

Editorial Board Members

Joaquim Filipe 

Polytechnic Institute of Setúbal, Setúbal, Portugal

Ashish Ghosh

Indian Statistical Institute, Kolkata, India

Raquel Oliveira Prates 

Federal University of Minas Gerais (UFMG), Belo Horizonte, Brazil

Lizhu Zhou

Tsinghua University, Beijing, China

More information about this series at <https://link.springer.com/bookseries/7899>

Chunjie Cao · Yuqing Zhang · Yuan Hong ·
Ding Wang (Eds.)

Frontiers in Cyber Security

4th International Conference, FCS 2021
Haikou, China, December 17–19, 2021
Revised Selected Papers

Editors

Chunjie Cao
Hainan University
Haikou, China

Yuan Hong 
Illinois Institute of Technology
Chicago, IL, USA

Yuqing Zhang
National Computer Network Intrusion
Protection Center (NCNIPC)
Beijing, China

Ding Wang
Nankai University
Tianjin, China

ISSN 1865-0929 ISSN 1865-0937 (electronic)
Communications in Computer and Information Science
ISBN 978-981-19-0522-3 ISBN 978-981-19-0523-0 (eBook)
<https://doi.org/10.1007/978-981-19-0523-0>

© Springer Nature Singapore Pte Ltd. 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 Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

This volume contains the papers from the 4th International Conference on Frontiers in Cyber Security (FCS 2021). The event was organized by School of Cyberspace Security (School of Cryptology), Hainan University. This series, which started in 2018, brings together individuals involved in multiple disciplines of cyber security in order to foster exchange of ideas.

In recent years, cyber security threats have increased rapidly. All kinds of extremely dangerous attack behaviors expose every common user to risks including privacy leakage, property loss, etc. Cyber security has also received increasing attention from researchers. The development of cyber security requires extensive communication. In view of this situation, and the permanent theme of FCS being “Cyber Security”, aiming to introduce security concepts and technology achievements from the international forefront in the field of information security, and to share insights into the latest development trends and innovative technology of cyber security, the FCS conference provides a good platform for researchers and practitioners to exchange the latest research achievements and discuss these questions of network security, system security, cryptography, trust management, privacy protection, information hiding, computer forensics, content security, and their applications, etc. keeping the pace with international security innovation concepts to provide theoretical and technical support for international cyber space development.

The FCS conference has been held four times, starting at the University of Electronic Science and Technology of China in 2018. In these four years, hundreds of researchers have exchanged ideas with each other at the FCS events, which has promoted the development of cyber security. In 2021, FCS was held in Haikou, China, and organized by Hainan University which is one of the most important research institutes in China. FCS 2021 received 58 papers and accepted 22 papers, including two short papers. Reviewers were assigned an average of 4.3 papers and the average number of reviews per paper was 2.7. A double-blind peer review process was employed to promote transparency.

The conference received great attention from all over the world, with participants from countries such as China, Japan, the Netherlands, Denmark, the USA, etc. Taking place during the COVID-19 pandemic, the conference needed to comply with the relevant prevention regulations. For the health of the participants, some overseas participants needed to participate in the conference online, which was a big challenge.

According to the accepted papers, the five topics of FCS 2021 classified by reviewers were as follows: cryptography, intelligent security, system security, network security, and multimedia security.

The proceedings editors wish to thank the dedicated Program Committee members and all the other reviewers for their contributions. We also thank Springer for their trust and for publishing the proceedings of FCS 2021.

September 2021

Chunjie Cao
Yuqing Zhang
Yuan Hong
Ding Wang

Organization

Steering Committee

| | |
|-----------------|---|
| Baocang Wang | Xidian University, China |
| Chunhua Su | University of Aizu, Japan |
| Fagen Li | University of Electronic Science and Technology of China, China |
| Guangquan Xu | Tianjin University, China |
| Kai Chen | Institute of Information Engineering, CAS, China |
| Kaitai Liang | Delft University of Technology, Netherlands |
| Mingwu Zhang | Hubei University of Technology, China |
| Robert H. Deng | Singapore Management University, Singapore |
| Tsuyoshi Takagi | University of Tokyo, Japan |
| Weizhi Meng | Technical University of Denmark, Denmark |
| Xiaojiang Du | Temple University, USA |

General Chairs

| | |
|---------------|---|
| Chunming Rong | University of Stavanger, Norway |
| Chunjie Cao | Hainan University, China |
| Yuqing Zhang | National Computer Network Intrusion Protection Center (NCNIPC), China |

Program Committee Chairs

| | |
|-----------|---------------------------------------|
| Yuan Hong | Illinois Institute of Technology, USA |
| Ding Wang | Nankai University, China |

Program Committee

| | |
|---------------|--|
| Si Chen | West Chester University, USA |
| Debasis Giri | Haldia Institute of Technology, India |
| Song Han | Zhejiang Gongshang University, China |
| Tao Li | Nankai University, China |
| Guozhu Meng | Institute of Information Engineering, CAS, China |
| Shanchen Pang | Tiangong University, China |
| Meng Shen | Beijing Institute of Technology, China |
| Ding Wang | Nankai University, China |
| Xiaofei Xie | Nanyang Technological University, Singapore |

| | |
|--------------------|--|
| Qiuling Yue | Hainan University, China |
| Debiao He | Wuhan University, China |
| Bok-Min Goi | University Tunku Abdul Rahman (UTAR), Malaysia |
| Fagen Li | University of Electronic Science and Technology of China, China |
| Jingqiang Lin | Institute of Information Engineering, CAS, China |
| Weizhi Meng | Technical University of Denmark, Denmark |
| Hao Peng | Zhejiang Normal University, China |
| Gautam Srivastava | Brandon University, Canada |
| Wei Wang | Beijing Jiaotong University, China |
| Hongyu Yang | Civil Aviation University of China, China |
| Fangguo Zhang | Sun Yat-sen University, China |
| Shaojing Fu | National University of Defense Technology, China |
| Guangquan Xu | Tianjin University, China |
| Jianxin Li | Beihang University, China |
| Wojciech Mazurczyk | Warsaw University of Technology, Poland |
| Wei Ou | Hainan University, China |
| Honggang Qi | University of Chinese Academy of Sciences, China |
| Baocang Wang | Xidian University, China |
| Zhijun Wu | Civil Aviation University of China, China |
| Jun Ye | Hainan University, China |
| Mingwu Zhang | Hubei University of Technology, China |
| Chao Zhang | Tsinghua University, China |
| Anmin Fu | Nanjing University of Science and Technology, China |
| Hong Lei | Hainan University, China |
| Jianhui Lv | Tsinghua University, China |
| Wenyuan Wu | Chongqing Institute of Green and Intelligent Technology, CAS, China |
| David Glance | University of Western Australia, Australia |
| Ali Yavari | Swinburne University of Technology, Australia |
| Wuping Xie | Jiangxi Normal University, China |
| Yu Wei | Purdue University, USA |
| Guixin Ye | Northwestern University, USA |
| Zhenzhuo Hou | Peking University, China |
| Qiyang Dong | Nankai University, China |
| Hao Wang | Shandong Normal University, China |
| Haoyu Ma | Xidian University, China |
| Jianfeng Wang | Xidian University, China |

| | |
|-------------------------------|--|
| Saru Kumari | Chaudhary Charan Singh University, India |
| Yunkai Zou | Nankai University, China |
| Xavier de Carné de Carnavalet | Hong Kong Polytechnic University, China |

Publicity Chairs

| | |
|-------------|---|
| Hao Peng | Zhejiang Normal University, China |
| Hongyu Yang | Civil Aviation University of China, China |
| Weizhi Meng | Technical University of Denmark, Denmark |
| Yong Ding | Pengcheng Lab, China |
| Yuanyuan Ma | Qingdao Agricultural University, China |

Organization Committee Chairs

| | |
|-------------|--------------------------|
| Xiaoyi Zhou | Hainan University, China |
| Dian Zhang | Hainan University, China |
| Zifeng Xu | Hainan University, China |
| Qiuling Yue | Hainan University, China |
| Xiaoli Qin | Hainan University, China |

Organization Committee

| | |
|----------------|--------------------------|
| Longjuan Wang | Hainan University, China |
| Xuefeng Fan | Hainan University, China |
| Lu Zhang | Hainan University, China |
| Tianshuo Zhang | Hainan University, China |
| Bingbing Zhu | Hainan University, China |

Contents

Intelligent Security

| | |
|--|----|
| DACN: Malware Classification Based on Dynamic Analysis and Capsule Networks | 3 |
| <i>Binghui Zou, Chunjie Cao, Longjuan Wang, and Fangjian Tao</i> | |
| Research on Automatic Analysis and Exploitation Technology of Remote Code Execution Vulnerability for Grid System | 14 |
| <i>Hongwen Wu, Xiaoming Wang, Ke Zhou, Jianming Zou, Congyun Wu, Wenjian Wen, Zhicheng Huang, Jiezhen Deng, and Tingyu Qiu</i> | |
| GWDGA: An Effective Adversarial DGA | 30 |
| <i>Xiang Shu, Chunjie Cao, Longjuan Wang, and Fangjian Tao</i> | |
| Imperceptible and Reliable Adversarial Attack | 49 |
| <i>Jiawei Zhang, Jinwei Wang, Xiangyang Luo, Bin Ma, and Naixue Xiong</i> | |
| Architecture and Security Analysis of Federated Learning-Based Automatic Modulation Classification | 63 |
| <i>Xianglin Wei, Chao Wang, Xiang Jiao, Qiang Duan, and Yongyang Hu</i> | |
| Detecting Inconsistent Vulnerable Software Version in Security Vulnerability Reports | 78 |
| <i>Hansong Ren, Xuejun Li, Liao Lei, Guoliang Ou, Hongyu Sun, Gaofei Wu, Xiao Tian, Jinglu Hu, and Yuqing Zhang</i> | |

System Security

| | |
|--|-----|
| Multi-modal Universal Embedding Representations for Language Understanding | 103 |
| <i>Xi Luo, Chunjie Cao, and Longjuan Wang</i> | |
| New Federation Algorithm Based on End-Edge-Cloud Architecture for Smart Grid | 120 |
| <i>Xin Ji, Haifeng Zhang, Juan Chu, Linxiao Dong, and Chengyue Yang</i> | |
| Certificateless Authentication and Consensus for the Blockchain-Based Smart Grid | 134 |
| <i>Egide Nkurunziza, Gervais Mwitende, Lawrence Tandoh, and Fagen Li</i> | |

| | |
|---|-----|
| Information System Security Risk Assessment Based on Entropy Weight Method - Bayesian Network | 152 |
| <i>Xinjian Lv, Nan Shi, Jing Wei, Yuan Tian, Jie Li, and Jian Li</i> | |
| Survey of 3D Printer Security Offensive and Defensive | 163 |
| <i>Jiayuan Zhang, Mengyue Feng, Yuhang Huang, Tao Feng, Wenjie Wang, He Wang, and Han Zhang</i> | |
| Network Security | |
| Requirements for Total Resistance to Pollution Attacks in HMAC-Based Authentication Schemes for Network Coding | 181 |
| <i>Lawrence Tandoh, Fagen Li, Ikram Ali, Charles Roland Haruna, Michael Y. Kpiebaareh, and Christopher Tandoh</i> | |
| Network Security Situation Assessment Method Based on MHSA-FL Model | 197 |
| <i>Kejun Zhang, Xinrui Jiang, Xinying Yu, and Liwen Feng</i> | |
| A Hybrid Network Intrusion Detection Model Based on CNN-LSTM and Attention Mechanism | 214 |
| <i>Jieru Mu, Hua He, Lin Li, Shanchen Pang, and Cong Liu</i> | |
| System Security Analysis of Different Link Proportions Between Nodes in the Cyber-Physical System Against Target Attack | 230 |
| <i>Hao Peng, Zhen Qian, Ming Zhong, Dandan Zhao, Guangquan Xu, Songyang Wu, and Jianming Han</i> | |
| Multimedia Security | |
| A GDIoU Loss Function-Based YOLOv4 Deep Learning Network for High-Performance Insulator Location in Field Images | 245 |
| <i>Bin Ma, Yongkang Fu, Jian Li, Chunpeng Wang, and Yuli Wang</i> | |
| Identification of Synthetic Spoofed Speech with Deep Capsule Network | 257 |
| <i>Terui Mao, Diqun Yan, Yongkang Gong, and Randing Wang</i> | |
| Privacy, Risk and Trust | |
| Cloud-Aided Scalable Revocable Identity-Based Encryption with Ciphertext Update from Lattices | 269 |
| <i>Yanhua Zhang, Ximeng Liu, Yupu Hu, and Huiwen Jia</i> | |

| | |
|--|-----|
| A Privacy-Preserving Medical Image Scheme Based on Secret Sharing and Reversible Data Hiding | 288 |
| <i>Ming Cheng, Yang Yang, Yingqiu Ding, and Weiming Zhang</i> | |
| Correlation Power Analysis and Protected Implementation on Block Cipher RainDrop | 308 |
| <i>Zhixuan Gao, Shuang Wang, Yaoling Ding, An Wang, and Qingjun Yuan</i> | |
| Data and Application Security | |
| Research on Security Assessment of Cross Border Data Flow | 327 |
| <i>Wang Na, Wu Gao, Yue Qiuling, Hu Jinglu, and Yuqing Zhang</i> | |
| A Review of Data Representation Methods for Vulnerability Mining Using Deep Learning | 342 |
| <i>Ying Li, Mianxue Gu, Hongyu Sun, Yuhao Lin, Qiuling Yue, Zhen Guo, Jinglu Hu, He Wang, and Yuqing Zhang</i> | |
| Author Index | 353 |