

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>

Jieren Cheng · Xiangyan Tang ·
Xiaozhang Liu (Eds.)

Cyberspace Safety and Security

12th International Symposium, CSS 2020
Haikou, China, December 1–3, 2020
Proceedings

Editors

Jieren Cheng
Hainan University
Haikou, China

Xiangyan Tang
Hainan University
Haikou, China

Xiaozhang Liu
Hainan University
Haikou, China

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-73670-5

ISBN 978-3-030-73671-2 (eBook)

<https://doi.org/10.1007/978-3-030-73671-2>

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

The 12th International Symposium on Cyberspace Safety and Security (CSS 2020) is the latest edition in a series of highly successful international events on cyberspace safety and security previously held as CSS 2019 (Guangzhou, China), CSS 2018 (Amalfi, Italy), CSS 2017 (Xi'an, China), CSS 2016 (Granada, Spain), CSS 2015 (New York, USA), CSS 2014 (Paris, France), CSS 2013 (Zhangjiajie, China), CSS 2012 (Melbourne, Australia), CSS 2012 (Milan, Italy), CSS 2009 (Chengdu, China), and CSS 2008 (Sydney, Australia).

The CSS Symposium aims to provide a leading-edge forum to foster interaction between researchers and developers within the cyberspace safety and security communities, and to give attendees an opportunity to network with experts in this field. It focuses on all areas of cyberspace safety and security, such as authentication, access control, availability, integrity, privacy, confidentiality, dependability, and sustainability. CSS 2020 was held in Haikou, China, during December 1–3, 2020, and organized by Hainan University, China. CSS 2020 attracted 82 high-quality research papers of which 27 were accepted, an acceptance rate of 33%.

The success of CSS 2020 is the result of the behind-the-scenes efforts of selfless individuals and organizations. We would like to thank all the authors. We are also very grateful for the support of the Program Committee members and reviewers, as well as the symposium chairs, without whose hard work the success of CSS 2020 would not have been possible.

Finally, we would like to thank all the contributors and all the conference attendees, the great team at Springer who helped produce the minutes, and the developers and maintainers of EasyChair.

December 2020

Jieren Cheng
Xiangyan Tang
Xiaozhang Liu

Organization

Honorary General Chair

Jieren Cheng Hainan University, China

General Co-chairs

Chunjie Cao Hainan University, China
Jin Li Guangzhou University, China

Program Co-chairs

Xu Yuan University of Louisiana at Lafayette, USA
Qinghua Zheng Xi'an Jiaotong University, China

Publication Chairs

Chunyang Ye Hainan University, China
Xiaoyi Zhou Hainan University, China
Xiaozhang Liu Hainan University, China

Publicity Co-chairs

Nan Jiang East China Jiaotong University, China
Yucong Duan Hainan University, China
Chunyuan Zhang Hainan University, China
Zhao Qiu Hainan University, China

Track Co-chairs

Xiangyan Tang Hainan University, China
Qi Qi Hainan University, China
Jun Ye Hainan University, China
Jianqiang Ma Hainan University, China
Yu Zhang Hainan University, China
Chaosheng Tang Hainan University, China

Steering Committee Chair

Yang Xiang Swinburne University of Technology, Australia

Program Committee

Chao Chen	James Cook University, Australia
Liqian Chen	National University of Defense Technology, China
Xiaochun Cheng	Middlesex University, UK
Yi He	University of Louisiana at Lafayette, USA
Xinyi Huang	Fujian Normal University, China
Jingbing Li	Hainan University, China
Wenjuan Li	The Hong Kong Polytechnic University, China
Fang Liu	Hunan University, China
Shigang Liu	Swinburne University of Technology, Australia
Xiaozhang Liu	Hainan University, China
Xinwang Liu	National University of Defense Technology, China
Jianfeng Ma	Xidian University, China
Lichuan Ma	Xidian University, China
Weizhi Meng	Technical University of Denmark, Denmark
Jiaohua Qin	Central South University of Forestry and Technology, China
Youyang Qu	Deakin University, Australia
Kui Ren	Zhejiang University, China
Yizhi Ren	Hangzhou University of Electronic Science and Technology, China
Hong Sheng	Beihang University, China
Victor S. Sheng	Texas Tech University, USA
Limin Sun	Chinese Academy of Sciences, China
Shifeng Sun	Monash University, Australia
Willy Susilo	University of Wollongong, Australia
Lei Wang	Hainan University, China
Xianmin Wang	Guangzhou University, China
Xianpeng Wang	Hainan University, China
Yu Wang	Guangzhou University, China
Bailin Xie	Guangdong University of Foreign Studies, China
Naixue Xiong	Tianjin University, China
Ping Xiong	Zhongnan University of Economics and Law, China
Hongyang Yan	Guangzhou University, China
Qiuling Yang	Hainan University, China
Jianping Yin	National University of Defense Technology, China
Dian Zhang	Hainan University, China
Jun Zhang	Swinburne University of Technology, Australia
Peng Zhang	Shenzhen University, China
En Zhu	National University of Defense Technology, China
Tianqing Zhu	University of Technology Sydney, Australia

Organization Committee

Jianping Yin	National University of Defense Technology, China
Xinwang Liu	National University of Defense Technology, China
Jianfeng Ma	National University of Defense Technology, China

Kui Ren	National University of Defense Technology, China
Limin Sun	National University of Defense Technology, China
Sheng Hong	Beihang University, China

Contents

Camdar-Adv: Method for Generating Adversarial Patches on 3D Object	1
<i>Chang Chen and Teng Huang</i>	
Universal Adversarial Perturbations of Malware	9
<i>Ruitao Hou, Xiaoyu Xiang, Qixiang Zhang, Jiabao Liu, and Teng Huang</i>	
A Semi-supervised Learning Approach for High Dimensional Android Malware Classification	20
<i>Qiao Shang, Ni Li, Qi Qi, and Xiao-Wei Lin</i>	
Kernel Optimization in SVM for Defense Against Adversarial Attacks	32
<i>Wanman Li and Xiaozhang Liu</i>	
An Empirical Study on the Status Quo of Higher Vocational Teachers’ Informatization Teaching Ability – A Case Study of Hainan Province	43
<i>Yi-nan Chen, Peng Sun, and Xia Liu</i>	
Reliability Optimization and Trust Computing of Composite Wing Based on Sparse PC Method	58
<i>Li Miao, Wang Lei, and Xu Chao</i>	
Malware Variants Detection Based on Feature Fusion	67
<i>Jianbin Mai, Chunjie Cao, and Qian Wu</i>	
Robust GAN Based on Attention Mechanism	78
<i>Qian Wu, Chunjie Cao, Jianbin Mai, and Fangjian Tao</i>	
Training Aggregation in Federated Learning	87
<i>Li Hu, Hongyang Yan, and Zulong Zhang</i>	
A Robust Digital Watermarking for Medical Images Based on PHTs-DCT	95
<i>Dan Yi, Jing Liu, Jingbing Li, Jingjun Zhou, Uzair Aslam Bhatti, Yangxiu Fang, and Saqib Ali Nawaz</i>	
A Robust Zero Watermarking Algorithm for Medical Images Based on Tetrolet-DCT	109
<i>Wenfeng Cui, Jing Liu, Jingbing Li, Yangxiu Fang, Xiliang Xiao, Uzair Aslam Bhatti, and Saqib Ali Nawaz</i>	
HOUGH-DCT Based Robust Watermarking for Medical Image	120
<i>Ruiqi Mo, Jing Liu, Jingbing Li, Yulin Wang, and Jingjun Zhou</i>	

The Blind Separation of Cockpit Mixed Signals Based on Fast Independent Component Analysis	132
<i>Zhengmao Wu, Sihai Li, Jing Sun, and Mingrui Chen</i>	
A Zero-Watermarking Algorithm for Medical Images Based on Gabor-DCT ...	144
<i>Xiliang Xiao, Jing Liu, Jingbing Li, Yangxiu Fang, Cheng Zeng, Jiabin Hu, and Uzair Aslam Bhatti</i>	
Analysis on Influencing Factors of Electricity Sales for Electric Data Security	157
<i>Hailing He, Wei Zou, Qinghong Guo, Wenxian Wu, and Kejiang Xiao</i>	
A Regularization-Based Positive and Unlabeled Learning Algorithm for One-Class Classification of Remote Sensing Data	172
<i>Yan Zhang, Tianjiao Yang, and Chenguang Zhang</i>	
SDSBT: A Secure Multi-party Data Sharing Platform Based on Blockchain and TEE	184
<i>Hong Lei, Yun Yan, Zijian Bao, Qinghao Wang, Yongxin Zhang, and Wenbo Shi</i>	
BID-HCP: Blockchain Identifier Based Health Certificate Passport System	197
<i>Yuwen Zhang, Yang Liu, and Cheng Chi</i>	
Research on Global Map Construction and Location of Intelligent Vehicles Based on Lidar	210
<i>Biyao Wang, Yi Han, and Jing Jin</i>	
A Problem-Driven Discussion Teaching Method Based on Progressive Cycle	225
<i>Xiaoyi Zhou, Shaohua Duan, and Wei Li</i>	
The Detection and Segmentation of Pulmonary Nodules Based on U-Net	236
<i>Guilai Han, Wei Liu, Benguo Yu, Lin Niu, Xiaoling Li, Lu Liu, and Haixia Li</i>	
Trajectory Shaping Guidance Law of Homing Missile with High Maneuver and Low Overload and Its Database Security	245
<i>Li Miao, Wang Lei, and Xu Chao</i>	
Bibliometric and Graph Analysis in Document Data Mining Based on the Cultivation of New Type Professional Farmers	261
<i>Chaosheng Tang and Lijin Qin</i>	

Privacy-Preserving Movie Scoring Algorithm Based on Deep Neural Network	275
<i>Weinan Song, Xinyu Fan, Jing Li, Aslam Niaz Khan, and Lei Wang</i>	
Research on a Malicious Code Detection Method Based on Convolutional Neural Network in a Domestic Sandbox Environment	290
<i>Jianhua Xing, Hong Sheng, Yuning Zheng, and Wei Li</i>	
Electricity Sales Forecasting Based on Model Fusion and Prophet Model	299
<i>Kai Li, Jian Li, Jun Tang, Siming Chen, Jiao Wu, Yaoheng Xie, and Kejiang Xiao</i>	
Research on Electricity Sales Forecast Model Based on Big Data	316
<i>Kai Li, Jian Li, Siming Chen, Jun Tang, Jiao Wu, Yingping Zhang, and Kejiang Xiao</i>	
Author Index	329