

Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering

398

Editorial Board Members

Ozgur Akan

Middle East Technical University, Ankara, Turkey

Paolo Bellavista

University of Bologna, Bologna, Italy

Jiannong Cao

Hong Kong Polytechnic University, Hong Kong, China

Geoffrey Coulson

Lancaster University, Lancaster, UK

Falko Dressler

University of Erlangen, Erlangen, Germany

Domenico Ferrari

Università Cattolica Piacenza, Piacenza, Italy

Mario Gerla

UCLA, Los Angeles, USA

Hisashi Kobayashi

Princeton University, Princeton, USA

Sergio Palazzo

University of Catania, Catania, Italy

Sartaj Sahni

University of Florida, Gainesville, USA

Xuemin (Sherman) Shen 

University of Waterloo, Waterloo, Canada

Mircea Stan

University of Virginia, Charlottesville, USA

Xiaohua Jia

City University of Hong Kong, Kowloon, Hong Kong

Albert Y. Zomaya

University of Sydney, Sydney, Australia

More information about this series at <http://www.springer.com/series/8197>


Joaquin Garcia-Alfaro · Shujun Li ·
Radha Poovendran · Hervé Debar ·
Moti Yung (Eds.)

Security and Privacy in Communication Networks

17th EAI International Conference, SecureComm 2021
Virtual Event, September 6–9, 2021
Proceedings, Part I


Editors

Joaquin Garcia-Alfaro 
Télécom SudParis,
Institut Polytechnique de Paris
Palaiseau, France

Radha Poovendran 
University of Washington
Seattle, WA, USA

Moti Yung 
Google Inc.
New York, NY, USA

Shujun Li 
University of Kent Canterbury
Canterbury, Kent, UK

Hervé Debar 
Télécom SudParis,
Institut Polytechnique de Paris
Palaiseau, France

ISSN 1867-8211 ISSN 1867-822X (electronic)
Lecture Notes of the Institute for Computer Sciences, Social Informatics
and Telecommunications Engineering
ISBN 978-3-030-90018-2 ISBN 978-3-030-90019-9 (eBook)
<https://doi.org/10.1007/978-3-030-90019-9>

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2021

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

We are delighted to introduce the proceedings of the 17th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2021). This conference brought together cybersecurity scholars from all around the world, advancing the state of the art and knowledge of cybersecurity and privacy by proposing new methods and tools to address the major cybersecurity challenges faced by our digital systems.

These proceedings contain 43 papers from the main conference, which were selected out of 126 submissions (with an acceptance rate around 34%) from authors in universities, national laboratories, and the private sector from the Americas, Europe, Asia, Australasia, and Africa. All submissions went through an extensive review process undertaken by 82 internationally-recognized experts in cybersecurity. The accepted papers are authored by researchers from 16 countries, with the USA and China being the top two countries with the most papers (18 and 12, respectively).

These proceedings also contain the following papers from two co-located workshops and two other tracks of the conference: five papers accepted to the International Workshop on Post-quantum Cryptography for Secure Communications (PQC-SC), two papers accepted to the International Workshop on Cyber-Physical Systems Strategic and Technical Security (CPS-STs), and four papers to the PhD and Poster Tracks. Submissions to these workshops and tracks were organized by the separate (co-)chairs: Kalpana Singh, Elisa Lorenzo Garcia, Rajeev Anand Sahu, Gaurav Sharma, and T. Chithralekha who co-chaired PQC-SC, Ali Ismail Awad, Charalambos Konstantinou, and Mohammed M. Alani who co-chaired CPS-STs, and Roger A. Hallman who chaired the PhD and Poster Tracks. The accepted papers in these workshops and tracks are authored by researchers from seven different countries (USA, China, Brazil, Italy, South Korea, UAE, and UK).

Any successful conference relies on the contribution of multiple stakeholders, who have volunteered their time and energy in disseminating and publicizing the call for papers, submitting original research results, participating in the reviewing process, and in the end contributing altogether to a great program. First and foremost, we would like to offer our gratitude to the entire Organizing Committee for guiding the entire process of the conference, keeping everything organized and in check. We are also deeply grateful to all the Technical Program Committee (TPC) members for their time and effort in reading, commenting, debating, and finally selecting the papers. We also thank the (co-)chairs, TPC members, and external reviewers of the co-located workshops and the PhD/Poster Tracks for their contributions to the conference. Last but not least, we also thank all the authors who submitted papers to the conference and all participants who attended the conference to support the conference and make it a successful event. Support from the Steering Committee and EAI staff members was also crucial in ensuring the success of the conference. It was a great privilege to work with such a large group of dedicated and talented individuals.

We had hoped for a physical event, and it is unfortunate that we once more had to revert to an online one. We nevertheless hope that you found the discussions and interactions at SecureComm 2021 enjoyable and that the proceedings will simulate further research.

August 2021

Shujun Li
Radha Poovendran
Hervé Debar
Moti Yung

Conference Organization

Steering Committee

Imrich Chlamtac	University of Trento, Italy
Guofei Gu	Texas A&M University, USA
Peng Liu	Pennsylvania State University, USA
Sencun Zhu	Pennsylvania State University, USA

Organizing Committee

General Chair

Shujun Li	University of Kent, UK
-----------	------------------------

General Co-chair

Radha Poovendran	University of Washington, USA
------------------	-------------------------------

Technical Program Committee Chair and Co-chair

Hervé Debar	Télécom SudParis/Institut Polytechnique de Paris, France
Moti Yung	Google Inc./Columbia University, USA

Sponsorship and Exhibit Chair

Theodosios Dimitrakos	Munich Research Centre, Huawei Technologies Ltd, Germany
-----------------------	---

Local Chairs

Budi Arief	University of Kent, UK
Gareth Howells	University of Kent, UK

Workshops Chair

David Arroyo Guardado	CSIC, Spain
-----------------------	-------------

Publicity and Social Media Chairs

Jason Nurse	University of Kent, UK
Kaitai Liang	TU Delft, The Netherlands

Publications Chair

Joaquin Garcia-Alfaro	Télécom SudParis/Institut Polytechnique de Paris, France
-----------------------	---

Web Chair

Christophe Kiennert	Télécom SudParis/Institut Polytechnique de Paris, France
---------------------	---

Posters and PhD Track Chair

Roger A. Hallman	Naval Information Warfare Center Pacific/Dartmouth College, USA
------------------	--

Panels Chairs

Julio Hernandez-Castro	University of Kent, UK
Sanjay Bhattacharjee	University of Kent, UK

Tutorials Chair

Anyi Liu	Oakland University, USA
----------	-------------------------

Technical Program Committee

Magnus Almgren	Chalmers University of Technology, Sweden
Elias Athanasopoulos	University of Cyprus, Cyprus
Gregory Blanc	Télécom SudParis/Institut Polytechnique de Paris, France
Sébastien Bardin	CEA LIST, France
Lorenzo Cavallaro	Kings College London, UK
Lucas Davi	University of Duisburg-Essen, Germany
Gabi Dreö	Bundeswehr University Munich, Germany
Sven Dietrich	City University of New York, USA
Daniel Gruss	Graz University of Technology, Austria
Christophe Hauser	University of Southern California, USA
Vasileios Kemerlis	Brown University, USA
Andrea Lanzi	University of Milan, Italy
Fabio Martinelli	CNR, Italy
Michael Meier	University of Bonn/Fraunhofer FKIE, Germany
Marius Muench	Vrije Universiteit Amsterdam, The Netherlands
William Robertson	Northeastern University, USA
Thomas Schreck	Munich University of Applied Sciences, Germany
Seungwon Shin	KAIST, South Korea
Angelos Stavrou	George Mason University, USA

Gianluca Stringhini	Boston University, USA
Giovanni Apruzzese	University of Liechtenstein, Liechtenstein
Urko Zurutuza	Mondragon University, Spain
Fabio Di Franco	ENISA, Greece
Platon Kotzias	NortonLifeLock Research Group, Greece
Sokratis Katsikas	NTNU, Norway
Razvan Beuran	JAIST, Japan
Youki Kadobayashi	NAIST, Japan
Franco Chiaraluze	UNIVPM, Italy
Igor Kotenko	St. Petersburg Federal Research Center of the Russian Academy of Sciences, Russia
Evangelos Markatos	FORTH, Greece
Silvia Bonomi	Sapienza University of Rome, Italy
Apostolis Zarras	TU Delft, The Netherlands
Jan Hajný	Brno University of Technology, Czech Republic
Gabriele Restuccia	CNIT, Italy
Jacques Traore	Orange, France
Jouni Viinikka	6Cure, France
Pavel Laskov	University of Lichtenstein, Lichtenstein
Michal Choras	ITTI, Poland
Olivier Thonnard	Amadeus, France
Roland Rieke	Fraunhofer SIT, Germany
Ali Abbasi	Ruhr University Bochum, Germany
Claudio Canella	TU Graz, Austria
Jun Xu	Stevens Institute of Technology, USA
Cristian-Alexander Staicu	CISPA, Germany
Guillaume Hiet	CentraleSupélec, France
Sharif Abuadbba	Data61, CSIRO, Australia
Mohiuddin Ahmed	Edith Cowan University, Australia
Nadeem Ahmed	Cyber Security Cooperative Research Centre, Australia
Ehab Al-Shaer	Carnegie Mellon University, USA
Budi Arief	University of Kent, UK
Anirban Basu	Hitachi, Ltd, Japan/University of Sussex, UK
Sanjay Bhattacharjee	University of Kent, UK
Liquan Chen	Southeastern University, China
Jinguang Han	Nanjing University of Finance and Economics, China
Debiao He	Wuhan University, China
Julio Hernandez-Castro	University of Kent, UK
Darren Hurley-Smith	Royal Holloway University of London, UK
Zahid Islam	Charles Sturt University, Australia

Helge Janicke	Cyber Security Cooperative Research Centre, Australia
Shancang Li	University of the West of England, UK
Yingjiu Li	University of Oregon, USA
Kaitai Liang	TU Delft, The Netherlands
Anyi Liu	Oakland University, USA
Zhe Liu	Nanjing University of Aeronautics and Astronautics, China
George Loukas	University of Greenwich, UK
Xiapu Luo	Hong Kong Polytechnic University, Hong Kong
Leandros Maglaras	De Montfort University, UK
Kalikinkar Mandal	University of New Brunswick, Canada
Mark Manulis	University of Surrey, UK
Carsten Maple	University of Warwick, UK
Wojciech Mazurczyk	Warsaw University of Technology, Poland
Weizhi Meng	Technical University of Denmark, Denmark
Nour Moustafa	UNSW Canberra, Australia
Toni Perković	University of Split, Croatia
Siraj Ahmed Shaikh	University of Coventry, UK
Chunhua Su	University of Aizu, Japan
Zhiyuan Tan	Edinburgh Napier University, UK
Ding Wang	Nankai University, China
Wei Wang	Beijing Jiaotong University, China
Yongdong Wu	Jinan University, China
Xiaosong Zhang	University of Electronic Science and Technology of China, China
Deqing Zou	Huazhong University of Science and Technology, China
Sushmita Ruj	Data61, CSIRO, Australia/ISI, Kolkata, India
Guomin Yang	University of Wollongong, Australia
Louis Rilling	Inria Rennes - Bretagne Atlantique, France

Contents – Part I

Cyber Threats and Defence

DeepHunter: A Graph Neural Network Based Approach for Robust Cyber Threat Hunting	3
<i>Renzheng Wei, Lijun Cai, Lixin Zhao, Aimin Yu, and Dan Meng</i>	
SIEMA: Bringing Advanced Analytics to Legacy Security Information and Event Management	25
<i>Pejman Najafi, Feng Cheng, and Christoph Meinel</i>	
Automatic Generation of Malware Threat Intelligence from Unstructured Malware Traces	44
<i>Yuheng Wei and Futai Zou</i>	
Towards Automated Assessment of Vulnerability Exposures in Security Operations	62
<i>Philip Huff and Qinghua Li</i>	
Repeatable Experimentation for Cybersecurity Moving Target Defense	82
<i>Jaime C. Acosta, Luisana Clarke, Stephanie Medina, Monika Akbar, Mahmud Shahriar Hossain, and Frederica Free-Nelson</i>	
MPD: Moving Target Defense Through Communication Protocol Dialects	100
<i>Yongsheng Mei, Kailash Gogineni, Tian Lan, and Guru Venkataramani</i>	

Blockchain and P2P Security

GuardedGossip: Secure and Anonymous Node Discovery in Untrustworthy Networks	123
<i>Andriy Panchenko, Asya Mitseva, Torsten Ziemann, and Till Hering</i>	
An Extensive Security Analysis on Ethereum Smart Contracts	144
<i>Mohammadreza Ashouri</i>	
A Distributed Ledger for Non-attributable Cyber Threat Intelligence Exchange	164
<i>Philip Huff and Qinghua Li</i>	

AI and Security/Privacy

Understanding ϵ for Differential Privacy in Differencing Attack Scenarios 187
Narges Ashena, Daniele Dell’Aglio, and Abraham Bernstein

Explanation-Guided Diagnosis of Machine Learning Evasion Attacks 207
Abderrahmen Amich and Birhanu Eshete

ToFi: An Algorithm to Defend Against Byzantine Attacks in Federated Learning 229
Qi Xia, Zeyi Tao, and Qun Li

TESLAC: Accelerating Lattice-Based Cryptography with AI Accelerator 249
Lipeng Wan, Fangyu Zheng, and Jingqiang Lin

Research of CPA Attack Methods Based on Ant Colony Algorithm 270
Xiaoyi Duan, You Li, Jianmin Tong, Xiuying Li, Siman He, and Peishu Zhang

Local Model Privacy-Preserving Study for Federated Learning 287
Kaiyun Pan, Daojing He, and Chuan Xu

Applied Cryptography

Cryptonite: A Framework for Flexible Time-Series Secure Aggregation with Non-interactive Fault Recovery 311
Ryan Karl, Jonathan Takeshita, and Taeho Jung

Cryptonomial: A Framework for Private Time-Series Polynomial Calculations 332
Ryan Karl, Jonathan Takeshita, Alamin Mohammed, Aaron Striegel, and Taeho Jung

Provably Secure Contact Tracing with Conditional Private Set Intersection 352
Jonathan Takeshita, Ryan Karl, Alamin Mohammed, Aaron Striegel, and Taeho Jung

Origin Attribution of RSA Public Keys 374
Enrico Branca, Farzaneh Abazari, Ronald Rivera Carranza, and Natalia Stakhanova

Network Security

Fine-Grained Intra-domain Bandwidth Allocation Against DDoS Attack	399
<i>Lijia Xie, Shuang Zhao, Xiao Zhang, Yiming Shi, Xin Xiao, and Zhiming Zheng</i>	
TMT-RF: Tunnel Mixed Traffic Classification Based on Random Forest	418
<i>Panpan Zhao, Gaopeng Gou, Chang Liu, Yangyang Guan, Mingxin Cui, and Gang Xiong</i>	
CROCUS: An Objective Approach for SDN Controllers Security Assessment	438
<i>Carlos Silva, Bruno Sousa, and João P. Vilela</i>	
Controlling Network Traffic Microstructures for Machine-Learning Model Probing	456
<i>Henry Clausen, Robert Flood, and David Aspinall</i>	
Using NetFlow to Measure the Impact of Deploying DNS-based Blacklists	476
<i>Martin Fejrskov, Jens Myrup Pedersen, and Emmanouil Vasilomanolakis</i>	
Digital Forensics	
A Forensic Tool to Acquire Radio Signals Using Software Defined Radio	499
<i>M. A. Hannan Bin Azhar and German Abadia</i>	
SEMFLOW: Accurate Semantic Identification from Low-Level System Data	513
<i>Mohammad Kavousi, Runqing Yang, Shiqing Ma, and Yan Chen</i>	
Author Index	537

Contents – Part II

Web/OSN Security and Privacy

Analyzing Security Risks of Ad-Based URL Shortening Services Caused by Users' Behaviors	3
<i>Naoki Fukushi, Takashi Koide, Daiki Chiba, Hiroki Nakano, and Mitsuaki Akiyama</i>	
XHunter: Understanding XXE Vulnerability via Automatic Analysis	23
<i>Zhenhua Wang, Wei Xie, Jing Tao, Yong Tang, and Enze Wang</i>	
Anonymous Short Communications over Social Networks	43
<i>Francesco Buccafurri, Vincenzo De Angelis, Maria Francesca Idone, and Cecilia Labrini</i>	
A Sybil Detection Method in OSN Based on DistilBERT and Double-SN-LSTM for Text Analysis	64
<i>Xiaojie Xu, Jian Dong, Zhengyu Liu, Jin Yang, Bin Wang, and Zhaoyuan Wang</i>	

ePayment Security

An Empirical Study on Mobile Payment Credential Leaks and Their Exploits	79
<i>Shangcheng Shi, Xianbo Wang, Kyle Zeng, Ronghai Yang, and Wing Cheong Lau</i>	
System-Wide Security for Offline Payment Terminals	99
<i>Nikolay Ivanov and Qiben Yan</i>	
Horus: A Security Assessment Framework for Android Crypto Wallets	120
<i>Md Shahab Uddin, Mohammad Mannan, and Amr Youssef</i>	

Systems Security

Leakuidator: Leaky Resource Attacks and Countermeasures	143
<i>Mojtaba Zaheri and Reza Curtmola</i>	
JABBIK Lookups: A Backend Telemetry-Based System for Malware Triage ...	164
<i>Octavian Ciprian Bordeanu, Gianluca Stringhini, Yun Shen, and Toby Davies</i>	

Facilitating Parallel Fuzzing with Mutually-Exclusive Task Distribution	185
<i>Yifan Wang, Yuchen Zhang, Chenbin Pang, Peng Li, Nikolaos Triandopoulos, and Jun Xu</i>	

Flowrider: Fast On-Demand Key Provisioning for Cloud Networks	207
<i>Nicolae Paladi, Marco Tiloca, Pegah Nikbakht Bideh, and Martin Hell</i>	

Mobile Security and Privacy

Mobile Handset Privacy: Measuring the Data iOS and Android Send to Apple and Google	231
<i>Douglas J. Leith</i>	

Who's Accessing My Data? Application-Level Access Control for Bluetooth Low Energy	252
<i>Pallavi Sivakumaran and Jorge Blasco</i>	

HTPD: Secure and Flexible Message-Based Communication for Mobile Apps	273
<i>Yin Liu, Breno Dantas Cruz, and Eli Tilevich</i>	

Smartphone Location Spoofing Attack in Wireless Networks	295
<i>Chengbin Hu, Yao Liu, Zhuo Lu, Shangqing Zhao, Xiao Han, and Junjie Xiong</i>	

IoT Security and Privacy

Compromised Through Compression: Privacy Implications of Smart Meter Traffic Analysis	317
<i>Pol Van Aubel and Erik Poll</i>	

iDDAF: An Intelligent Deceptive Data Acquisition Framework for Secure Cyber-Physical Systems	338
<i>Md Hasan Shahriar, Mohammad Ashiqur Rahman, Nur Intiazul Haque, Badrul Chowdhury, and Steven G. Whisenant</i>	

PhD and Poster Track

Encouraging the Adoption of Post-Quantum Hybrid Key Exchange in Network Security	363
<i>Alexandre Augusto Giron</i>	

Quantitative and Qualitative Investigations into Trusted Execution Environments	372
<i>Ryan Karl</i>	

Phishing Web Page Detection with Semi-Supervised Deep Anomaly Detection	384
<i>Linshu Ouyang and Yongzheng Zhang</i>	
Poisoning Attack for Inter-agent Transfer Learning	394
<i>Zelei Cheng and Zuotian Li</i>	
PQC-SC Workshop	
An Efficient Post-Quantum PKE from RLWR with Simple Security Proof	407
<i>Parhat Abla and Mingsheng Wang</i>	
Kyber on ARM64: Compact Implementations of Kyber on 64-Bit ARM Cortex-A Processors	424
<i>Pakize Sanal, Emrah Karagoz, Hwajeong Seo, Reza Azarderakhsh, and Mehran Mozaffari-Kermani</i>	
Compressed SIKE Round 3 on ARM Cortex-M4	441
<i>Mila Anastasova, Mojtaba Bisheh-Niasar, Reza Azarderakhsh, and Mehran Mozaffari Kermani</i>	
A Quantum Circuit to Speed-Up the Cryptanalysis of Code-Based Cryptosystems	458
<i>Simone Perriello, Alessandro Barenghi, and Gerardo Pelosi</i>	
Hardware Deployment of Hybrid PQC: SIKE+ECDH	475
<i>Reza Azarderakhsh, Rami Elkhatib, Brian Koziel, and Brandon Langenberg</i>	
CPS-STs Workshop	
Towards Stealing Deep Neural Networks on Mobile Devices	495
<i>Shashank Reddy Danda, Xiaoyong Yuan, and Bo Chen</i>	
Phishing Website Detection from URLs Using Classical Machine Learning ANN Model	509
<i>Said Salloum, Tarek Gaber, Sunil Vadera, and Khaled Shaalan</i>	
Author Index	525