


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

Jacques Carette, Department of Computer Science, McMaster University, Hamilton, ON, Canada

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

Lukasz Stettner, Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland

TC 8 – Information Systems

Jan Pries-Heje, Roskilde University, Denmark


TC 9 – ICT and Society

David Kreps , National University of Ireland, Galway, Ireland

TC 10 – Computer Systems Technology

Achim Rettberg, Hamm-Lippstadt University of Applied Sciences, Hamm, Germany


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 Advances in Information and Communication Technology

The IFIP AICT series publishes state-of-the-art results in the sciences and technologies of information and communication. The scope of the series includes: foundations of computer science; software theory and practice; education; computer applications in technology; communication systems; systems modeling and optimization; information systems; ICT and society; computer systems technology; security and protection in information processing systems; artificial intelligence; and human-computer interaction.

Edited volumes and proceedings of refereed international conferences in computer science and interdisciplinary fields are featured. These results often precede journal publication and represent the most current research.

The principal aim of the IFIP AICT series is to encourage education and the dissemination and exchange of information about all aspects of computing.

More information about this series at <https://link.springer.com/bookseries/6102>


Norbert Meyer · Anna Grocholewska-Czuryło
Editors

ICT Systems Security and Privacy Protection

38th IFIP TC 11 International Conference, SEC 2023
Poznan, Poland, June 14–16, 2023
Revised Selected Papers

Editors

Norbert Meyer 
Poznan Supercomputing
and Networking Center
Poznań, Poland

Anna Grocholewska-Czuryło 
Poznań University of Technology
Poznań, Poland

ISSN 1868-4238 ISSN 1868-422X (electronic)
IFIP Advances in Information and Communication Technology
ISBN 978-3-031-56325-6 ISBN 978-3-031-56326-3 (eBook)
<https://doi.org/10.1007/978-3-031-56326-3>

© IFIP International Federation for Information Processing 2024

This work is subject to copyright. All rights are solely and exclusively licensed 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

Paper in this product is recyclable.

Preface

The 38th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2023) was held in Poznań on June 14–16, 2023. The conference focused on current and future IT Security and Privacy Challenges and was organized by the Poznan Supercomputing and Networking Center (PSNC) in Poznan, Poland. The conference was a part of a series of well-established international conferences on Security and Privacy. SEC is the flagship event of the International Federation for Information Processing (IFIP) Technical Committee 11 (TC-11).

From a total of 80 papers that were submitted from all over the world, 27 were selected for publication in the conference proceedings by the Program Committee (PC). The Program Chair was supported by a PC consisting of 80 leading experts in the field of IT security and privacy.

The selection of papers was made through a double-blind peer review process. Each submitted paper was assigned to at least 3 reviewers. Following the review phase, the discussions phase took place. The conflict-of-interest rules were imposed to ensure that papers are not handled by PC members with a close working relationship with the authors. Authors of the rejected papers received feedback on their work to help them improve future submissions.

This volume of the conference proceedings contains the revised versions of the 26 papers that were selected. The final revised versions of papers were not reviewed again, and the authors are responsible for their contents.

The IFIP SEC 2023 program featured two excellent invited talks. On the first day of the conference Josef Pieprzyk gave a talk on “Joint Compression and Encryption”. Then, on the second day, Sebastiano Batiati presented his research on “DeepFake Technology: Current Trends and Perspectives”.

Many people contributed to the success of IFIP SEC 2023 conference. First and foremost, we would like to thank the authors for submitting their innovative research results to the conference. We are very grateful to all the PC members for their hard work during the papers’ review process determining the program of the conference. We sincerely thank Norbert Meyer and Andrzej Jaszkiwicz, the general chairs of the conference, Paul Haskell-Dowland, IFIP TC11 Chair, and the members of the local Organizing Committee of the Poznan Supercomputing and Networking Center for handling all the organizational work of the conference. We also thank the Springer team for managing the publication of these conference proceedings. Last but not least, we thank the invited speakers, session chairs, and all participants for coming to Poznań and contributing to IFIP SEC 2023.

December 2023

Norbert Meyer
Anna Grochowska-Czuryło

Organization

General Chairs

Norbert Meyer	Poznan Supercomputing and Networking Center Institute of Bioorganic Chemistry PAS, Poland
Andrzej Jaszekiewicz	Poznan University of Technology, Poland

Program Committee Chairs

Norbert Meyer	Poznan Supercomputing and Networking Center Institute of Bioorganic Chemistry PAS, Poland
Anna Grocholewska-Czuryło	Poznan University of Technology, Poland

IFIP TC-11 Chair

Paul Haskell-Dowland	Edith Cowan University, Australia
----------------------	-----------------------------------

Local Organizing + Web Chair

Donata Sikorska	Poznan Supercomputing and Networking Center Institute of Bioorganic Chemistry PAS, Poland
-----------------	--

Program Committee

Rose-Mharie Åhlfeldt	University of Skövde, Sweden
Magnus Almgren	Chalmers University of Technology, Sweden
Claudio Ardagna	Università degli Studi di Milano, Italy
Joao Paulo Barraca	University of Aveiro, Portugal
Marcus Belder	Defence Science and Technology Group, Australia
Tamas Bisztray	University of Oslo, Norway
Ravishankar Borgaonkar	SINTEF, Norway
Michał Choraś	ITTI, Poland
K. P. Chow	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	University di Salerno, Italy
Bernardo David	IT University of Copenhagen, Denmark
Ed Dawson	Queensland University of Technology, Australia
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy

Yvo Desmedt	University of Texas at Dallas, USA
Nicola Dragoni	Technical University of Denmark, Denmark
Givemore Dube	CSZ, Zimbabwe
Isao Echizen	National Institute of Informatics, Japan
Simone Fischer-Hübner	Karlstad University, Sweden
Gerard Frankowski	Poznan Supercomputing and Networking Center, Poland
Steven Furnell	University of Nottingham, UK
Mariusz Głabowski	Poznan University of Technology, Poland
Hélder Gomes	Universidade de Aveiro, Portugal
Nils Gruschka	University of Oslo, Norway
Rene Rydhof Hansen	Aalborg University, Denmark
Paul Haskell-Dowland	Edith Cowan University, Australia
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
Jan Jürjens	University of Koblenz-Landau, Germany
Georgios Kambourakis	University of the Aegean, Greece
Farzaneh Karegar	Karlstad University, Sweden
Stefan Katzenbeisser	University of Passau, Germany
Dogan Kesdogan	Universität Regensburg, Germany
Zbigniew Kotulski	Warsaw University of Technology, Poland
Stephan Krenn	AIT Austrian Institute of Technology, Austria
Łukasz Krzywiecki	Wroclaw University of Technology, Poland
Peeter Laud	Cybernetica AS, Estonia
Wenjuan Li	Hong Kong Polytechnic University, China
Maciej Liskiewicz	University of Luebeck, Germany
Luigi Logrippo	Université du Québec en Outaouais, Canada
Javier Lopez	University of Malaga, Spain
Suryadipta Majumdar	Concordia University, Canada
Salman Manzoor	TU Darmstadt, Germany
Marian Margraf	Hochschule Darmstadt, Germany
Vashek Matyas	Masaryk University, Czechia
Weizhi Meng	Technical University of Denmark, Denmark
Zlatogor Minchev	Bulgarian Academy of Sciences, Bulgaria
Yuko Murayama	Tsuda College, Japan
Maurizio Naldi	LUMSA University, Italy
Lili Nemes Zlatolas	University of Maribor, Slovenia
Brajendra Panda	University of Arkansas, USA
Miguel Pardal	Universidade de Lisboa, Portugal
António Pinto	Politécnico do Porto, Portugal
Kai Rannenber	Goethe University Frankfurt, Germany
Carlos Rieder	ISEC AG, Switzerland
Juha Röning	University of Oulu, Norway

Reihaneh Safavi-Naini	University of Calgary, Canada
Christophe Rosenberger	Normandy University, France
Pierangela Samarati	Università degli Studi di Milano, Italy
Jürgen Schönwälder	Jacobs University Bremen, Germany
Jun Shao	Zhejiang Gongshang University, China
Nicolas Sklavos	University of Patras, Greece
Daniel Slamanig	AIT Austrian Institute of Technology, Austria
Agusti Solanas	Rovira i Virgili University, Spain
Shamik Sural	IIT, Kharagpur, India
Neeraj Suri	Lancaster University, UK
Vicenc Torra	University of Skovde, Sweden
Lingyu Wang	Concordia University, Canada
Edgar Weippl	University of Vienna, Austria
Roman Wyrzykowski	Czestochowa University of Technology, Poland
Øyvind Ytrehus	University of Bergen, Norway
André Zúquete	University of Aveiro, Portugal

Contents

Web Content Integrity: Tamper-Proof Websites Beyond HTTPS	1
<i>Sven Zemanek, Sebastian Tauchert, Max Jens Ufer, and Lilli Bruckschen</i>	
Privacy-Preserving Clustering for Multi-dimensional Data Randomization Under LDP	15
<i>Hiroaki Kikuchi</i>	
Hierarchical Model-Based Cybersecurity Risk Assessment During System Design	30
<i>Tino Jungebloud, Nhung H. Nguyen, Dong Seong Kim, and Armin Zimmermann</i>	
The Influence of Privacy Concerns on Cryptocurrency Acceptance	45
<i>Peter Hamm, Sebastian Pape, and Kai Rannenber</i>	
Automated Enrichment of Logical Attack Graphs via Formal Ontologies	59
<i>Kéren Saint-Hilaire, Frédéric Cuppens, Nora Cuppens, and Joaquin Garcia-Alfaro</i>	
Detecting Web Bots via Mouse Dynamics and Communication Metadata.	73
<i>August See, Tatjana Wingarz, Matz Radloff, and Mathias Fischer</i>	
Practical Single-Round Secure Wildcard Pattern Matching	87
<i>Jun Xu, Shengnan Zhao, Chuan Zhao, Zhenxiang Chen, Zhe Liu, and Liming Fang</i>	
Efficient Non-interactive Anonymous Communication	102
<i>Sigurd Eskeland and Svetlana Boudko</i>	
PointPuff: An Ed25519 Optimization Implementation	117
<i>Mengqing Yang, Chunxiao Ye, Yuanmu Liu, Yan Jin, and Chunming Ye</i>	
Detecting Web Tracking at the Network Layer	131
<i>Maximilian Wittig and Doğan Kesdoğan</i>	
What’s Inside a Node? Malicious IPFS Nodes Under the Magnifying Glass . . .	149
<i>Christos Karapapas, George C. Polyzos, and Constantinos Patsakis</i>	

Quantum-Secure Communication for Trusted Edge Computing with IoT Devices 163
George Kornaros, Georgia Berki, and Miltos Grammatikakis

Evaluation of a Red Team Automation Tool in Live Cyber Defence Exercises 177
Hannes Holm and Jenni Reuben

Automated and Improved Detection of Cyber Attacks via an Industrial IDS Probe. 191
Almamy Touré, Youcef Imine, Thierry Delot, Antoine Gallais, Alexis Semmont, and Robin Giraud

An Accurate and Real-Time Detection Method for Concealed Slow HTTP DoS in Backbone Network. 207
Jinfeng Chen, Hua Wu, Suyue Wang, Guang Cheng, and Xiaoyan Hu

Towards an Information Privacy Competency Model for the Usage of Mobile Applications 222
Aikaterini Soumelidou and Aggeliki Tsohou

SecPassInput: Towards Secure Memory and Password Handling in Web Applications 236
Pascal Wichmann, August See, and Hannes Federrath

Bl0ck: Paralyzing 802.11 Connections Through Block Ack Frames. 250
Efstratios Chatzoglou, Vyron Kampourakis, and Georgios Kambourakis

Enhancing the ACME Protocol to Automate the Management of All X.509 Web Certificates 265
David A. Cordova Morales, Ahmad Samer Wazan, David W. Chadwick, Romain Laborde, April Rains Reyes Maramara, and Kalil Cabral

MADONNA: Browser-Based MALicious Domain Detection Through Optimized Neural Network with Feature Analysis 279
Janaka Senanayake, Sampath Rajapaksha, Naoto Yanai, Chika Komiya, and Harsha Kalutarage

Cyber Key Terrain Identification Using Adjusted PageRank Centrality 293
Lukáš Sadlek and Pavel Čeleda

Machine Learning Metrics for Network Datasets Evaluation 307
Dominik Soukup, Daniel Uhříček, Daniel Vašata, and Tomáš Čejka

Factors of Intention to Use a Photo Tool: Comparison Between
 Privacy-Enhancing and Non-privacy-enhancing Tools 321
Vanessa Bracamonte, Sebastian Pape, and Sascha Löbner

Real-Time Platform Identification of VPN Video Streaming Based on
 Side-Channel Attack 335
Anting Lu, Hua Wu, Hao Luo, Guang Cheng, and Xiaoyan Hu

Toward the Establishment of Evaluating URL Embedding Methods Using
 Intrinsic Evaluator via Malicious URLs Detection 350
Qisheng Chen and Kazumasa Omote

Key Management Based on Ownership of Multiple Authenticators
 in Public Key Authentication 361
Kodai Hatakeyama, Daisuke Kotani, and Yasuo Okabe

Author Index 377