

## Preface

Li, Fengjun; Liang, Kaitai; Lin, Zhiqiang; Katsikas, Sokratis K.

### Publication date

2023

### Document Version

Final published version

### Published in

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

### Citation (APA)

Li, F., Liang, K., Lin, Z., & Katsikas, S. K. (2023). Preface. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 462 LNICST*.

### Important note

To cite this publication, please use the final published version (if applicable). Please check the document version above.

### Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

### Takedown policy

Please contact us and provide details if you believe this document breaches copyrights. We will remove access to the work immediately and investigate your claim.

***Green Open Access added to TU Delft Institutional Repository***

***'You share, we take care!' - Taverne project***

**<https://www.openaccess.nl/en/you-share-we-take-care>**

Otherwise as indicated in the copyright section: the publisher is the copyright holder of this work and the author uses the Dutch legislation to make this work public.

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

462

## 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 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 <https://link.springer.com/bookseries/8197>

Fengjun Li · Kaitai Liang · Zhiqiang Lin ·  
Sokratis K. Katsikas (Eds.)

# Security and Privacy in Communication Networks


18th EAI International Conference, SecureComm 2022  
Virtual Event, October 2022  
Proceedings

*Editors*

Fengjun Li   
University of Kansas  
Lawrence, KS, USA

Zhiqiang Lin   
The Ohio State University  
Columbus, OH, USA

Kaitai Liang   
Delft University of Technology  
Delft, The Netherlands

Sokratis K. Katsikas   
Norwegian University of Science and Tech  
Gjøvik, Norway

ISSN 1867-8211

ISSN 1867-822X (electronic)

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

ISBN 978-3-031-25537-3

ISBN 978-3-031-25538-0 (eBook)

<https://doi.org/10.1007/978-3-031-25538-0>

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2023

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 18th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2022). This conference brought together researchers and practitioners working in academia, industry, government, to explore important research directions in the field.

These proceedings contain 40 papers, which were selected from 126 submissions (an acceptance rate of 31.7%) from universities, national laboratories, and the private sector from the Americas, Europe, Asia, Australasia, and Africa. All the submissions went through an extensive review process by internationally recognized experts in cybersecurity. The accepted papers are authored by researchers from 11 countries, with China and the USA being the top two countries with the most papers. These proceedings also contain three papers from the International Workshop on Security and Privacy-preserving Solutions in the Internet of Things (S/P-IoT).

Any successful conference requires the contributions of different stakeholder groups and individuals, who have unselfishly volunteered their time and energy in disseminating the call for papers, submitting their research findings, participating in the peer reviews and discussions, etc. First and foremost, we would like to offer our gratitude to the entire Organizing Committee for guiding the entire process of the conference. We are also deeply grateful to all the Technical Program Committee members for their time and efforts in reading, commenting, debating, and finally selecting the papers. We also thank all the external reviewers for assisting the Technical Program Committee in their particular areas of expertise as well as all the authors, participants, and session chairs for their valuable contributions. 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 be working with such a large group of dedicated and talented individuals.

The 18th SecureComm Conference was originally planned to be held in Kansas City, KS, USA. It is unfortunate that we had to revert to an online conference in 2022. We hope that the discussions and interactions were enjoyable, and that the proceedings will stimulate further research.

October 2022

Fengjun Li  
Kaitai Liang  
Zhiqiang Lin  
Sokratis K. Katsikas

# Conference Organization

## Steering Committee

Imrich Chlamtac	Bruno Kessler Professor, 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 Co-chairs

Fengjun Li	University of Kansas, USA
Kaitai Liang	TU Delft, The Netherlands

### TPC Chair and Co-chair

Zhiqiang Lin	The Ohio State University, USA
Sokratis Katsikas	Norwegian University of Science and Technology, Norway

### Sponsorship and Exhibit Chair

Drew Davidson	The University of Kansas, USA
---------------	-------------------------------

### Local Chairs

Bo Luo	The University of Kansas, USA
Alex Bardas	The University of Kansas, USA

### Workshops Chairs

Lannan Luo	George Mason University, USA
Fatih Turkmen	University of Groningen, The Netherlands

### Publicity and Social Media Chairs

Peng Liu	Pennsylvania State University, USA
Jingqiang Lin	University of Science and Technology of China, China



## **Publications Chairs**

Jun Shao Zhejiang Gongshang University, China  
Stjepan Picek Radboud University, The Netherlands

## **Web Chair**

Apostolis Zarras TU Delft, The Netherlands

## **Technical Program Committee**

Ali Abbasi Ruhr-University Bochum, Germany  
Sharif Abuadbbba CSIRO's Data61, Australia  
Mohiuddin Ahmed Edith Cowan University, Australia  
Nadeem Ahmed The University of New South Wales (UNSW),  
Australia  
Magnus Almgren Chalmers University of Technology, Sweden  
Ehab Al-Shaer Carnegie Mellon University, USA  
Marios Anagnostopoulos Aalborg University, Denmark  
Giovanni Apruzzese University of Liechtenstein, Liechtenstein  
David Arroyo Spanish National Research Council, Spain  
Elias Athanasopoulos University of Cyprus, Cyprus  
Razvan Beuran Japan Advanced Institute of Science and  
Technology, Japan  
Silvia Bonomi Sapienza University of Rome, Italy  
Sanchuan Chen Fordham University, USA  
Bo Chen Michigan Technological University, USA  
Guoxing Chen Shanghai Jiao Tong University, China  
Franco Chiaraluce Università Politecnica delle Marche, Italy  
Fabio Di Franco ENISA, Greece  
Shanqing Guo Shandong University, China  
Guillaume Hiet CentraleSupélec, France  
Darren Hurley-Smith Royal Holloway University of London, UK  
Taeho Jung University of Notre Dame, USA  
Nesrine Kaaniche Télécom SudParis, France  
Georgios Kavallieratos Norwegian University of Science and Technology,  
Norway  
Igor Kotenko St. Petersburg Institute for Informatics and  
Automation, Russia  
Platon Kotzias Norton LifeLock Research Labs, USA  
Shaofeng Li PengCheng Laboratory, China  
Juanru Li Shanghai Jiao Tong University, China  
Ming Li UT Arlington, USA  
George Loukas University of Greenwich, UK

Bo Luo	University of Kansas, USA
Xiapu Luo	The Hong Kong Polytechnic University, Hong Kong, China
Leandros Maglaras	De Montfort University, UK
Kalikinkar Mandal	University of New Brunswick, Canada
Evangelos Markatos	ICS-FORTH, Greece
Fabio Martinelli	Italian National Research Council, Italy
Wojciech Mazurczyk	Warsaw University of Technology, Poland
Weizhi Meng	Technical University of Denmark, Denmark
Nour Moustafa	UNSW Canberra, Australia
Mehari Msgna	Norwegian University of Science and Technology, Norway
Toni Perkovic	University of Split, Croatia
Roberto Di Pietro	Hamad Bin Khalifa University, Qatar
Nikolaos Pitropakis	Edinburgh Napier University, UK
Gabriele Restuccia	University of Palermo, Italy
Roland Schmitz	Stuttgart Media University, Germany
Thomas Schreck	Munich University of Applied Sciences, Germany
Georgios Spathoulas	Norwegian University of Science and Technology, Norway
Yuzhe Tang	Syracuse University, USA
Jacques Traore	Orange Labs, France
Ding Wang	Nankai University, China
Christos Xenakis	University of Piraeus, Greece
Qiben Yan	Michigan State University, USA
Guomin Yang	University of Wollongong, Australia
Xu Yuan	University of Louisiana at Lafayette, USA
Apostolis Zarras	TU Delft, The Netherlands
Yingpei Zeng	Hangzhou Dianzi University, China
Ning Zhang	Washington University in St. Louis, USA
Tianwei Zhang	Nanyang Technological University, Singapore
Xiaokuan Zhang	George Mason University, USA
Yue Zhang	The Ohio State University, USA
Qingchuan Zhao	City University of Hong Kong, Hong Kong, China
Ziming Zhao	University at Buffalo, USA
Haojin Zhu	Shanghai Jiaotong University, China
Urko Zurutuza	Mondragon Unibertsitate, Spain

# Contents

## AI for Security

Classification-Based Anomaly Prediction in XACML Policies .....	3
<i>Maryam Davari and Mohammad Zulkernine</i>	
An Evolutionary Learning Approach Towards the Open Challenge of IoT Device Identification .....	20
<i>Jingfei Bian, Nan Yu, Hong Li, Hongsong Zhu, Qiang Wang, and Limin Sun</i>	
SecureBERT: A Domain-Specific Language Model for Cybersecurity .....	39
<i>Ehsan Aghaei, Xi Niu, Waseem Shadid, and Ehab Al-Shaer</i>	
CapsITD: Malicious Insider Threat Detection Based on Capsule Neural Network .....	57
<i>Haitao Xiao, Chen Zhang, Song Liu, Bo Jiang, Zhigang Lu, Fei Wang, and Yuling Liu</i>	
Towards High Transferability on Neural Network for Black-Box Adversarial Attacks .....	72
<i>Haochen Zhai, Futai Zou, Junhua Tang, and Yue Wu</i>	
Coreference Resolution for Cybersecurity Entity: Towards Explicit, Comprehensive Cybersecurity Knowledge Graph with Low Redundancy .....	89
<i>Zhengyu Liu, Haochen Su, Nannan Wang, and Cheng Huang</i>	

## Applied Cryptography

Another Lattice Attack Against ECDSA with the wNAF to Recover More Bits per Signature .....	111
<i>Ziqiang Ma, Shuaigang Li, Jingqiang Lin, Quanwei Cai, Shuqin Fan, Fan Zhang, and Bo Luo</i>	
MAG-PUF: Magnetic Physical Unclonable Functions for Device Authentication in the IoT .....	130
<i>Omar Adel Ibrahim, Savio Sciancalepore, and Roberto Di Pietro</i>	
A Cross-layer Plausibly Deniable Encryption System for Mobile Devices .....	150
<i>Niusen Chen, Bo Chen, and Weisong Shi</i>	

**Binary Analysis**

Language and Platform Independent Attribution of Heterogeneous Code ..... 173  
*Farzaneh Abazari, Enrico Branca, Evgeniya Novikova,  
 and Natalia Stakhanova*

Multi-relational Instruction Association Graph for Cross-Architecture  
 Binary Similarity Comparison ..... 192  
*Qige Song, Yongzheng Zhang, and Shuhao Li*

Cost-Effective Malware Classification Based on Deep Active Learning ..... 212  
*Qian Qiang, Yige Chen, Yang Hu, Tianning Zang, Mian Cheng,  
 Quanbo Pan, Yu Ding, and Zisen Qi*

**Blockchain**

CTDRB: Controllable Timed Data Release Using Blockchains ..... 231  
*Jingzhe Wang and Balaji Palanisamy*

FairBlock: Preventing Blockchain Front-Running with Minimal Overheads .... 250  
*Peyman Momeni, Sergey Gorbunov, and Bohan Zhang*

Blockchain-Based Ciphertext Policy-Hiding Access Control Scheme ..... 272  
*Ruizhong Du and Tianhe Zhang*

Granting Access Privileges Using OpenID Connect in Permissioned  
 Distributed Ledgers ..... 290  
*Shohei Kakei, Yoshiaki Shiraishi, and Shoichi Saito*

Decentralized and Efficient Blockchain Rewriting with Bi-level Validity  
 Verification ..... 309  
*Kemin Zhang, Li Yang, Lu Zhou, and Jianfeng Ma*

**Cryptography**

TERSE: Tiny Encryptions and Really Speedy Execution for Post-Quantum  
 Private Stream Aggregation ..... 331  
*Jonathan Takeshita, Zachariah Carmichael, Ryan Karl, and Taeho Jung*

Symmetrical Disguise: Realizing Homomorphic Encryption Services  
 from Symmetric Primitives ..... 353  
*Alexandros Bakas, Eugene Frimpong, and Antonis Michalas*

Replicated Additive Secret Sharing with the Optimized Number of Shares . . . . .	371
<i>Juanjuan Guo, Mengjie Shuai, Qiong Xiao Wang, Wenyuan Li, and Jingqiang Lin</i>	
Generic 2-Party PFE with Constant Rounds and Linear Active Security, and Efficient Instantiation . . . . .	390
<i>Hanyu Jia, Xiangxue Li, Qiang Li, Yue Bao, and Xintian Hou</i>	
<b>Data Security</b>	
A Random Reversible Watermarking Scheme for Relational Data . . . . .	413
<i>Qiang Liu, Hequ Xian, Jiancheng Zhang, and Kunpeng Liu</i>	
Enabling Accurate Data Recovery for Mobile Devices Against Malware Attacks . . . . .	431
<i>Wen Xie, Niusen Chen, and Bo Chen</i>	
Bootstrapping Trust in Community Repository Projects . . . . .	450
<i>Sangat Vaidya, Santiago Torres-Arias, Justin Cappos, and Reza Curtmola</i>	
<b>Intrusion Detection</b>	
Assessing the Quality of Differentially Private Synthetic Data for Intrusion Detection . . . . .	473
<i>Md Ali Reza Al Amin, Sachin Shetty, Valerio Formicola, and Martin Otto</i>	
Forensic Analysis and Detection of Spoofing Based Email Attack Using Memory Forensics and Machine Learning . . . . .	491
<i>Sanjeev Shukla, Manoj Misra, and Gaurav Varshney</i>	
AttackMiner: A Graph Neural Network Based Approach for Attack Detection from Audit Logs . . . . .	510
<i>Yuedong Pan, Lijun Cai, Tao Leng, Lixin Zhao, Jiangang Ma, Aimin Yu, and Dan Meng</i>	
Hiatus: Unsupervised Generative Approach for Detection of DoS and DDoS Attacks . . . . .	529
<i>Sivaanandh Muneeswaran, Vinay Sachidananda, Rajendra Patil, Hongyi Peng, Mingchang Liu, and Mohan Gurusamy</i>	
<b>Mobile Security</b>	
What Data Do the Google Dialer and Messages Apps on Android Send to Google? . . . . .	549
<i>Douglas J. Leith</i>	

Detection and Privacy Leakage Analysis of Third-Party Libraries in Android Apps .....	569
<i>Xiantong Hao, Dandan Ma, and Hongliang Liang</i>	
Secure CV2X Using COTS Smartphones over LTE Infrastructure .....	588
<i>Spandan Mahadevegowda, Ryan Gerdes, Thidapat Chantem, and Rose Qingyang Hu</i>	
<b>Network Security</b>	
DQR: A Double Q Learning Multi Agent Routing Protocol for Wireless Medical Sensor Network .....	611
<i>Muhammad Shadi Hajar, Harsha Kalutarage, and M. Omar Al-Kadri</i>	
Message Recovery Attack of Kyber Based on Information Leakage in Decoding Operation .....	630
<i>Mengyao Shi, Zhu Wang, Tingting Peng, and Fenghua Li</i>	
PII-PSM: A New Targeted Password Strength Meter Using Personally Identifiable Information .....	648
<i>Qiyong Dong, Ding Wang, Yaosheng Shen, and Chunfu Jia</i>	
<b>Privacy</b>	
Silver Surfers on the Tech Wave: Privacy Analysis of Android Apps for the Elderly .....	673
<i>Pranay Kapoor, Rohan Pagey, Mohammad Mannan, and Amr Youssef</i>	
MetaPriv: Acting in Favor of Privacy on Social Media Platforms .....	692
<i>Robert Cantaragiu, Antonis Michalas, Eugene Frimpong, and Alexandros Bakas</i>	
Adversary for Social Good: Leveraging Attribute-Obfuscating Attack to Protect User Privacy on Social Networks .....	710
<i>Xiaoting Li, Lingwei Chen, and Dinghao Wu</i>	
<b>Software Security</b>	
No-Fuzz: Efficient Anti-fuzzing Techniques .....	731
<i>Zhengxiang Zhou, Cong Wang, and Qingchuan Zhao</i>	
eSROP Attack: Leveraging Signal Handler to Implement Turing-Complete Attack Under CFI Defense .....	752
<i>Tianning Zhang, Miao Cai, Diming Zhang, and Hao Huang</i>	

**Breaking Embedded Software Homogeneity with Protocol Mutations** ..... 770  
*Tongwei Ren, Ryan Williams, Sirshendu Ganguly, Lorenzo De Carli, and Long Lu*

**Security and Privacy-Preserving Solutions in the Internet of Things (S/P-IoT) Workshop**

**A Generalized Unknown Malware Classification** ..... 793  
*Nanda Rani, Ayushi Mishra, Rahul Kumar, Sarbajit Ghosh, Sandeep K. Shukla, and Priyanka Bagade*

**Research on the Grouping Method of Side-Channel Leakage Detection** ..... 807  
*Xiaoyi Duan, Ye Huang, YongHua Su, Yujin Li, and XiaoHong Fan*

**PREFHE, PREFHE-AES and PREFHE-SGX: Secure Multiparty Computation Protocols from Fully Homomorphic Encryption and Proxy ReEncryption with AES and Intel SGX** ..... 819  
*Cavidan Yakupoglu and Kurt Rohloff*

**Author Index** ..... 839