routes for Tor AS-Level Adversaries with RIPE Atlas 234
Wilfried Mayer, Georg Merzdovnik, and Edgar Weippl

Zeek-Osquery: Host-Network Correlation for Advanced Monitoring
and Intrusion Detection 248
Steffen Haas, Robin Sommer, and Mathias Fischer

Access Control and Authentication

Revisiting Security Vulnerabilities in Commercial Password Managers 265
Michael Carr and Siamak F. Shahandashti

Evaluation of Risk-Based Re-Authentication Methods 280
Stephan Wiefling, Tanvi Patil, Markus Dürmuth, and Luigi Lo Iacono

Fuzzy Vault for Behavioral Authentication System 295
Md Morshedul Islam and Reihaneh Safavi-Naini

Crypto Currencies

Improvements of the Balance Discovery Attack on Lightning Network Payment Channels	313
<i>Gijs van Dam, Rabiah Abdul Kadir, Puteri N. E. Nohuddin, and Halimah Badioze Zaman</i>	
CCBRNS: A System with High Embedding Capacity for Covert Communication in Bitcoin	324
<i>Weizheng Wang and Chunhua Su</i>	
Privacy-Friendly Monero Transaction Signing on a Hardware Wallet.	338
<i>Dusan Klinec and Vashek Matyas</i>	

Privacy and Security Management

A Matter of Life and Death: Analyzing the Security of Healthcare Networks	355
<i>Guillaume Dupont, Daniel Ricardo dos Santos, Elisa Costante, Jerry den Hartog, and Sandro Etalle</i>	
Establishing a Strong Baseline for Privacy Policy Classification	370
<i>Najmeh Mousavi Nejad, Pablo Jabat, Rostislav Nedelchev, Simon Scerri, and Damien Graux</i>	
Cross-Platform File System Activity Monitoring and Forensics – A Semantic Approach	384
<i>Kabul Kurniawan, Andreas Ekelhart, Fajar Ekaputra, and Elmar Kiesling</i>	

Machine Learning and Security

A Correlation-Preserving Fingerprinting Technique for Categorical Data in Relational Databases	401
<i>Tanja Sarcevic and Rudolf Mayer</i>	
PDFtNet: Facing Off Fake Images Using Fake Detection Fine-Tuning Network	416
<i>Hyeonseong Jeon, Youngoh Bang, and Simon S. Woo</i>	
Escaping Backdoor Attack Detection of Deep Learning	431
<i>Yayuan Xiong, Fengyuan Xu, Sheng Zhong, and Qun Li</i>	

Author Index	447
-------------------------------	-----