

Debin Gao  
Qi Li  
Xiaohong Guan  
Xiaofeng Liao (Eds.)

LNCS 12919

# Information and Communications Security

23rd International Conference, ICICS 2021  
Chongqing, China, November 19–21, 2021  
Proceedings, Part II

2  
Part II

ICICS

 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*

Gerhard Woeginger 

*RWTH Aachen, Aachen, Germany*

Moti Yung

*Columbia University, New York, NY, USA*

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

Debin Gao · Qi Li · Xiaohong Guan ·  
Xiaofeng Liao (Eds.)

# Information and Communications Security


23rd International Conference, ICICS 2021  
Chongqing, China, November 19–21, 2021  
Proceedings, Part II

*Editors*

Debin Gao   
Singapore Management University  
Singapore, Singapore

Xiaohong Guan  
Xi'an Jiaotong University  
Xi'an, China

Qi Li   
Tsinghua University  
Beijing, China

Xiaofeng Liao   
Chongqing University  
Chongqing, China

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-88051-4              ISBN 978-3-030-88052-1 (eBook)  
<https://doi.org/10.1007/978-3-030-88052-1>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 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

This volume contains papers that were selected for presentation and publication at the 23rd International Conference on Information and Communications Security (ICICS 2021), which was jointly organized by Chongqing University, Xi'an Jiaotong University, and Peking University in China during November 19–21, 2021. 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 141 members with diverse backgrounds and broad research interests. A total of 202 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. Most papers were reviewed by four or more PC members. The PC meeting was held online with intensive discussion over more than two weeks. Finally, 49 papers were selected for presentation at the conference giving an acceptance rate of 24%.

A "Best Paper Selection Committee" with five PC members of diverse backgrounds from around the world was formed, which selected the two best papers after a lengthy discussion. The paper "Rethinking Adversarial Examples Exploiting Frequency-Based Analysis" authored by Sicong Han, Chenhao Lin, Chao Shen, and Qian Wang received the Best Paper Award, while the paper "CyberRel: Joint Entity and Relation Extraction for Cybersecurity Concepts" authored by Yongyan Guo, Zhengyu Liu, Cheng Huang, Jiayong Liu, Wangyuan Jing, Ziwang Wang, and Yanghao Wang received the Best Student Paper Award. Both awards were generously sponsored by Springer.

ICICS 2021 was honored to offer two outstanding keynote talks: "Engineering Trustworthy Data-Centric Software: Intelligent Software Engineering and Beyond" by Tao Xie and "Securing Smart Cars – Opportunities and Challenges" by Long Lu. Our deepest gratitude to Tao and Long for sharing their insights during the conference.

For the success of ICICS 2021, 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 general chairs, Xiaohong Guan and Xiaofeng Liao, the publicity chairs, Qingni Shen, Qiang Tang, and Yang Zhang, and the publication chair, Dongmei Liu. Special thanks to Tao Xiang for the local arrangements. Finally, we thank everyone else, speakers, session chairs, and volunteer helpers for their contributions to the program of ICICS 2021.

Last but not least, we wish to extend a huge thank you to healthcare frontliners and our colleagues in the research of vaccine and immunization in fighting COVID-19. ICICS 2021 could not have become one of the first mainstream security conferences returning to an in-person setting without their enormous contribution.

# Organization

## Steering Committee

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, CAS, China
Jiaying Zhou	Singapore University of Technology and Design, Singapore

## General Chairs

Xiaohong Guan	Xi'an Jiaotong University, China
Xiaofeng Liao	Chongqing University, China

## Program Committee Chairs

Debin Gao	Singapore Management University, Singapore
Qi Li	Tsinghua University, China

## Program Committee

Chuahdhy M. Ahmed	University of Strathclyde, UK
Cristina Alcaraz	University of Malaga, Spain
Man Ho Au	The University of Hong Kong, Hong Kong, China
Zhongjie Ba	Zhejiang University, China
Joonsang Baek	University of Wollongong, Australia
Guangdong Bai	The University of Queensland, Australia
Jia-Ju Bai	Tsinghua University, China
Diogo Barradas	Universidade de Lisboa, Portugal
Yinzhi Cao	Johns Hopkins University, USA
Guangke Chen	ShanghaiTech University, China
Rongmao Chen	National University of Defense Technology, China
Songqing Chen	George Mason University, USA
Ting Chen	University of Electronic Science and Technology of China, China
Xiaofeng Chen	Xidian University, China
Xun Chen	Samsung Research America, USA
Yaohui Chen	Facebook, USA
Sherman S. M. Chow	The Chinese University of Hong Kong, Hong Kong, China

Mauro Conti	University of Padua, Italy
Wenrui Diao	Shandong University, China
Jintai Ding	Tsinghua University, China
Xuhua Ding	Singapore Management University, Singapore
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Ruian Duan	Palo Alto Networks Inc, USA
Xinwen Fu	University of Massachusetts Lowell, USA
Zhangjie Fu	Nanjing University of Information Science and Technology, China
Jose Maria de Fuentes	Universidad Carlos III de Madrid, Spain
Fei Gao	Beijing University of Posts and Telecommunications, China
Xing Gao	University of Delaware, USA
Joaquin Garcia-Alfaro	Institut Polytechnique de Paris, France
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	Massachusetts Institute of Technology, USA
Xinyi Huang	Fujian Normal University, China
Shouling Ji	Zhejiang University, China
Jinyuan Jia	Duke University, USA
Chenglu Jin	CWI Amsterdam, The Netherlands
Georgios Kambourakis	University of the Aegean, Greece
Sokratis Katsikas	Norwegian University of Science and Technology, Norway
Dongseong Kim	The University of Queensland, Australia
Doowon Kim	University of Tennessee, Knoxville, USA
Hyoungshick Kim	Sungkyunkwan University, South Korea
Shujun Li	University of Kent, UK
Wenjuan Li	The Hong Kong Polytechnic University, Hong Kong, China
Feng Lin	Zhejiang University, China
Jingqiang Lin	University of Science and Technology of China, China
Yan Lin	Singapore Management University, Singapore
Jian Liu	Zhejiang University, China
Tongping Liu	University of Massachusetts Amherst, USA
Xiangyu Liu	Alibaba Inc., China
Zhuotao Liu	Tsinghua University, China
Giovanni Livraga	University of Milan, Italy
Javier Lopez	UMA, Spain
Jian Lou	Emory University, USA



Kangjie Lu	University of Minnesota, USA
Bo Luo	The University of Kansas, USA
Xiapu Luo	The Hong Kong Polytechnic University, Hong Kong, China
Haoyu Ma	Xidian University, China
Christian Mainka	Ruhr University Bochum, Germany
Daisuke Mashima	Advanced Digital Sciences Center, Singapore
Jake Massimo	Amazon Web Services, USA
Weizhi Meng	Technical University of Denmark, Denmark
Jiang Ming	UTA, USA
Chris Mitchell	Royal Holloway, University of London, UK
Yuhong Nan	Purdue University, USA
Jianbing Ni	Queen's University, Canada
Jianting Ning	Singapore Management University, Singapore
Liang Niu	New York University, USA
Satoshi Obana	Hosei University, Japan
Rolf Oppliger	eSECURITY Technologies, Switzerland
Roberto Di Pietro	Hamad Bin Khalifa University, Qatar
Joachim Posegga	University of Passau, Germany
Giovanni Russello	The 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	CAS, China
Hung-Min Sun	National Tsing Hua University, Taiwan, China
Kun Sun	George Mason University, USA
Willy Susilo	University of Wollongong, Australia
Qiang Tang	Luxembourg Institute of Science and Technology, Luxemburg
Yuzhe Tang	Syracuse University, USA
Luca Viganò	King's College London, UK
Binghui Wang	Duke University, USA
Cong Wang	City University of Hong Kong, Hong Kong, China
Ding Wang	Nankai University, China
Gang Wang	University of Illinois at Urbana-Champaign, USA
Haining Wang	Virginia Tech, USA
Haoyu Wang	Beijing University of Posts and Telecommunications, China
Lei Wang	Shanghai Jiao Tong University, China
Lingyu Wang	Concordia University, Canada
Shuai Wang	The Hong Kong University of Science and Technology, Hong Kong, China
Ting Wang	East China Normal University, China

Xiuhua Wang	Huazhong University of Science and Technology, China
Zhe Wang	ICT, China
Jinpeng Wei	University of North Carolina at Charlotte, USA
Weiping Wen	Peking University, China
Daoyuan Wu	The Chinese University of Hong Kong, Hong Kong, China
Zhe Xia	Wuhan University of Technology, China
Xiaofei Xie	Nanyang Technological University, Singapore
Dongpeng Xu	University of New Hampshire, USA
Jia Xu	NUS-Singtel Cyber Security R&D Lab, Singapore
Jun Xu	Stevens Institute of Technology, USA
Minhui Xue	The University of Adelaide, Australia
Toshihiro Yamauchi	Okayama University, Japan
Feng Yan	University of Nevada, Reno, USA
Qiben Yan	Michigan State University, USA
Guomin Yang	University of Wollongong, Australia
Zheng Yang	Southwest University, China
Roland Yap	National University of Singapore, Singapore
Xun Yi	RMIT University, Australia
Qilei Yin	Tsinghua University, China
Meng Yu	Roosevelt University, USA
Yu Yu	Shanghai Jiao Tong University, China
Xingliang Yuan	Monash University, Australia
Chuan Yue	Colorado School of Mines, USA
Tsz Hon Yuen	The University of Hong Kong, Hong Kong, China
Chao Zhang	Tsinghua University, China
Fan Zhang	Zhejiang University, China
Fengwei Zhang	SUSTech, China
Jialong Zhang	ByteDance, China
Jiang Zhang	State Key Laboratory of Cryptology, China
Kehuan Zhang	The Chinese University of Hong Kong, Hong Kong, China
Yang Zhang	CISPA Helmholtz Center for Information Security, Germany
Yinqian Zhang	Southern University of Science and Technology, China
Lei Zhao	Computer School of Wuhan University, China
Qingchuan Zhao	Ohio State University, USA
Tianwei Zhang	Nanyang Technological University, Singapore
Yuan Zhang	Fudan University, China
Yongjun Zhao	Nanyang Technological University, Singapore
Yunlei Zhao	Fudan University, China
Yajin Zhou	Zhejiang University, China
Yongbin Zhou	Chinese Academy of Sciences, China
Shuofei Zhu	Pennsylvania State University, USA

## Additional Reviewers

Isaac Agudo  
Md Rabbi Alam  
Cristina Alcaraz  
Ahsan Ali  
Saed Alsayigh  
Enkeleda Bardhi  
Christof Beierle  
Christian Berger  
Alessandro Brighente  
Cailing Cai  
Giovanni Calore  
Xinle Cao  
Kwan Yin Chan  
Jinrong Chen  
Long Chen  
Min Chen  
Tianyang Chen  
Tommy Chin  
Murilo Coutinho  
Andrei Cozma  
Handong Cui  
Vasiliki Diamantopoulou  
Qiyang Dong  
Minxin Du  
Orr Dunkelman  
Alexandros Fakis  
Pengbin Feng  
Ankit Gangwal  
Yiwen Gao  
Nicholas Genise  
Junqing Gong  
Qingyuan Gong  
Kamil D. Gur  
Yonglin Hao  
Ke He  
Xu He  
Jiaqi Hong  
Xinyue Hu  
Yupu Hu  
Mengdie Huang  
Huiwen Jia  
Xiangkun Jia  
Ziming Jiang  
Georgios Karopoulos  
Maria Karyda  
Andrei Kelarev  
Minjune Kim  
Felix Klement  
Vasileios Kouliaridis  
Gulshan Kumar  
Jianchang Lai  
Qiqi Lai  
Chhagan Lal  
Gregor Leander  
Bo Li  
Huizhong Li  
Shaofeng Li  
Wanpeng Li  
Yannan Li  
Zheng Li  
Ziyuan Liang  
Kyungchan Lim  
Chaoge Liu  
Gang Liu  
Songsong Liu  
Xiaoning Liu  
Xueqiao Liu  
Yichen Liu  
Yiyong Liu  
Yuejun Liu  
Yunpeng Liu  
Zengrui Liu  
Eleonora Losiouk  
Xin Lou  
Junwei Luo  
Lan Luo  
Xiaolong Ma  
Zhou Ma  
Ahmed Tanvir Mahdad  
Fei Meng  
Vladislav Mladenov  
William H. Y. Mui  
Lucien K. L. Ng  
Shimin Pan  
Dimitris Papamartzivanos  
Bryan Pearson

Henrich C. Pöhls  
Hunter Price  
Xianrui Qin  
Yue Qin  
Tingting Rao  
Pengcheng Ren  
Yujie Ren  
Ruben Rios  
Shalini Saini  
Md Sajidul Islam Sajid  
Stewart Santanoe  
Shiqi Shen  
Siyu Shen  
Menghan Sun  
Shuo Sun  
Azadeh Tabiban  
Fei Tang  
Jiaxun Steven Tang  
Utku Tefek  
Guangwei Tian  
Guohua Tian  
Zhihua Tian  
Yosuke Todo  
Zisis Tsiatsikas  
Payton Walker  
Hongbing Wang  
Jiafan Wang  
Jianfeng Wang  
Kailong Wang  
Lihchung Wang  
Lu Wang  
Shu Wang  
Ti Wang  
Ting Wang  
Wenhao Wang  
Xinda Wang  
Xinying Wang  
Yunling Wang  
Rui Wen  
Mingli Wu  
Yi Xie  
Guorui Xu  
Jing Xu  
Shengmin Xu  
Bolin Yang  
Fan Yang  
Hanmei Yang  
Shishuai Yang  
Wenjie Yang  
Xu Yang  
Zhichao Yang  
Amirhesam Yazdi  
Quanqi Ye  
Jun Yi  
Xiao Yi  
Qilei Yin  
Pinghai Yuan  
Syed Zawad  
Zhe Zhao  
Zhiyu Zhao  
Ziming Zhao  
Chennan Zhang  
Yuexin Zhang  
Yubo Zheng  
Ce Zhou  
Jin Zhou  
Rahman Ziaur  
Max Zinkus  
Yang Zou  
Yunkai Zou

## Sponsors

### Gold Sponsor



### Silver Sponsors



# **Keynotes**

# Engineering Trustworthy Data-Centric Software: Intelligent Software Engineering and Beyond

Tao Xie

Peking University

**Abstract.** As an example of exploiting the synergy between AI and software engineering, the field of intelligent software engineering has emerged with various advances in recent years. Such field broadly addresses issues on intelligent [software engineering] and [intelligence software] engineering. The former, intelligent [software engineering], focuses on instilling intelligence in approaches developed to address various software engineering tasks to accomplish high effectiveness and efficiency. The latter, [intelligence software] engineering, focuses on addressing various software engineering tasks for intelligence software, e.g., AI software. However, engineering trustworthy data-centric software (which AI software components are part of) requires research contributions from compiler, programming languages, formal verification, security, and software engineering besides systems and hardware. This talk will discuss recent research and future directions in the field of intelligent software engineering along with the broad scope of engineering trustworthy data-centric software.

# Securing Smart Cars – Opportunities and Challenges

Long Lu

NIO

**Abstract.** As cars become more intelligent and connected, the security of on-car systems, software, and data has caught heavy attention from academia, industry, and regulators. This talk will discuss the key technical aspects of smart car security, including low-level system security, secure and robust autonomous driving, V2X security, data security, etc., highlighting the research and technical opportunities and challenges.



## Contents – Part II

### Machine Learning Security

Exposing DeepFakes via Localizing the Manipulated Artifacts . . . . .	3
<i>Wenxin Li, Qi Wang, Run Wang, Lei Zhao, and Lina Wang</i>	
Improved Differential-ML Distinguisher: Machine Learning Based Generic Extension for Differential Analysis . . . . .	21
<i>Gao Wang and Gaoli Wang</i>	
Black-Box Buster: A Robust Zero-Shot Transfer-Based Adversarial Attack Method . . . . .	39
<i>Yuxuan Zhang, Zhaoyang Wang, Boyang Zhang, Yu Wen, and Dan Meng</i>	
A Lightweight Metric Defence Strategy for Graph Neural Networks Against Poisoning Attacks . . . . .	55
<i>Yang Xiao, Jie Li, and Wengui Su</i>	
Rethinking Adversarial Examples Exploiting Frequency-Based Analysis . . . .	73
<i>Sicong Han, Chenhao Lin, Chao Shen, and Qian Wang</i>	

### Multimedia Security

Compressive Sensing Image Steganography via Directional Lifting Wavelet Transform . . . . .	93
<i>Zan Chen, Chaocheng Ma, Yuanjing Feng, and Xingsong Hou</i>	
Remote Recovery of Sound from Speckle Pattern Video Based on Convolutional LSTM . . . . .	110
<i>Dali Zhu, Long Yang, and Hualin Zeng</i>	
Secure Image Coding Based on Compressive Sensing with Optimized Rate-Distortion . . . . .	125
<i>Di Xiao and Shuwen Lan</i>	
Black-Box Audio Adversarial Example Generation Using Variational Autoencoder. . . . .	142
<i>Wei Zong, Yang-Wai Chow, and Willy Susilo</i>	

## Security Analysis

Security Analysis of Even-Mansour Structure Hash Functions. . . . .	163
<i>Shiwei Chen, Ting Cui, and Chenhui Jin</i>	
Rare Variants Analysis in Genetic Association Studies with Privacy Protection via Hybrid System . . . . .	174
<i>Mohammed Shujaa Aldeen and Chuan Zhao</i>	
Rotational-Linear Attack: A New Framework of Cryptanalysis on ARX Ciphers with Applications to Chaskey . . . . .	192
<i>Yaqi Xu, Baofeng Wu, and Dongdai Lin</i>	
A Novel Approach for Supervisor Synthesis to Enforce Opacity of Discrete Event Systems . . . . .	210
<i>Nour Elhouda Souid and Kais Klai</i>	

## Post-quantum Cryptography

Lattice-Based Secret Handshakes with Reusable Credentials . . . . .	231
<i>Zhiyuan An, Zhuoran Zhang, Yamin Wen, and Fangguo Zhang</i>	
When NTT Meets Karatsuba: Preprocess-then-NTT Technique Revisited . . . .	249
<i>Yiming Zhu, Zhen Liu, and Yanbin Pan</i>	
Predicting the Concrete Security of LWE Against the Dual Attack Using Binary Search. . . . .	265
<i>Shuaigang Li, Xianhui Lu, Jiang Zhang, Bao Li, and Lei Bi</i>	
Small Leaks Sink a Great Ship: An Evaluation of Key Reuse Resilience of PQC Third Round Finalist NTRU-HRSS . . . . .	283
<i>Xiaohan Zhang, Chi Cheng, and Ruoyu Ding</i>	
Efficient and Fully Secure Lattice-Based IBE with Equality Test. . . . .	301
<i>Zhenghao Wu, Jian Weng, Anjia Yang, Lisha Yao, Xiaojian Liang, Zike Jiang, and Jinghang Wen</i>	

## Applied Cryptography

Forward-Secure Revocable Identity-Based Encryption . . . . .	321
<i>Baodong Qin, Xue Bai, Dong Zheng, Hui Cui, and Yiyuan Luo</i>	
An Optimized Inner Product Argument with More Application Scenarios. . . .	341
<i>Zongyang Zhang, Zibo Zhou, Weihai Li, and Hongyu Tao</i>	
Updatable All-But-One Dual Projective Hashing and Its Applications . . . . .	358
<i>Kai Zhang, Zhe Jiang, Junqing Gong, and Haifeng Qian</i>	

On Tightly-Secure (Linkable) Ring Signatures ..... 375  
*Guofeng Tang*

More Efficient Construction of Anonymous Signatures ..... 394  
*Yunfeng Ji, Yang Tao, and Rui Zhang*

**Author Index** ..... 413