Lecture Notes in Computer Science 12972

More information about this subseries at http://www.springer.com/series/7410

Elisa Bertino · Haya Shulman ·
Michael Waidner (Eds.)

Computer Security – ESORICS 2021

26th European Symposium
on Research in Computer Security
Darmstadt, Germany, October 4–8, 2021
Proceedings, Part I

Springer

Editors
Elisa Bertino
Purdue University
West Lafayette, IN, USA

Michael Waidner
National Research Center for Applied Cybersecurity ATHENE
Technische Universität Darmstadt,
Fraunhofer Institute for Secure Information Technology SIT
Darmstadt, Germany

Haya Shulman
National Research Center for Applied Cybersecurity ATHENE
Fraunhofer Institute for Secure Information Technology SIT
Darmstadt, Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-88417-8 ISBN 978-3-030-88418-5 (eBook)
https://doi.org/10.1007/978-3-030-88418-5

LNCS Sublibrary: SL4 – Security and Cryptology

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 26th European Symposium on Research in Computer Security (ESORICS 2021) was held together with the affiliated workshops during the week of October 4–8, 2021. Due to the COVID-19 pandemic the conference and the workshops took place digitally, hosted by the Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT), within the National Research Center for Applied Cybersecurity ATHENE, Germany.

This year's ESORICS introduced for the first time in the ESORICS conference series two review cycles: a winter cycle and a spring cycle. This follows the general trends for conferences of providing multiple submission deadlines and is not only more convenient for the authors but also allows revision and resubmission for papers. In the case of ESORICS, papers submitted in the winter cycle could be recommended for revision and resubmission to the spring cycle.

In response to the call for papers 351 papers were submitted to the conference. These papers were peer reviewed and subsequently discussed based on their novelty, quality, and contribution by the members of the Program Committee. The submissions were single blind, and all the members of the Program Committee had access to all the submissions and their reviews at all times to facilitate discussions among the members. The submission of the papers and the review process were carried out using the Easychair platform. Based on the reviews and the discussion 71 papers were selected for presentation at the conference. As a result ESORICS had an interesting program covering timely and interesting security and privacy topics in theory, systems, networks, and applications.

The papers that were selected for presentation at ESORICS 2021 were published in a two volume set of proceedings: LNCS 12972 and LNCS 12973.

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 the developers, standardization bodies, and policy makers and by encouraging links with researchers in related fields.

We were honoured to have four keynote speakers: Shafi Goldwasser, Christof Paar, Nicolas Papernot, and Yuval Yarom. Their talks provided interesting insights and research directions in important research areas. The program was complemented by six tutorials given by Anna Cinzia Squicciarini, Yossi Oren, Michael Schwarz, Avishai Wool, and Daphne Yao. For tutorials, ESORICS introduced a novel organization, in that tutorials were given in advance with respect to the conference dates, with the first tutorial given on June 30, 2021, and the last one on September 8, 2021. Tutorial presentations were recorded and are available online. This arrangement takes advantage of today's availability of content dissemination platforms and allows researchers to access the tutorial contents at their own pace.

The Program Committee consisted of 185 members across 31 countries. There were submissions from a total of 1150 authors across 41 countries, with 25 countries represented among the accepted papers. We would like to thank the members of the Program Committee and the external referees for their hard work in supporting the review process as well as everyone who supported the organization of ESORICS. We are grateful to the workshops chairs, Adrian Perrig and David Hay, and all of the workshop co-chairs, the poster chair, Simone Fischer-Hübner, and the ESORICS Steering Committee. We are also grateful to Huawei and IBM Research – Haifa, Israel, for supporting the organization of ESORICS 2021. Finally, we would like to thank the authors for submitting their papers to ESORICS 2021. We hope that the proceedings will promote the research and facilitate future work in the field of security.

September 2021

Elisa Bertino
Haya Shulman
Michael Waidner

Organization

General Chair

Michael Waidner	National Research Center for Applied Cybersecurity ATHENE/Technische Universität Darmstadt/Fraunhofer SIT, Germany

Program Committee Chairs

Elisa Bertino	Purdue University, USA
Haya Shulman	National Research Center for Applied Cybersecurity ATHENE/Fraunhofer SIT, Germany

Steering Committee

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

Program Committee

Ruba Abu-Salma	International Computer Science Institute / University of California, Berkeley, USA
Yehuda Afek	Tel Aviv University, Israel
Mitsuaki Akiyama	NTT, Japan
Cristina Alcaraz	UMA, Spain
Mark Allman	International Computer Science Institute, USA
Vijay Atluri	Rutgers University, USA
Erman Ayday	Case Western Reserve University, USA
Guangdong Bai	University of Queensland, Australia
Lejla Batina	Radboud University, The Netherlands

Steven M. Bellovin	Columbia University, USA
Antonio Bianchi	Purdue University, USA
Marina Blanton	University at Buffalo, USA
Carlo Blundo	Università degli Studi di Salerno, Italy
Tamara Bonaci	Northeastern University, USA
Nora Boulahia Cuppens	Polytechnique Montréal, Canada
Alejandro Cabrera Aldaya	Tampere University of Technology, Finland
Lorenzo Cavallaro	King's College London, UK
Berkay Celik	Purdue University, USA
Aldar C.-F. Chan	BIS Innovation Hub Hong Kong Centre, Hong Kong
Liqun Chen	University of Surrey, UK
Rongmao Chen	National University of Defense Technology, China
Xiaofeng Chen	Xidian University, China
Yu Chen	School of Cyber Science and Technology, Shandong University, China
Sherman Chow	Chinese University of Hong Kong, Hong Kong
Mauro Conti	University of Padua, Italy
Scott Coull	FireEye, Inc., USA
Bruno Crispo	University of Trento, Italy
Michel Cukier	University of Maryland, USA
Frédéric Cuppens	Polytechnique Montréal, Canada
George Danezis	University College London, UK
Sanchari Das	University of Denver, USA
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Hervé Debar	Télécom SudParis, France
Roberto Di Pietro	Hamad Bin Khalifa University, Qatar
Wenrui Diao	Shandong University, China
Tassos Dimitriou	Computer Technology Institute, Greece/Kuwait University, Kuwait
Shlomi Dolev	Ben-Gurion University, Israel
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Changyu Dong	Newcastle University, UK
Haixin Duan	Tsinghua University, China
François Dupressoir	University of Surrey, UK
Pardis Emami Naeini	Carnegie Mellon University, USA
Paulo Esteves-Veríssimo	Université du Luxembourg, Luxembourg
Jose-Luis Ferrer-Gomila	University of the Balearic Islands, Spain
Sara Foresti	Università degli Studi di Milano, Italy
Michael Franz	University of California, Irvine, USA
David Galindo	University of Birmingham, UK
Debin Gao	Singapore Management University, Singapore
Joaquin Garcia-Alfaro	Telecom SudParis, France
Siddharth Garg	New York University, USA
Thanassis Giannetsos	Technical University of Denmark, Denmark
Dieter Gollmann	Hamburg University of Technology, Germany

Neil Gong	Duke University, USA
Stefanos Gritzalis	University of Piraeus, Greece
Daniel Gruss	Graz University of Technology, Austria
Zhongshu Gu	IBM T.J. Watson Research Center, USA
Thomas Haines	Norwegian University of Science and Technology, Norway
Feng Hao	University of Warwick, UK
Juan Hernández-Serrano	Universitat Politècnica de Catalunya, Spain
Xinyi Huang	Fujian Normal University, China
Syed Hussain	Pennsylvania State University, USA
Sotiris Ioannidis	Technical University of Crete, Greece
Tibor Jager	Bergische Universität Wuppertal, Germany
Philipp Jeitner	Fraunhofer SIT, Germany
Yuseok Jeon	Ulsan National Institute of Science and Technology, South Korea
Shouling Ji	Zhejiang University, China
Ghassan Karame	NEC Laboratories Europe, Germany
Sokratis Katsikas	Norwegian University of Science and Technology, Norway
Aggelos Kiayias	University of Edinburgh, UK
Hyoungshick Kim	Sungkyunkwan University, South Korea
Ryan Ko	University of Queensland, Australia
Juliane Krämer	TU Darmstadt, Germany
Steve Kremer	Inria France
Marina Krotofil	Honeywell Industrial Cyber Security Lab, USA
Christopher Kruegel	University of California, Santa Barbara, USA
Yonghwi Kwon	University of Virginia, USA
Costas Lambrinoudakis	University of Piraeus, Greece
Shir Landau-Feibish	The Open University of Israel, Israel
Kyu Hyung Lee	University of Georgia, USA
Corrado Leita	VMware, UK
Shujun Li	University of Kent, UK
Zitao Li	Purdue University, USA
Kaitai Liang	Delft University of Technology, The Netherlands
Xiaojing Liao	Indiana University Bloomington, USA
Hoon Wei Lim	Trustwave, Singapore
Zhiqiang Lin	Ohio State University, USA
Xiangyu Liu	Alibaba Group, China
Joseph Liu	Monash University, Australia
Rongxing Lu	University of New Brunswick, Canada
Xiapu Luo	Hong Kong Polytechnic University, Hong Kong
Shiqing Ma	Rutgers University, USA
Leandros Maglaras	De Montfort University, UK
Fabio Martinelli	IIT-CNR, Italy
Sjouke Mauw	Université du Luxembourg, Luxembourg
Weizhi Meng	Technical University of Denmark, Denmark

Nele Mentens	KU Leuven, Belgium
Mira Mezini	TU Darmstadt, Germany
Chris Mitchell	Royal Holloway, University of London, UK
Tal Moran	Interdisciplinary Center Herzliya, Israel
Tatsuya Mori	Waseda University, Japan
Johannes Mueller	University of Luxembourg, Luxembourg
Max Mühlhäuser	TU Darmstadt, Germany
David Naccache	Ecole normale suprieure, France
Siaw-Lynn Ng	Royal Holloway, University of London, UK
Nick Nikiforakis	Stony Brook University, USA
Jianting Ning	National University of Singapore/Singapore Management University, Singapore
Satoshi Obana	Hosei University, Japan
Martín Ochoa	AppGate Inc., Colombia
Rolf Oppliger	eSECURITY Technologies, Switzerland
Rebekah Overdorf	Ecole Polytechnique Fédérale de Lausanne, Switzerland
Sikhar Patranabis	Visa Research, Palo Alto, USA
Jiaxin Pan	Norwegian University of Science and Technology, Norway
Radia Perlman	Dell EMC, USA
Günther Pernul	Universität Regensburg, Germany
Tran Viet Xuan Phuong	University of Wollongong, Australia
Frank Piessens	KU Leuven, Belgium
Joachim Posegga	University of Passau, Germany
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
Siddharth Prakash Rao	Nokia Bell Labs, USA
Awais Rashid	University of Bristol, UK
Michael Reiter	Duke University, USA
Kui Ren	Zhejiang University, China
Junghwan Rhee	University of Central Oklahoma, USA
Giovanni Russello	University of Auckland, New Zealand
Peter Ryan	University of Luxembourg, Luxembourg
Reihaneh Safavi-Naini	University of Calgary, Canada
Merve Sahin	SAP Security Research, France
Amin Sakzad	Monash University, Australia
Pierangela Samarati	Università degli Studi di Milano, Italy
Damien Sauveron	University of Limoges/CNRS, France
Sebastian Schinzel	FH Münster, Germany
Steve Schneider	University of Surrey, UK
Bruce Schneier	BT, USA
Dominique Schröder	Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
Michael Schwarz	CISPA Helmholtz Center for Information Security, Germany
Joerg Schwenk	Ruhr-Universität Bochum, Germany

Kent Seamons	Brigham Young University, UK
Bardin Sébastien	CEA LIST, France
Jean-Pierre Seifert	TU Berlin, Germany
Siamak F. Shahandashti	University of York, UK
Kris Shrishak	TU Darmstadt, Germany
Radu Sion	Stony Brook University, USA
Nigel Smart	KU Leuven, Belgium
Einar Snekkenes	Norwegian University of Science and Technology, Norway
Juraj Somorovsky	Ruhr-Universität Bochum, Germany
Thorsten Strufe	KIT, Germany
Willy Susilo	University of Wollongong, Australia
Paul Syverson	U.S. Naval Research Laboratory, USA
Qiang Tang	Luxembourg Institute of Science and Technology, Luxembourg
Qiang Tang	University of Sydney, USA
Dave Tian	Purdue University, USA
Laura Tinnel	SRI International, USA
Nils Ole Tippenhauer	CISPA Helmholtz Center for Information Security, Germany
Jacob Torrey	Amazon Web Services, USA
Ari Trachtenberg	Boston University, USA
Helen Treharne	University of Surrey, UK
Aggeliki Tsohou	Ionian University, Greece
Mathy Vanhoef	New York University Abu Dhabi, Abu Dhabi
Luca Viganò	King's College London, UK
Michael Waidner	Fraunhofer SIT/National Research Center for Applied Cybersecurity ATHENE, Germany
Cong Wang	City University of Hong Kong, Hong Kong
Haining Wang	Virginia Tech Research Center - Arlington, USA
Lingyu Wang	Concordia University, Canada
Weihang Wang	SUNY University at Buffalo, USA
Bing Wang	University of Connecticut, USA
Edgar Weippl	University of Vienna/SBA Research, Austria
Avishai Wool	Tel Aviv University, Israel
Christos Xenakis	University of Piraeus, Greece
Yang Xiang	Swinburne University of Technology, Australia
Minhui Xue	University of Adelaide, Australia
Guomin Yang	University of Wollongong, Australia
Jie Yang	Florida State University, USA
Kang Yang	State Key Laboratory of Cryptology, China
Yuval Yarom	University of Adelaide, Australia
Xun Yi	RMIT University, Australia
Yu Yu	Shanghai Jiao Tong University, China
Fengwei Zhang	SUSTech, China
Kehuan Zhang	The Chinese University of Hong Kong, Hong Kong

Yang Zhang	CISPA Helmholtz Center for Information Security, Germany
Yinqian Zhang	Southern University of Science and Technology, China
Yuan Zhang	Fudan University, China
Zhenfeng Zhang	Chinese Academy of Sciences, China
Yunlei Zhao	Fudan University, China
Jianying Zhou	Singapore University of Technology and Design, Singapore
Sencun Zhu	Pennsylvania State University, USA

Workshop Chairs

David Hay	Hebrew University of Jerusalem, Israel
Adrian Perrig	ETH Zurich, Switzerland

Posters Chair

Simone Fischer-Hübner	Karlstad University, Sweden

Publication Chairs

Philipp Jeitner	Fraunhofer SIT, Germany
Hervais Simo	Fraunhofer SIT, Germany

Publicity Chairs

Oliver Küch	Fraunhofer SIT, Germany
Anna Spiegel	Fraunhofer SIT, Germany

Sponsorship Chair

Ute Richter	Fraunhofer SIT, Germany

Local Arrangements Chair

Linda Schreiber	National Research Center for Applied Cybersecurity ATHENE, Germany

Web Chair

Ingo Siedermann	Fraunhofer SIT, Germany

Posters Program Committee

Patricia Arias	KIT, Germany
Xinlei He	CISPA Helmholtz Center for Information Security, Germany
Juliane Krämer	TU Darmstadt, Germany
Erwin Quiring	TU Braunschweig, Germany
Neta Shiff Rozen	Hebrew University of Jerusalem, Israel
Tobias Urban	Westphalian University of Applied Sciences, Germany
Di Wang	King Abdullah University of Science and Technology, Saudi Arabia
Zhikun Zhang	CISPA Helmholtz Center for Information Security, Germany

Additional Reviewers

Alexopoulos, Nikolaos
Amiri Eliasi, Parisa
Andreina, Sebastien
Angelogianni, Anna
Avizheh, Sepideh
Bag, Samiran
Bagheri, Sima
Bamiloshin, Michael
Bampatsikos, Michail
Baumer, Thomas
Baumgärtner, Lars
Binun, Alexander
Bolgouras, Vaios
Bonte, Charlotte
Brighente, Alessandro
Böhm, Fabian
Cao, Yanmei
Caprolu, Maurantonio
Catuogno, Luigi
Cecconello, Stefano
Chen, Jinrong
Chen, Long
Chen, Min
Chen, Xihui
Ciampi, Michele
Cicala, Fabrizio
Dang, Hai-Van
Daudén, Cristòfol
Davies, Gareth
Diemert, Denis
Ding, Hailun
Divakaran, Dinil Mon
Dolev, Shlomi
Dong, Naipeng
Du, Jianqi
Du, Minxin
Duman, Onur
Dutta, Sabyasachi
Eckhart, Matthias
Ehsanpour, Maryam
El Kassem, Nada
Empl, Philip
Esgin, Muhammed F.
Feng, Qi
Ferrag, Mohamed Amine
Freisleben, Bernd
Gaballah, Sarah
Gangwal, Ankit
Gellert, Kai
Ghaedi Bardeh, Navid
Gong, Boru
Han, Donggyun
Handirk, Tobias
Hao, Shuai
Hassan, Fadi
Hatzivasilis, George
Hou, Huiying
Huang, Mengdie

Huang, Zonghao
Ismail, Maliha
Jiang, Hetong
Jiang, Shaoquan
Judmayer, Aljosha
Junming, Ke
Kantarcioglu, Murat
Karim, Imtiaz
Kasinathan, Prabhakaran
Kasra Kermanshahi, Shabnam
Kelarev, Andrei
Kern, Andreas
Kern, Sascha
Kim, Hyungsub
Klement, Felix
Komissarov, Rony
Koutroumpouchos, Nikolaos
Kuchta, Veronika
Kumar, Manish
Kwon, Yonghwi
Köstler, Johannes
Lai, Jianchang
Lakka, Eftychia
Lal, Chhagan
Lampropoulos, Konstantinos
Lee, Jehyun
Li, Rui
Li, Yanan
Li, Yannan
Liber, Matan
Lima Pereira, Hilder Vitor
Lin, Chengyu
Lin, Yan
Liu, Guannan
Liu, Lin
Livsey, Lee
Lopez, Christian
Loss, Julian
Lyu, Lin
Ma, Haoyu
Ma, Jack P. K.
Ma, Mimi
Makriyannis, Nikolaos
Mariot, Luca
Marson, Giorgia Azzurra
Martínez, Sergio
Mateu, Victor
Merzouk, Mohamed-Amine
Mestel, David
Mitropoulos, Charalambos
Mohammadi, Farnaz
Niehues, David
Noorman, Job
O'Connell, Sioli
Oppermann, Alexander
Palamidessi, Catuscia
Pan, Jing
Pang, Bo
Panwar, Nisha
Park, Jeongeun
Petroulakis, Nikolaos
Poeplau, Sebastian
Pradel, Gaëtan
Qiu, Tian
Qiu, Zhi
Rabbani, Md Masoom
Ramírez-Cruz, Yunior
Ringerud, Magnus
Rivera, Esteban
Rizomiliotis, Panagiotis
Román-García, Fernando
Saha, Sayandeep
Sanchez-Rola, Iskander
Schindler, Philipp
Schlette, Daniel
Sentanoe, Stewart
Setayeshfar, Omid
Sharifian, Setareh
Shen, Jun
Shen, Xinyue
Silde, Tjerand
Singla, Ankush
Skrobot, Marjan
Song, Zirui
Spolaor, Riccardo
Stifter, Nicholas
Striecks, Christoph
Struck, Patrick
Tabatabaei, Masoud
Tan, Teik Guan
Teague, Vanessa
Tengana, Lizzy

Tian, Guangwei
Trujillo, Rolando
Tschorsch, Florian
Tu, Binbin
Turrin, Federico
Van Strydonck, Thomas
Vielberth, Manfred
Wang, Coby
Wang, Jiafan
Wang, Kailong
Wang, Qian
Wang, Xiaofeng
Wang, Xiaolei
Wang, Yi
Watanabe, Yohei
Wen, Rui
Wisiol, Nils
Wong, Harry W. H.
Wu, Chen
Wu, Huangting
Xu, Fenghao
Xu, Jia
Yang, Rupeng
Yang, S. J.
Yang, Shishuai
Yang, Xu
Yang, Xuechao
Yang, Zheng
Ying, Jason
Yung, Moti
Zhang, Cong
Zhang, Min
Zhang, Wenlu
Zhang, Yanjun
Zhang, Yubao
Zhang, Yuexin
Zhang, Zhiyi
Zhao, Yongjun
Zou, Yang
Zuo, Cong

Additional Reviewers for Posters

Alexopoulos, Nikolaos
Ma, Yihan
Wang, Cheng-Long
Wen, Rui
Xiang, Zihang
Zhang, Minxing

Keynotes

Algorithms and the Law

Shafi Goldwasser

Massachusetts Institute of Technology (MIT),
Weizmann Institute of Science (WIS)

Abstract. Today, algorithms are proposed to replace several key processes governed by laws, regulations and policies. This requires mathematical definitions of regulations and proofs of algorithmic adherence. We will discuss several such developments.

The Politics and Technology of (Hardware) Trojans

Christof Paar

Ruhr University

Abstract. Over the last decade or so, hardware Trojans have drawn increased attention by the scientific community. They have been mainly considered a technical problem that arises in the context of the globalized semiconductor supply chain. However, low-level Trojans and other forms of backdoors have also a fascinating societal and political component. In this keynote we will present some interesting technical issues of hardware Trojans, especially if they are designed to avoid detection. We will also summarize some of the reported cases of cryptographic backdoors and put them in a political context.

Increasing Trust in ML Through Governance

Nicolas Papernot

University of Toronto

Abstract. The attack surface of machine learning is large: training data can be poisoned, predictions manipulated using adversarial examples, models exploited to reveal sensitive information contained in training data, etc. This is in large parts due to the absence of security and privacy considerations in the design of ML algorithms. Designing secure ML requires that we have a solid understanding as to what we expect legitimate model behavior to look like. We illustrate these directions with recent work on adversarial examples, model stealing, privacy-preserving ML, machine unlearning, and proof of learning.

The Science of Computer Science: An Offensive Research Perspective

Yuval Yarom

School of Computer Science at the University of Adelaide

Abstract. Is computer science a real science? Is offensive security research a scientific activity? To answer these questions, in this talk we explore the state of the art in hardware security research. We discuss anecdotes, directions, and methods and draw parallels to established sciences. Finally, we reach somewhat non-surprising conclusions.

Contents – Part I

Malware

User Behaviour and Underground Economy

Blockchain

Machine Learning

Automotive

Anomaly Detection

Contents – Part II

Encryption

Cryptography

Privacy