

Cristina Alcaraz
Liqun Chen
Shujun Li
Pierangela Samarati (Eds.)

LNCS 13407

Information and Communications Security

24th International Conference, ICICS 2022
Canterbury, UK, September 5–8, 2022
Proceedings



 Springer

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>


Cristina Alcaraz · Liqun Chen · Shujun Li ·
Pierangela Samarati (Eds.)

Information and Communications Security

24th International Conference, ICICS 2022
Canterbury, UK, September 5–8, 2022
Proceedings

Editors

Cristina Alcaraz 
University of Malaga
Malaga, Spain

Shujun Li 
University of Kent
Canterbury, UK

Liqun Chen 
University of Surrey
Guildford, UK

Pierangela Samarati 
University of Milan
Milan, Italy

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-15776-9

ISBN 978-3-031-15777-6 (eBook)

<https://doi.org/10.1007/978-3-031-15777-6>

© 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

This volume contains the papers that were selected for presentation and publication at the 24th International Conference on Information and Communications Security (ICICS 2022), which was jointly organized by the University of Kent (UK), the Università degli Studi di Milano (Italy), the University of Surrey (UK), and the University of Malaga (Spain). The conference was held at the main campus of the University of Kent, Canterbury, UK, during September 5–8, 2022. Due to post-pandemic conditions and travel limitations in some countries, the conference was held as a hybrid event, offering both in-person and remote participation options for attendees.

ICICS is one of the mainstream security conferences with the longest history. It started in 1997 and aims at bringing together leading researchers and practitioners from both academia and industry to discuss and exchange their experiences, lessons learned, and insights related to computer and communication security. This year's Program Committee (PC) consisted of 114 members with diverse backgrounds and broad research interests. A total of 150 valid paper submissions were received. The review process was double blind, and the papers were evaluated on the basis of their significance, novelty, and technical quality. Practically all the papers were reviewed by four or more PC members and then discussed among the Program Committee. The discussions were held online intensively over more than three weeks. Finally, 34 papers were selected for presentation at the conference giving an acceptance rate of 22.7%.

Following the reviews, two papers were selected for the Best Paper Award and the Best Student Paper Award, respectively. Both awards were generously sponsored by Springer. The conference also selected winners of four additional awards, a Best Presentation Award, a Best Artifact Award, a Best Poster Award and a Best Demo Award, all sponsored by the Institute of Cyber Security for Society (iCSS), University of Kent. Additionally, ICICS 2022 was honored to offer three outstanding keynote talks by Ross Anderson, University of Cambridge (UK), Nicholas Carlini, Google (USA), and Guang Gong, University of Waterloo (Canada). Our deepest and sincere thanks to Ross, Nicholas, and Guang for sharing their knowledge and experience during the conference. The conference also called for posters and demo presentations of “already published/accepted work”, which were presented at a Poster/Demo session. In addition, a panel discussion was also organized at the conference.

For the success of ICICS 2022, we would like to first thank the authors of all submissions and the PC members for their great effort in selecting the papers. We also thank all the external reviewers for assisting the reviewing process. For the conference organization, we would like to thank the ICICS Steering Committee, the Publicity Chairs, Kalikinkar Mandal and Ding Wang, the Local Arrangement Co-Chairs, Budi Arief and Sanjay Bhattacharjee, the Poster/Demo Chairs, Özgür Kafalı and Vineet Rajani, the Panel Chair Zonghua Zhang, the Local Award Judging Chair Keenan Jones, the Sponsorship

Chairs, Fauzia Idrees and Clare Patterson, and the VI (Visual Identity) Designers, Yinglong He and Zhonghai Liu. Finally, we thank everyone else, speakers, session chairs, and volunteer helpers, for their contributions to the program of ICICS 2022.

September 2022

Cristina Alcaraz
Liqun Chen
Shujun Li
Pierangela Samarati

Organization

Steering Committee

Jianying Zhou	Singapore University of Technology and Design, Singapore
Robert Deng	Singapore Management University, Singapore
Dieter Gollmann	Hamburg University of Technology, Germany
Javier Lopez	University of Malaga, Spain
Qingni Shen	Peking University, China
Zhen Xu	Institute of Information Engineering, Chinese Academy of Sciences, China

General Chairs

Shujun Li	University of Kent, UK
Pierangela Samarati	Università degli Studi di Milano, Italy

Program Chairs

Cristina Alcaraz	University of Malaga, Spain
Liqun Chen	University of Surrey, UK

Local Arrangement Chairs

Budi Arief	University of Kent, UK
Sanjay Bhattacharjee	University of Kent, UK

Publicity Chairs

Kalikinkar Mandal	University of New Brunswick, Canada
Ding Wang	Nankai University, China

Poster/Demo Chairs

Özgür Kafalı	University of Kent, UK
Vineet Rajani	University of Kent, UK

Panel Chair

Zonghua Zhang

Huawei Paris Research Center, Huawei
Technologies France S.A.S.U, France

Sponsorship Chairs

Fauzia Idrees

Royal Holloway, University of London, UK

Clare Patterson

University of Kent, UK

Local Award Judging Chair

Keenan Jones

University of Kent, UK

VI (Visual Identity) Designers

Yinglong He

University of Birmingham, UK

Zhonghai Liu

Guangdong Vgreen Intelligent Home Technology
Co., Ltd., China

Program Committee

Chuadhry Mujeeb Ahmed	Singapore University of Technology and Design, Singapore
Man Ho Au	University of Hong Kong, Hong Kong
Zhongjie Ba	Zhejiang University, China
Joonsang Baek	University of Wollongong, Australia
Guangdong Bai	University of Queensland, Australia
Jia-Ju Bai	Tsinghua University, China
Diogo Barradas	University of Waterloo, Canada
Yinzhi Cao	Johns Hopkins University, USA
Guangke Chen	ShanghaiTech University, China
Rongmao Chen	National University of Defense Technology, China
Ting Chen	University of Electronic Science and Technology of China, China
Xiaofeng Chen	Xidian University, China
Xun Chen	Samsung Research America, USA
Sherman S. M. Chow	Chinese University of Hong Kong, Hong Kong
Mauro Conti	University of Padua, Italy
Nora Cuppens-Boulahia	Polytechnique Montréal, Canada
Jose Maria de Fuentes	Universidad Carlos III de Madrid, Spain
Roberto Di Pietro	Hamad Bin Khalifa University, Qatar
Wenrui Diao	Shandong University, China
Changyu Dong	Newcastle University, UK
Constantin Catalin Dragan	University of Surrey, UK
François Dupressoir	University of Bristol, UK
Afonso Ferreira	CNRS - Institut de Recherches en Informatique de Toulouse, France
Debin Gao	Singapore Management University, Singapore
Fei Gao	Beijing University of Posts and Telecommunications, China
Xing Gao	University of Delaware, USA
Joaquin Garcia-Alfaro	Institut Polytechnique de Paris, France
Amrita Ghosal	University of Limerick, Ireland
Dieter Gollmann	Hamburg University of Technology, Germany
Stefanos Gritzalis	University of Piraeus, Greece
Le Guan	University of Georgia, USA
Fuchun Guo	University of Wollongong, Australia
Shuai Hao	Old Dominion University, USA
Jiaqi Hong	Singapore Management University, Singapore
Hongxin Hu	University at Buffalo, SUNY, USA
Pengfei Hu	Shandong University, China

Jun Huang	City University of Hong Kong, Hong Kong
Xinyi Huang	Fujian Normal University, China
Jinyuan Jia	Duke University, USA
Chenglu Jin	CWI Amsterdam, The Netherlands
Sokratis Katsikas	Norwegian University of Science and Technology, Norway
Doowon Kim	University of Tennessee, USA
Hyoungshick Kim	Sungkyunkwan University, South Korea
Costas Lambrinoudakis	University of Piraeus, Greece
Wenjuan Li	Hong Kong Polytechnic University, Hong Kong
Kaitai Liang	Delft University of Technology, The Netherlands
Feng Lin	Zhejiang University, China
Jingqiang Lin	University of Science and Technology of China, China
Xiangyu Liu	Alibaba Inc., China
Zhuotao Liu	Tsinghua University, China
Javier Lopez	University of Malaga, Spain
Kangjie Lu	University of Minnesota, USA
Rongxing Lu	University of New Brunswick, Canada
Bo Luo	University of Kansas, USA
Xiapu Luo	Hong Kong Polytechnic University, Hong Kong
Haoyu Ma	Xidian University, China
Christian Mainka	Ruhr University Bochum, Germany
Daisuke Mashima	Advanced Digital Sciences Center, Singapore
Jake Massimo	Royal Holloway, University of London, UK
Weizhi Meng	Technical University of Denmark, Denmark
Jiang Ming	University of Texas at Arlington, USA
Yuhong Nan	Sun Yat-sen University, China
Siaw-Lynn Ng	Royal Holloway, University of London, UK
Jianbing Ni	Queen's University, Canada
Jianting Ning	Singapore Management University, Singapore
Liang Niu	New York University, USA
Rolf Oppliger	eSECURITY Technologies, Switzerland
Manos Panousis	University of Greenwich, UK
Günther Pernul	Universität Regensburg, Germany
Joachim Posegga	University of Passau, Germany
Elizabeth Quaglia	Royal Holloway, University of London, UK
Giovanni Russello	University of Auckland, New Zealand
Nitesh Saxena	Texas A&M University, USA
Shawn Shan	University of Chicago, USA
Vishal Sharma	Queen's University Belfast, UK
Qingni Shen	Peking University, China

Wenbo Shen	Zhejiang University, China
Purui Su	Institute of Software, Chinese Academy of Sciences, China
Hung-Min Sun	National Tsing Hua University, Taiwan
Kun Sun	George Mason University, USA
Willy Susilo	University of Wollongong, Australia
Qiang Tang	Luxembourg Institute of Science and Technology, Luxembourg
Yuzhe Tang	Syracuse University, USA
Luca Viganò	King's College London, UK
Ding Wang	Nankai University, China
Haoyu Wang	Huazhong University of Science and Technology, China
Lingyu Wang	Concordia University, Canada
Ting Wang	East China Normal University, China
Xiuhua Wang	Huazhong University of Science and Technology, China
Zhe Wang	Institute of Computing Technology, Chinese Academy of Sciences, China
Jinpeng Wei	University of North Carolina at Charlotte, USA
Weiping Wen	Peking University, China
Zhe Xia	Wuhan University of Technology, China
Dongpeng Xu	University of New Hampshire, USA
Jia Xu	NUS-Singtel Cyber Security R&D Lab, Singapore
Toshihiro Yamauchi	Okayama University, Japan
Guomin Yang	University of Wollongong, Australia
Kang Yang	State Key Laboratory of Cryptology, China
Zheng Yang	Southwest University, China
Xun Yi	RMIT University, Australia
Qilei Yin	Tsinghua University, China
Meng Yu	Roosevelt University, USA
Xingliang Yuan	Monash University, Australia
Chuan Yue	Colorado School of Mines, USA
Fan Zhang	Zhejiang University, China
Jiang Zhang	Institute of Software, Chinese Academy of Sciences, China
Kehuan Zhang	Chinese University of Hong Kong, Hong Kong
Tianwei Zhang	Amazon Web Services, USA
Yuan Zhang	Fudan University, China
Liang Zhao	Sichuan University, China
Qingchuan Zhao	City University of Hong Kong, Hong Kong
Yongjun Zhao	Nanyang Technological University, Singapore

Yunlei Zhao
Yongbin Zhou

Fudan University, China
Nanjing University of Science and Technology,
China

Additional Reviewers

Bai, Weiheng	Limniotis, Konstantinos
Biswas, Partha	Lin, Chao
Cao, Nhat Quang	Little, Rachael
Chen, Chenyang	Liu, Lin
Chen, Jinrong	Liu, Xiaoning
Chen, Tianyang	Liu, Yuejun
Lin, Chengjun	Lou, Xin
Cui, Hongrui	Lu, Xingye
Du, Minxin	Luo, Junwei
Ehsanpour, Maryam	Lv, Chunyang
Eichhammer, Philipp	Ma, Mimi
Empl, Philip	Mladenov, Vladislav
Feng, Qi	Mui, William H. Y.
Fernandez, Carmen	Muñoz, Antonio
Fouque, Pierre-Alain	Nissenbaum, Olga
Friedl, Sabrina	Nowroozi, Ehsan
Gao, Yiwen	Pakki, Aditya
Gholipour, Mahmood	Pei, Weiping
Glas, Magdalena	Pöhls, Henrich C.
Gong, Borui	Rios, Ruben
Guo, Hui	Schlette, Daniel
Guo, Xiaojie	Shen, Jun
He, Xu	Shi, Wenhao
Jia, Xiangkun	Song, Qiyang
Jiang, Anqi	Song, Shang
Jin, Renjie	Spielvogel, Korbinian
Kabir, Mohammad Ekramul	Spolaor, Riccardo
Kailun, Yan	Tao, Yang
Kelarev, Andrei	Tefek, Utku
Knittel, Lukas	Tian, Guangwei
Kumar, Gulshan	Tian, Guohua
Lai, Qiqi	Torabi, Sadegh
Lee, Moon Sung	Tricomi, Pier Paolo
Lepore, Cristian	Tsohou, Aggeliki
Li, Bingyu	Wang, Jiafan
Li, Rui	Wang, Shu
Li, Xinyu	Wang, Tianyu
Li, Yannan	Wang, Xinda
Li, Yongqiang	Wang, Yi

Wei, Jianghong
Wong, Harry W. H.
Wu, Huangting
Xiang, Binwu
Xu, Xin
Xue, Haiyang
Yan, Di
Yang, Haining
Yang, Rupeng
Yang, S. J.
Yang, Shishuai

Yang, Zhichao
Yu, Mengyang
Yu, Zuoxia
Zhang, Kai
Zhang, Yudi
Zhang, Zidong
Zhao, Zhe
Zheng, Yubo
Zhou, Yuyang
Zhu, Fei

Contents

Cryptography

BS: Blockwise Sieve Algorithm for Finding Short Vectors from Sublattices	3
<i>Jinzheng Cao, Qingfeng Cheng, Xinghua Li, and Yanbin Pan</i>	
Calibrating Learning Parity with Noise Authentication for Low-Resource Devices	19
<i>Teik Guan Tan, De Wen Soh, and Jianying Zhou</i>	
New Results of Breaking the CLS Scheme from ACM-CCS 2014	37
<i>Jing Gao, Jun Xu, Tianyu Wang, and Lei Hu</i>	
A Note on the Security Framework of Two-key DbHtS MACs	55
<i>Tingting Guo and Peng Wang</i>	
Maliciously Secure Multi-party PSI with Lower Bandwidth and Faster Computation	69
<i>Zhi Qiu, Kang Yang, Yu Yu, and Lijing Zhou</i>	
Conditional Cube Attacks on Full Members of KNOT-AEAD Family	89
<i>Siwei Chen, Zejun Xiang, Xiangyong Zeng, and Shasha Zhang</i>	
Fast Fourier Orthogonalization over NTRU Lattices	109
<i>Shuo Sun, Yongbin Zhou, Rui Zhang, Yang Tao, Zehua Qiao, and Jingdian Ming</i>	
Secure Sketch and Fuzzy Extractor with Imperfect Randomness: An Information-Theoretic Study	128
<i>Kaini Chen, Peisong Shen, Kewei Lv, and Chi Chen</i>	
Tight Analysis of Decryption Failure Probability of Kyber in Reality	148
<i>Boyue Fang, Weize Wang, and Yunlei Zhao</i>	

Authentication

Improving Deep Learning Based Password Guessing Models Using Pre-processing	163
<i>Yuxuan Wu, Ding Wang, Yunkai Zou, and Ziyi Huang</i>	

Exploring Phone-Based Authentication Vulnerabilities in Single Sign-On Systems	184
<i>Matthew M. Tolbert, Elie M. Hess, Matheus C. Nascimento, Yunsen Lei, and Craig A. Shue</i>	
FRACTAL: Single-Channel Multi-factor Transaction Authentication Through a Compromised Terminal	201
<i>Savio Sciancalepore, Simone Raponi, Daniele Caldarola, and Roberto Di Pietro</i>	
Privacy and Anonymity	
Lightweight and Practical Privacy-Preserving Image Masking in Smart Community	221
<i>Zhen Liu, Yining Liu, and Weizhi Meng</i>	
Using Blockchains for Censorship-Resistant Bootstrapping in Anonymity Networks	240
<i>Yang Han, Dawei Xu, Jiaqi Gao, and Liehuang Zhu</i>	
Repetitive, Oblivious, and Unlinkable SkNN Over Encrypted-and-Updated Data on Cloud	261
<i>Meng Li, Mingwei Zhang, Jianbo Gao, Chhagan Lal, Mauro Conti, and Mamoun Alazab</i>	
Privacy-Aware Split Learning Based Energy Theft Detection for Smart Grids	281
<i>Arwa Alromih, John A. Clark, and Prosanta Gope</i>	
Attacks and Vulnerability Analysis	
Query-Efficient Black-Box Adversarial Attack with Random Pattern Noises ...	303
<i>Makoto Yuito, Kenta Suzuki, and Kazuki Yoneyama</i>	
Autoencoder Assist: An Efficient Profiling Attack on High-Dimensional Datasets	324
<i>Qi Lei, Zijia Yang, Qin Wang, Yaoling Ding, Zhe Ma, and An Wang</i>	
TZ-IMA: Supporting Integrity Measurement for Applications with ARM TrustZone	342
<i>Liantao Song, Yan Ding, Pan Dong, Yong Guo, and Chuang Wang</i>	
FuzzBoost: Reinforcement Compiler Fuzzing	359
<i>Xiaoting Li, Xiao Liu, Lingwei Chen, Rupesh Prajapati, and Dinghao Wu</i>	

Secure Boolean Masking of Gimli: Optimization and Evaluation on the Cortex-M4	376
<i>Tzu-Hsien Chang, Yen-Ting Kuo, Jiun-Peng Chen, and Bo-Yin Yang</i>	
DeepC2: AI-Powered Covert Command and Control on OSNs	394
<i>Zhi Wang, Chaoge Liu, Xiang Cui, Jie Yin, Jiayi Liu, Di Wu, and Qixu Liu</i>	
Artificial Intelligence for Detection	
ODDITY: An Ensemble Framework Leverages Contrastive Representation Learning for Superior Anomaly Detection	417
<i>Hongyi Peng, Vinay Sachidananda, Teng Joon Lim, Rajendra Patil, Mingchang Liu, Sivaanandh Muneeswaran, and Mohan Gurusamy</i>	
Deep Learning Based Webshell Detection Coping with Long Text and Lexical Ambiguity	438
<i>Tongjian An, Xuefei Shui, and Hongkui Gao</i>	
SimCGE: Simple Contrastive Learning of Graph Embeddings for Cross-Version Binary Code Similarity Detection	458
<i>Fengliang Xia, Guixing Wu, Guochao Zhao, and Xiangyu Li</i>	
FN2: Fake News DetectioN Based on Textual and Contextual Features	472
<i>Mouna Rabhi, Spiridon Bakiras, and Roberto Di Pietro</i>	
Malware Detection with Limited Supervised Information via Contrastive Learning on API Call Sequences	492
<i>Mohan Gao, Peng Wu, and Li Pan</i>	
Semi-supervised Context Discovery for Peer-Based Anomaly Detection in Multi-layer Networks	508
<i>Bo Dong, Yuhang Wu, Micheal Yeh, Yusan Lin, Yuzhong Chen, Hao Yang, Fei Wang, Wanxin Bai, Krupa Brahmkestri, Zhang Yimin, Chinna Kummitha, and Verma Abhisar</i>	
Peekaboo: Hide and Seek with Malware Through Lightweight Multi-feature Based Lenient Hybrid Approach	525
<i>Mingchang Liu, Vinay Sachidananda, Hongyi Peng, Rajendra Patil, Sivaanandh Muneeswaran, and Mohan Gurusamy</i>	
TapTree: Process-Tree Based Host Behavior Modeling and Threat Detection Framework via Sequential Pattern Mining	546
<i>Mohammad Mamun and Scott Buffett</i>	

Network Security and Forensics

Dependency-Based Link Prediction for Learning Microsegmentation Policy 569
Steven Noel and Vipin Swarup

Chuchotage: In-line Software Network Protocol Translation for (D)TLS 589
Pegah Nikbakht Bideh and Nicolae Paladi

Study on the Effect of Face Masks on Forensic Speaker Recognition 608
Georgiana Bogdanel, Nadia Belghazi-Mohamed, Hilario Gómez-Moreno, and Sergio Lafuente-Arroyo

Video Forensics for Object Removal Based on Darknet3D 622
Kejun Zhang, Yuhao Wang, and Xinying Yu

Author Index 639