

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Moti Yung 

Columbia University, New York, NY, USA


More information about this series at <https://link.springer.com/bookseries/558>

Vijayalakshmi Atluri · Roberto Di Pietro ·
Christian D. Jensen · Weizhi Meng (Eds.)


Computer Security – ESORICS 2022

27th European Symposium
on Research in Computer Security
Copenhagen, Denmark, September 26–30, 2022
Proceedings, Part III

Editors

Vijayalakshmi Atluri 
Rutgers University
Newark, NJ, USA

Roberto Di Pietro 
Hamad Bin Khalifa University
Doha, Qatar

Christian D. Jensen 
Technical University of Denmark
Kongens Lyngby, Denmark

Weizhi Meng 
Technical University of Denmark
Kongens Lyngby, Denmark

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-17142-0

ISBN 978-3-031-17143-7 (eBook)

<https://doi.org/10.1007/978-3-031-17143-7>

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2022

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

The 27th European Symposium on Research in Computer Security (ESORICS 2022) was held together with the affiliated workshops during the week of September 26–30, 2022. Due to the COVID-19 pandemic, the conference and the workshops took place in a hybrid mode. The virtual and in-person attendance was hosted and managed by the Technical University of Denmark.

ESORICS is a flagship European security conference. The aim of ESORICS is to advance the research in computer security and privacy by establishing a European forum, bringing together researchers in these areas, and promoting the exchange of ideas with developers, standardization bodies, and policy makers, as well as by encouraging links with researchers in related fields.

Continuing the model introduced in 2021, this year ESORICS also offered two review cycles: a winter cycle and a spring cycle. We believe that such an approach sports great advantages. On the one hand, it is more convenient for the authors and, on the other hand, it also increases the number of submissions, thus securing high-quality papers. In response to the call for papers, which covered a few new topics, we received a record-high number of papers: 562. This is a testimony of the growth and vitality of the computer security field, the expansion of the research community in this field, and the growing importance of ESORICS itself.

These papers were peer-reviewed and subsequently discussed based on the quality of their scientific contribution, novelty, and impact by the members of the Program Committee. The submissions were single-blind, and in almost all cases there were vivid discussions among the members of the Program Committee to decide the merit of reviewed papers.

The submission of the papers and the review process was carried out using the Easy-Chair platform. Based on the reviews and the discussion, 104 papers were selected for presentation at the conference, resulting in an acceptance rate of 18.5%. The most tangible result of this whole process was that ESORICS had an exciting scientific program covering timely and interesting security and privacy topics in theory, systems, networks, and applications.

The papers that were selected for presentation at ESORICS 2022 have been published in a three-volume set of proceedings: LNCS 13554, LNCS 13555, and LNCS 13556.

Aside from the paper presentations, we were honored to have four outstanding keynote speakers: Giuseppe Ateniese, Paulo Esteves-Verissimo, Ahmad Reza Sadeghi, and Ravi Sandhu. Their talks provided interesting insights and research directions in important research areas.

The Program Committee (PC) consisted of 180 members. We would like to thank the members of the PC and the external referees for their hard work in supporting the review process, as well as everyone who supported the organization of ESORICS 2022. In particular, the exceptional number of submissions put quite a burden on the reviewers (over the two cycles of submission, an average of 12 papers were reviewed by each reviewer).

We are grateful to the general co-chairs, Christian D. Jensen and Weizhi Meng; the workshops chairs, Mauro Conti and Jianying Zhou, and all of the workshop co-chairs; the poster chair, Joaquin Garcia-Alfaro; the publicity co-chair's Cristina Alcaraz and Wenjuan Li; the web chair, Wei-Yang Chiu; and the ESORICS Steering Committee and its chair, Sokratis Katsikas.

We are also grateful to BlockSec for supporting the organization of ESORICS 2022.

Finally, we would like to provide a heartfelt thank you to the authors for submitting their papers to ESORICS 2022. It is their efforts that, in the end, decided the success of ESORICS 2022, confirmed ESORICS as a top-notch security conference, planted the seeds for future successes, and advanced science.

We hope that the proceedings will promote research and facilitate future work in the exciting, challenging, and evolving field of security.

September 2022

Roberto Di Pietro
Vijayalakshmi Atluri

Organization

General Chairs

Christian D. Jensen
Weizhi Meng

Technical University of Denmark, Denmark
Technical University of Denmark, Denmark

Program Committee Chairs

Vijayalakshmi Atluri
Roberto Di Pietro

Rutgers University, USA
Hamad Bin Khalifa University, Qatar

Steering Committee

Sokratis Katsikas (Chair)
Joachim Biskup
Véronique Cortier
Frédéric Cuppens
Sabrina De Capitani di Vimercati
Joaquin Garcia-Alfaro
Dieter Gollmann
Kutyłowski Mirek
Javier Lopez
Jean-Jacques Quisquater
Peter Ryan
Pierangela Samarati
Einar Snekkenes
Michael Waidner

NTNU, Norway
University of Dortmund, Germany
CNRS, France
Polytechnique Montréal, Canada
Università degli Studi di Milano, Italy
Institut Polytechnique de Paris, France
Hamburg University of Technology, Germany
Wrocław University of Technology, Poland
Universidad de Malaga, Spain
University of Louvain, Belgium
University of Luxembourg, Luxembourg
Università degli Studi di Milano, Italy
NTNU, Norway
ATHENE, Germany

Program Committee

Abu-Salma, Ruba
Afek, Yehuda
Akiyama, Mitsuaki
Albanese, Massimiliano
Alcaraz, Cristina
Allman, Mark
Alrabaee, Saed
Asif, Hafiz

King's College London, UK
Tel-Aviv University, Israel
NTT, Japan
George Mason University, USA
University of Malaga, Spain
International Computer Science Institute, USA
United Arab Emirates University, UAE
Rutgers University, USA

Ayday, Erman	Case Western Reserve University, USA, and Bilkent University, Turkey
Bai, Guangdong	University of Queensland, Australia
Bakiras, Spiridon	Singapore Institute of Technology, Singapore
Bardin, Sebastien	CEA LIST, France
Batra, Gunjan	Kennesaw State University, USA
Bertino, Elisa	Purdue University, USA
Blasco, Jorge	Royal Holloway, University of London, UK
Blundo, Carlo	Università degli Studi di Salerno, Italy
Bonaci, Tamara	Northeastern University, USA
Camtepe, Seyit	CSIRO Data61, Australia
Ceccato, Mariano	Università di Verona, Italy
Chakraborti, Anrín	Stony Brook University, USA
Chan, Aldar C-F.	University of Hong Kong, Hong Kong
Chen, Bo	Michigan Technological University, USA
Chen, Xiaofeng	Xidian University, China
Chen, Liquan	University of Surrey, UK
Chen, Rongmao	National University of Defense Technology, China
Chen, Yu	Shandong University, China
Chow, Sherman S. M.	The Chinese University of Hong Kong, Hong Kong
Chowdhury, Omar	University of Iowa, USA
Conti, Mauro	Università di Padova, USA
Coull, Scott	Mandiant, USA
Crispo, Bruno	University of Trento, Italy
Cukier, Michel	University of Maryland, USA
Cuppens, Frédéric	Polytechnique Montréal, Canada
Cuppens-Boulahia, Nora	Polytechnique Montréal, Canada
Damiani, Ernesto	University of Milan, Italy
Daza, Vanesa	Universitat Pompeu Fabra, Spain
De Capitani di Vimercati, Sabrina	Università degli Studi di Milano, Italy
Debar, Hervé	Télécom SudParis, France
Desmedt, Yvo	University of Texas at Dallas, USA
Diao, Wenrui	Shandong University, China
Dimitriou, Tassos	Kuwait University, Kuwait
Domingo-Ferrer, Josep	Universitat Rovira i Virgili, Spain
Dong, Changyu	Newcastle University, UK
Ferrara, Anna Lisa	University of Bristol, UK
Ferrer-Gomila, Jose-Luis	University of the Balearic Islands, Spain
Fila, Barbara	INSA Rennes, IRISA, France
Fischer-Hübner, Simone	Karlstad University, Sweden

Gadyatskaya, Olga
 Gao, Debin
 Garcia-Alfaro, Joaquin
 Garg, Siddharth
 Giacinto, Giorgio
 Gollmann, Dieter
 Gong, Neil
 Gope, Prosanta
 Gosain, Devashish
 Gritzalis, Stefanos
 Gu, Zhongshu
 Gulmezoglu, Berk
 Haines, Thomas
 He, Xinlei

 Hernández-Serrano, Juan
 Hong, Yuan
 Huang, Xinyi
 Jager, Tibor
 Jeon, Yuseok

 Ji, Shouling
 Jonker, Hugo

 Karame, Ghassan
 Katsikas, Sokratis
 Kim, Hyoungshick
 Klai, Kais
 Kremer, Steve
 Krotofil, Marina
 Kruegel, Christopher
 Lambrinoudakis, Costas
 Landau Feibish, Shir
 Lee, Adam
 Leita, Corrado
 Li, Shujun
 Li, Zitao
 Liang, Kaitai
 Lin, Zhiqiang
 Liu, Xiangyu
 Liu, Peng
 Livraga, Giovanni

Leiden University, The Netherlands
 Singapore Management University, Singapore
 Institut Polytechnique de Paris, France
 New York University, USA
 University of Cagliari, Italy
 Hamburg University of Technology, Germany
 Duke University, USA
 University of Sheffield, UK
 Max Planck Institute for Informatics, Germany
 University of Piraeus, Greece
 IBM, USA
 Iowa State University, USA
 Queensland University of Technology, Australia
 CISP Helmholtz Center for Information
 Security, Germany
 Universitat Politècnica de Catalunya, Spain
 Illinois Institute of Technology, USA
 Fujian Normal University, China
 Bergische Universität Wuppertal, Germany
 Ulsan National Institute of Science and
 Technology, South Korea
 Zhejiang University, China
 Open University of the Netherlands,
 The Netherlands
 NEC Laboratories Europe, Germany
 NTNU, Norway
 Sungkyunkwan University, South Korea
 Sorbonne University, France
 Inria, France
 Kudelski Security, Switzerland
 University of California, Santa Barbara, USA
 University of Piraeus, Greece
 The Open University of Israel, Israel
 University of Pittsburg, USA
 VMware, UK
 University of Kent, UK
 Purdue University, USA
 TU Delft, The Netherlands
 Ohio State University, USA
 Alibaba Inc., China
 Pennsylvania State University, USA
 University of Milan, Italy

Lombardi, Flavio	National Research Council, Italy
Lou, Wenjing	Virginia Tech, USA
Lu, Rongxing	University of New Brunswick, Canada
Lu, Haibing	Santa Clara University, USA
Luo, Xiapu	The Hong Kong Polytechnic University, Hong Kong
Ma, Shiqing	Rutgers University, USA
Marin-Fabregas, Eduard	Telefonica Research, Spain
Martinelli, Fabio	National Research Council, Italy
Mauw, Sjouke	University of Luxembourg, Luxembourg
Meng, Weizhi	Technical University of Denmark, Denmark
Mohan, Sibin	Oregon State University, USA
Mori, Tatsuya	Waseda University, Japan
Mueller, Johannes	University of Luxembourg, Luxembourg
Ng, Siaw-Lynn	Royal Holloway, University of London, and Bedford New College, UK
Ning, Jianting	Singapore Management University, Singapore
Obana, Satoshi	Hosei University, Japan
Oligieri, Gabriele	Hamad Bin Khalifa University, Qatar
Overdorf, Rebekah	Ecole Polytechnique Fédérale de Lausanne, Switzerland
Pal, Shantanu	Queensland University of Technology, Australia
Pan, Jiaxin	NTNU, Norway
Papadimitratos, Panos	KTH Royal Institute of Technology, Sweden
Paraboschi, Stefano	Università di Bergamo, Italy
Patranabis, Sikhar	IBM Research India, India
Pernul, Günther	Universität Regensburg, Germany
Poovendran, Radha	University of Washington, USA
Posegga, Joachim	University of Passau, Germany
Quiring, Erwin	Technische Universität Braunschweig, Germany
Quisquater, Jean-Jacques	University of Louvain, Belgium
Rao, Siddharth Prakash	Aalto University, Finland
Rashid, Awais	University of Bristol, UK
Ren, Kui State	University of New York at Buffalo, USA
Rhee, Junghwan	University of Central Oklahoma, USA
Ricci, Laura	University of Pisa, Italy
Russello, Giovanni	University of Auckland, New Zealand
Ryan, Peter	University of Luxembourg, Luxembourg
Safavi-Naini, Reihaneh	University of Calgary, Canada
Saileshwar, Gururaj	Georgia Institute of Technology, USA
Sakzad, Amin	Monash University, Australia
Samarati, Pierangela	Università degli Studi di Milano, Italy

Schinzel, Sebastian	Münster	Münster University of Applied Sciences, Germany
Schneider, Steve		University of Surrey, UK
Schroeder, Dominique		Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
Schwarz, Michael		CISPA Helmholtz Center for Information Security, Germany
Schwenk, Joerg		Ruhr-Universität Bochum, Germany
Sciancalepore, Savio		Eindhoven University of Technology, The Netherlands
Shahandashti, Siamak		University of York, UK
Sharma, Piyush Kumar		Indraprastha Institute of Information Technology Delhi, India
Shulman, Haya		Fraunhofer SIT, Germany
Sinanoglu, Ozgur		New York University Abu Dhabi, UAE
Sklavos, Nicolas		University of Patras, Greece
Snekkenes, Einar		NTNU, Norway
Somorovsky, Juraj		Paderborn University, Germany
Strufe, Thorsten		Karlsruhe Institute of Technology, Germany
Sural, Shamik		IIT Kharagpur, India
Susilo, Willy		University of Wollongong, Australia
Tang, Qiang		University of Sydney, Australia
Tang, Qiang		Luxembourg Institute of Science and Technology, Luxembourg
Tapiador, Juan Manuel		Universidad Carlos III de Madrid, Spain
Tian, Dave		Purdue University, USA
Torrey, Jacob		Thinkst Applied Research, USA
Trachtenberg, Ari		Boston University, USA
Treharne, Helen		University of Surrey, UK
Trieu, Ni		Arizona State University, USA
Tripunitara, Mahesh		University of Waterloo, Canada
Tsohou, Aggeliki		Ionian University, Greece
Urban, Tobias		Institute for Internet Security, Germany
Esteves-Verissimo, Paulo		KAUST, Saudi Arabia
Vigano, Luca		King's College London, UK
Visconti, Ivan		University of Salerno, Italy
Voulimeneas, Alexios		KU Leven, Belgium
Waidner, Michael		ATHENE, Germany
Wang, Cong		City University of Hong Kong, Hong Kong
Wang, Tianhao		Purdue University, USA
Wang, Di		State University of New York at Buffalo, USA
Wang, Haining		University of Delaware, USA

Wang, Lingyu	Concordia University, Canada
Wool, Avishai	Tel Aviv University, Israel
Xenakis, Christos	University of Piraeus, Greece
Xiang, Yang	Swinburne University of Technology, Australia
Xu, Jun	University of Utah, USA
Yang, Jie	Florida State University, USA
Yang, Kang	State Key Laboratory of Cryptology, China
Yang, Guomin	University of Wollongong, Australia
Yeun, Chan	Khalifa University, Abu Dhabi, UAE
Yi, Xun	RMIT University, Australia
Yu, Yu	Shanghai Jiao Tong University, China
Yuen, Tsz	University of Hong Kong, Hong Kong
Zhang, Zhikun	CISPA Helmholtz Center for Information Security, Germany
Zhang, Yuan	Fudan University, China
Zhang, Kehuan	The Chinese University of Hong Kong, Hong Kong
Zhao, Yunlei	Fudan University, China
Zhou, Jianying	Singapore University of Technology and Design, Singapore
Zhu, Rui	Indiana University, USA
Zhu, Sencun	Pennsylvania State University, USA

Workshops Chairs

Conti Mauro	University of Padua, Italy
Zhou Jianying	Singapore University of Technology and Design, Singapore

Poster Chair

Garcia-Alfaro Joaquin	Institut Polytechnique de Paris, France
-----------------------	---

Publicity Chairs

Alcaraz Cristina	University of Malaga, Spain
Li Wenjuan	Hong Kong Polytechnic University, Hong Kong

Web Chair

Chiu Wei-Yang	Technical University of Denmark, Denmark
---------------	--

Posters Program Committee

Atluri, Vijay	Rutgers University, USA
de Fuentes, Jose M.	Universidad Carlos III de Madrid, Spain
Di Pietro, Roberto	Hamad Bin Khalifa University, Qatar
González Manzano, Lorena	Universidad Carlos III de Madrid, Spain
Hartenstein, Hannes	Karlsruhe Institute of Technology, Germany
Kikuchi, Hiroaki	Meiji University, Japan
Matsuo, Shin'Ichiro	Georgetown University, USA
Navarro-Arribas, Guillermo	Universitat Autònoma de Barcelona, Spain
Nespoli, Pantaleone	Universidad de Murcia, Spain
Ranise, Silvio	University of Trento and Fondazione Bruno Kessler, Italy
Saint-Hilarire, Kéren	Institut Polytechnique de Paris, France
Signorini, Matteo	Nokia Bell Labs, France
Vasilopoulos, Dimitrios	IMDEA Software Institute, Spain
Zannone, Nicola	Eindhoven University of Technology, The Netherlands

Additional Reviewers

Abadi, Aydin	Berger, Christian
Abbadini, Marco	Berrang, Pascal
Ahmadi, Sharar	Blanco-Justicia, Alberto
Akand, Mamun	Böhm, Fabian
Akbar, Yousef	Bolgouras, Vaïos
Alrahis, Lilas	Botta, Vincenzo
Ameur Abid, Chiheb	Bountakas, Panagiotis
Amine Merzouk, Mohamed	Brighente, Alessandro
Anagnostopoulos, Marios	Bursuc, Sergiu
Angelogianni, Anna	C. Pöhls, Henrich
Anglés-Tafalla, Carles	Cachin, Christian
Apruzzese, Giovanni	Cai, Cailing
Arapinis, Myrto	Cao, Chen
Arriaga, Afonso	Casolare, Rosangela
Arzt, Steven	Chen, Xihui
Avitabile, Gennaro	Chen, Niusen
Avizheh, Sepideh	Chen, Min
Bag, Arnab	Chen, Jinrong
Bagheri, Sima	Chen, Chao
Bampatsikos, Michail	Chen, Long
Battarbee, Christopher	Chen, Zeyu
Baumer, Thomas	Chu, Hien
Benaloh, Josh	Ciampi, Michele

Cicala, Fabrizio
 Cinà, Antonio
 Coijanovic, Christoph
 Costantino, Gianpiero
 Craaijo, Jos
 Crochelet, Pierre
 Cui, Hui
 Cui, Handong
 Dai, Tianxiang
 Damodaran, Aditya
 Daniyal Dar, Muhammad
 Das Chowdhury, Partha
 Daudén-Esmel, Cristòfol
 Davies, Peter
 Davies, Gareth
 de Ruck, Dairo
 Debant, Alexandre
 Debnath, Joyanta
 Degani, Luca
 Demetrio, Luca
 Deuber, Dominic
 Dexheimer, Thomas
 Diemert, Denis
 Dodd, Charles
 Dragan, Constantin Catalin
 Driouich, Youssef
 Du, Changlai
 Du, Linkang
 Du, Minxin
 Duman, Onur
 Duong, Dung
 Dutta, Priyanka
 Dutta, Sabyasachi
 Dutta, Moumita
 Duttagupta, Sayon
 Ebrahimi, Ehsan
 Echeverria, Mitziu
 Ehsanpour, Maryam
 Eichhammer, Philipp
 Ekramul Kabir, Mohammad
 Empl, Philip
 Eyal, Ittay
 Facchinetti, Dario
 Fadavi, Mojtaba
 Fallahi, Matin

Farao, Aristeidis
 Fauzi, Prastudy
 Feng, Hanwen
 Feng, Qi
 Feng, Shuya
 Fisseha Demissie, Biniam
 Fournaris, Apostolos
 Fraser, Ashley
 Friedl, Sabrina
 Friess, Jens
 Friolo, Daniele
 Gao, Jiahui
 Gardiner, Joseph
 Garfatta, Ikram
 Gattermayer, Tobias
 Gellert, Kai
 George, Dominik
 Gerault, David
 Gerhart, Paul
 Ghadafi, Essam
 Gholipourchoubek, Mahmood
 Gil-Pons, Reynaldo
 Glas, Magdalena
 Golinelli, Matteo
 Gong, Junqing
 Grisafi, Michele
 Groll, Sebastian
 Große-Kampmann, Matteo
 Guan Tan, Teik
 Guo, Xiaojie
 Haffar, Rami
 Haffey, Preston
 Hallett, Joseph
 Hammad Mazhar, M.
 Han, Jinguang
 Handirk, Tobias
 Hao, Xuexuan
 Hao, Shuai
 Hasan Shahriar, Md
 Heftrig, Elias
 Heitjohann, Raphael
 Henry Castellanos, John
 Herranz, Javier
 Hirschi, Lucca
 Hlavacek, Tomas

Hobbs, Nathaniel
 Hong, Hanbin
 Horne, Ross
 Horváth, Máté
 Hu, Zhenkai
 Hu, Lijie
 Hu, Yan
 Huang, Jianwei
 Huso, Ingrid
 Iadarola, Giacomo
 Ioannidis, Thodoris
 Iovino, Vincenzo
 Ising, Fabian
 Jacobs, Adriaan
 Jebreel, Najeeb
 Jeitner, Philipp
 Jensen, Meiko
 Jesús A., Zihang
 Jin, Lin
 Kailun, Yan
 Kaiser, Fabian
 Kaplan, Alexander
 Karim, Imtiaz
 Karyda, Maria
 Katsis, Charalampos
 Kavousi, Alireza
 Kelarev, Andrei
 Kempinski, Stash
 Kermabon-Bobinnec, Hugo
 Kern, Sascha
 Khalili, Mojtaba
 Khandpur Singh, Ashneet
 Khin Shar, Lwin
 Knechtel, Johann
 Kokolakis, Spyros
 Krumnow, Benjamin
 Ksontini, Rym
 Kulkarni, Tejas
 Lai, Jianchang
 Lee, Hyunwoo
 Léger, Marc-André
 Li, Jinfeng
 Li, Rui
 Li, Shaoyu
 Li, Yanan

Li, Shuang
 Li, Guangpu
 Liang, Yuan
 Likhitha Mankali, Lakshmi
 Limbasiya, Trupil
 Lin, Chao
 Lin Aung, Yan
 Liu, Lin
 Liu, Xiaoning
 Liu, Bingyu
 Liu, Guannan
 Liu, Xiaoyin
 Liu, Jiahao
 Liu, Zhen
 Liu, Xueqiao
 Liu, Xiaoyuan
 Lu, Yun
 Lucchese, Marco
 Luo, Junwei
 Lv, Chunyang
 Lyu, Lin
 Lyvas, Christos
 Ma, Wanlun
 Ma, Mimi
 Maiorca, Davide
 Maitra, Sudip
 Makriyannis, Nikolaos
 Manjón, Jesús A.
 Martinez, Sergio
 Mccarthy, Sarah
 Mei, Qian
 Menegatos, Andreas
 Meng, Long
 Mercaldo, Francesco
 Merget, Robert
 Mestel, David
 Meyuhas, Bar
 Michalas, Antonis
 Mirdita, Donika
 Mizera, Andrzej
 Mohammadi, Farnaz
 Mohammed, Ameer
 Morillo, Paz
 Morrison, Adam
 Mujeeb Ahmed, Chuadhry

Nabi, Mahmudun	Schlette, Daniel
Neal, Christopher	Schmidt, Carsten
Nguyen, Son	Sentanoe, Stewart
Niehues, David	Sha, Zeyang
Nixon, Brian	Shao, Jun
Oldani, Gianluca	Shi, Shanghao
Oqaily, Momen	Shibahara, Toshiki
Oqaily, Alaa	Shioji, Eitaro
Oслиak, Oleksii	Shojafar, Mohammad
P. K. Ma, Jack	Shreeve, Benjamin
Pan, Shimin	Silde, Tjerand
Pan, Jianli	Singh, Animesh
Pang, Chengbin	Singh Sehrawat, Vipin
Pang, Bo	Sinha, Sayani
Panja, Somnath	Siniscalchi, Luisa
Paolo Tricomi, Pier	Skrobot, Marjan
Paspatis, Ioannis	Sohrabi, Nasrin
Peng, Hui	Sollomoni, Avi
Pitropakis, Nikolaos	Song, Shang
Polato, Mirko	Sotgiu, Angelo
Pryvalov, Ivan	Soud, Nourelhouda
Pu, Sihang	Soumelidou, Katerina
Puchta, Alexander	Sun, Shihua
Putz, Benedikt	Tabatabaei, Masoud
Qian, Chen	Tabiban, Azadeh
Qin, Baodong	Taha Bennani, Mohamed
Qin, Xianrui	Talibi Alaoui, Younes
Rabhi, Mouna	Tang, Lihong
Radomirovic, Sasa	Tao, Youming
Ramokapane, Kopo M.	Tedeschi, Pietro
Rangarajan, Nikhil	Terrovitis, Manolis
Ravi, Divya	Tian, Guohua
Rawat, Abhimanyu	Tian, Yangguang
Raza, Ali	Turrin, Federico
Román-García, Fernando	Umayya, Zeya
Rossi, Matthew	Vinayagamurthy, Dhinakaran
Rovira, Sergi	Visintin, Alessandro
S. M. Asadujjaman, A.	Vollmer, Marcel
Saatjohann, Christoph	von der Heyden, Jonas
Sadighian, Alireza	Voudouris, Anastassios
Saha, Rahul	W. H. Wong, Harry
Samanis, Emmanouil	Wagner, Benedikt
Sarathi Roy, Partha	Wang, Han
Sarkar, Pratik	Wang, Ning
Schiff Agron, Shir	Wang, Kailong

Wang, Xiuhua	Yang, Xu
Wang, Yalan	Yang, S. J.
Wang, Shu	Yang, Xuechao
Wang, Jiafan	Yang, Junwen
Wang, Haizhou	Yin Chan, Kwan
Wang, Zhilong	You, Weijing
Wang, Xiaolei	Yu, Hexuan
Wang, Yunling	Yurkov, Semen
Wang, Qin	Zeng, Runzhi
Wang, Yu	Zhang, Sepideh
Wang, Cheng-Long	Zhang, Min
Wang, Weijia	Zhang, Yanjun
Wang, Xinyue	Zhang, Zicheng
Wang, Yi	Zhang, Cong
Wang, Yuyu	Zhang, Lan
Wang, Yangde	Zhang, Xinyu
Watanabe, Takuya	Zhang, Kai
Wu, Huangting	Zhang, Tao
Wu, Yulian	Zhang, Yunhang
Wu, Chen	Zhang, Xiaoyu
Wu, Mingli	Zhang, Zidong
Wu, Qiushi	Zhang, Rongjunchen
Xiang, Zihang	Zhao, Yongjun
Xiao, Yang	Zhao, Shujie
Xiao, Jidong	Zhao, Lingchen
Xie, Shangyu	Zheng, Xiang
Xu, Shengmin	Zhou, Xiaotong
Yadav, Tarun	Zhu, Fei
Yan, Di	Zikas, Vassilis
Yang, Zhichao	Zou, Qingtian
Yang, Shishuai	

Contents – Part III

Formal Analysis

A Formal Analysis of the FIDO2 Protocols	3
<i>Jingjing Guan, Hui Li, Haisong Ye, and Ziming Zhao</i>	
A Composable Security Treatment of ECVRF and Batch Verifications	22
<i>Christian Badertscher, Peter Gazi, Iñigo Querejeta-Azurmendi, and Alexander Russell</i>	
Efficient Proofs of Knowledge for Threshold Relations	42
<i>Gennaro Avitabile, Vincenzo Botta, Daniele Friolo, and Ivan Visconti</i>	
A Tale of Two Models: Formal Verification of KEMTLS via Tamarin	63
<i>Sofia Celi, Jonathan Hoyland, Douglas Stebila, and Thom Wiggers</i>	

Web Security

Browser-Based CPU Fingerprinting	87
<i>Leon Trampert, Christian Rossow, and Michael Schwarz</i>	
Polymorphic Protocols at the Example of Mitigating Web Bots	106
<i>August See, Leon Fritz, and Mathias Fischer</i>	
Unlinkable Delegation of WebAuthn Credentials	125
<i>Nick Frymann, Daniel Gardham, and Mark Manulis</i>	
Large Scale Analysis of DoH Deployment on the Internet	145
<i>Sebastián García, Joaquín Bogado, Karel Hynek, Dmitrii Vekshin, Tomáš Čejka, and Armin Wasicek</i>	
Equivocal URLs: Understanding the Fragmented Space of URL Parser Implementations	166
<i>Joshua Reynolds, Adam Bates, and Michael Bailey</i>	
Exploring the Characteristics and Security Risks of Emerging Emoji Domain Names	186
<i>Mingxuan Liu, Yiming Zhang, Baojun Liu, and Haixin Duan</i>	

Hardware Security

CPU Port Contention Without SMT 209
Thomas Rokicki, Clémentine Maurice, and Michael Schwarz

Protocols for a Two-Tiered Trusted Computing Base 229
José Moreira, Mark D. Ryan, and Flavio D. Garcia

Using Memristor Arrays as Physical Unclonable Functions 250
*Florian Frank, Tolga Arul, Nikolaos Athanasios Anagnostopoulos,
and Stefan Katzenbeisser*

Multiparty Computation

SecureBiNN: 3-Party Secure Computation for Binarized Neural Network
Inference 275
Wenxing Zhu, Mengqi Wei, Xiangxue Li, and Qiang Li

Mixed-Technique Multi-Party Computations Composed of Two-Party
Computations 295
Erik-Oliver Blass and Florian Kerschbaum

PEA: Practical Private Epistasis Analysis Using MPC 320
*Kay Hamacher, Tobias Kussel, Thomas Schneider,
and Oleksandr Tkachenko*

ML Techniques

Hide and Seek: On the Stealthiness of Attacks Against Deep Learning
Systems 343
Zeyan Liu, Fengjun Li, Jingqiang Lin, Zhu Li, and Bo Luo

Precise Extraction of Deep Learning Models via Side-Channel Attacks
on Edge/Endpoint Devices 364
*Younghan Lee, Sohee Jun, Yungi Cho, Woorim Han, Hyungon Moon,
and Yunheung Paek*

Real-Time Adversarial Perturbations Against Deep Reinforcement
Learning Policies: Attacks and Defenses 384
Buse G. A. Tekgul, Shelly Wang, Samuel Marchal, and N. Asokan

FLMJR: Improving Robustness of Federated Learning via Model Stability 405
Qi Guo, Di Wu, Yong Qi, Saiyu Qi, and Qian Li

MaleficNet: Hiding Malware into Deep Neural Networks Using Spread-Spectrum Channel Coding	425
<i>Dorjan Hitaj, Giulio Pagnotta, Briland Hitaj, Luigi V. Mancini, and Fernando Perez-Cruz</i>	
Long-Short History of Gradients Is All You Need: Detecting Malicious and Unreliable Clients in Federated Learning	445
<i>Ashish Gupta, Tie Luo, Mao V. Ngo, and Sajal K. Das</i>	
MLFM: Machine Learning Meets Formal Method for Faster Identification of Security Breaches in Network Functions Virtualization (NFV)	466
<i>Alaa Oqaily, Yosr Jarraya, Lingyu Wang, Makan Pourzandi, and Suryadipta Majumdar</i>	
Cyber-Physical Systems Security	
Perspectives from a Comprehensive Evaluation of Reconstruction-based Anomaly Detection in Industrial Control Systems	493
<i>Clement Fung, Shreya Srinarasi, Keane Lucas, Hay Bryan Phee, and Lujo Bauer</i>	
A Novel High-Performance Implementation of CRYSTALS-Kyber with AI Accelerator	514
<i>Lipeng Wan, Fangyu Zheng, Guang Fan, Rong Wei, Lili Gao, Yuewu Wang, Jingqiang Lin, and Jiankuo Dong</i>	
From Click to Sink: Utilizing AIS for Command and Control in Maritime Cyber Attacks	535
<i>Ahmed Amro and Vasileios Gkioulos</i>	
Efficient Hash-Based Redactable Signature for Smart Grid Applications	554
<i>Fei Zhu, Xun Yi, Alsharif Abuadbbba, Junwei Luo, Surya Nepal, and Xinyi Huang</i>	
Can Industrial Intrusion Detection Be SIMPLE?	574
<i>Konrad Wolsing, Lea Thiemt, Christian van Sloun, Eric Wagner, Klaus Wehrle, and Martin Henze</i>	
For Your Voice Only: Exploiting Side Channels in Voice Messaging for Environment Detection	595
<i>Matteo Cardaioli, Mauro Conti, and Arpita Ravindranath</i>	
Towards Efficient Auditing for Real-Time Systems	614
<i>Ayoosh Bansal, Anant Kandikuppa, Chien-Ying Chen, Monowar Hasan, Adam Bates, and Sibin Mohan</i>	

Network and Software Security

Towards a Systematic and Automatic Use of State Machine Inference
to Uncover Security Flaws and Fingerprint TLS Stacks 637
Aina Toky Rasoamanana, Olivier Levillain, and Hervé Debar

PanoptiCANs - Adversary-Resilient Architectures for Controller Area
Networks 658
*Bogdan Groza, Lucian Popa, Tudor Andreica, Pal-Stefan Murvay,
Asaf Shabtai, and Yuval Elovici*

Detecting Cross-language Memory Management Issues in Rust 680
Zhuohua Li, Jincheng Wang, Mingshen Sun, and John C. S. Lui

Reach Me if You Can: On Native Vulnerability Reachability in Android
Apps 701
*Luca Borzacchiello, Emilio Coppa, Davide Maiorca, Andrea Columbu,
Camil Demetrescu, and Giorgio Giacinto*

Extensible Virtual Call Integrity 723
*Yuancheng Jiang, Gregory J. Duck, Roland H. C. Yap, Zhenkai Liang,
and Pinghai Yuan*

Posters

Is Your Password Sexist? a Gamification-Based Analysis of the Cultural
Context of Leaked Passwords 743
Daniel Mølmark-O'Connor and Emmanouil Vasilomanolakis

A Fast, Practical and Simple Shortest Path Protocol for Multiparty
Computation 749
Abdelrahman Aly and Sara Cleemput

Audio Spoofing Detection Using Constant-Q Spectral Sketches
and Parallel-Attention SE-ResNet 756
Feng Yue, Jiale Chen, Zhaopin Su, Niansong Wang, and Guofu Zhang

MixCT: Mixing Confidential Transactions from Homomorphic
Commitment 763
*Jiajun Du, Zhonghui Ge, Yu Long, Zhen Liu, Shifeng Sun, Xian Xu,
and Dawu Gu*

Multi-Freq-LDPy: Multiple Frequency Estimation Under Local Differential Privacy in Python	770
<i>Héber H. Arcolez, Jean-François Couchot, Sébastien Gambs, Catuscia Palamidessi, and Majid Zolfaghari</i>	
The Devil Is in the GAN: Backdoor Attacks and Defenses in Deep Generative Models	776
<i>Amrith Rawat, Killian Levacher, and Mathieu Sinn</i>	
Author Index	785