

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 <https://link.springer.com/bookseries/7410>

Joseph K. Liu · Sokratis Katsikas ·
Weizhi Meng · Willy Susilo · Rolly Intan (Eds.)

Information Security

24th International Conference, ISC 2021
Virtual Event, November 10–12, 2021
Proceedings


Editors

Joseph K. Liu 
Monash University
Clayton, VIC, Australia

Weizhi Meng 
Technical University of Denmark
Kongens Lyngby, Denmark

Rolly Intan
Petra Christian University
Surabaya, Indonesia

Sokratis Katsikas 
Norwegian University of Science
and Technology
Gjøvik, Norway

Willy Susilo 
University of Wollongong
Wollongong, NSW, Australia

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-91355-7 ISBN 978-3-030-91356-4 (eBook)
<https://doi.org/10.1007/978-3-030-91356-4>

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

On behalf of the Program Committee, it is our pleasure to present the proceedings of the 24th Information Security Conference (ISC 2021). ISC is an annual international conference covering research in theory and applications of information security. Both academic research with high relevance to real-world problems and developments in industrial and technical frontiers fall within the scope of the conference.

The 24th edition of ISC was organized by the Petra Christian University, Surabaya, Indonesia, and was held entirely online (due to the COVID-19 pandemic) during November 10–12, 2021. Willy Susilo (University of Wollongong, Australia) and Rolly Intan (Petra Christian University, Indonesia) served as the general chairs, whilst we—Joseph Liu (Monash University, Australia) and Sokratis K. Katsikas (Norwegian University of Science and Technology, Norway)—served as the program co-chairs. The Program Committee comprised 54 members from top institutions around the world. Out of 87 submissions, the Program Committee eventually selected 21 papers for presentation at the conference and publication in the proceedings, resulting in an acceptance rate of 24.1%. The review process was double-blind, and it was organized and managed through the EasyChair online reviewing system, with all papers receiving at least three reviews. The final program was quite balanced in terms of topics, containing both theoretical/cryptography papers and more practical/systems security papers.

A successful conference is the result of the joint effort of many people. We would like to express our appreciation to the Program Committee members and external reviewers for the time spent reviewing papers and participating in the online discussion. We deeply thank our invited speakers for their willingness to participate in the conference, especially during the difficult times in the middle of the global pandemic. Further, we express our appreciation to Weizhi Meng (Technical University of Denmark, Denmark), who served as the publication chair. Finally, we thank Springer for publishing these proceedings as part of their LNCS series, and the ISC Steering Committee for their continuous support and assistance.

ISC 2021 would not have been possible without the authors who submitted their work and presented their contributions, as well as the attendees who joined the conference sessions. We would like to thank them all, and we look forward to their future contributions to ISC.

October 2021

Joseph Liu
Sokratis Katsikas

Organization

Steering Committee

Zhiqiang Lin	The Ohio State University, USA
Javier Lopez	University of Malaga, Spain
Masahiro Mambo	Kanazawa University, Japan
Eiji Okamoto	University of Tsukuba, Japan
Michalis Polychronakis	Stony Brook University, USA
Jianying Zhou	Singapore University of Technology and Design, Singapore

General Chairs

Willy Susilo	University of Wollongong, Australia
Rolly Intan	Petra Christian University, Indonesia

Program Chairs

Joseph Liu	Monash University, Australia
Sokratis K. Katsikas	Norwegian University of Science and Technology, Norway

Publication Chair

Weizhi Meng	Technical University of Denmark, Denmark
-------------	--

Technical Program Committee

Masayuki Abe	NTT Secure Platform Laboratories, Japan
Cristina Alcaraz	University of Malaga, Spain
Man Ho Au	University of Hong Kong, Hong Kong
Liqun Chen	University of Surrey, UK
Xiaofeng Chen	Xidian University, China
Mauro Conti	University of Padua, Italy
Frédéric Cuppens	Polytechnique Montreal, Canada
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Dung Hoang Duong	University of Wollongong, Australia
Steven Furnell	University of Nottingham, UK
Joaquin Garcia-Alfaro	Institut Polytechnique de Paris, France
Vasileios Gkioulos	Norwegian University of Science and Technology, Norway
Stefanos Gritzalis	University of Piraeus, Greece
Fuchun Guo	University of Wollongong, Australia

Jinguang Han	Queen's University Belfast, UK
Shoichi Hirose	University of Fukui, Japan
Xinyi Huang	Fujian Normal University, China
Christos Kalloniatis	University of the Aegean, Greece
Sokratis K. Katsikas	Norwegian University of Science and Technology, Norway
Angelos Keromytis	Georgia Institute of Technology, Georgia
Hiroaki Kikuchi	Meiji University, Japan
Hyoungshick Kim	Sungkyunkwan University, South Korea
Mirosław Kutylowski	Wrocław University of Science and Technology, Poland
Shangqi Lai	Monash University, Australia
Jooyoung Lee	Korea Advanced Institute of Science and Technology, South Korea
Yannan Li	University of Wollongong, Australia
Kaitai Liang	Delft University of Technology, Netherlands
Joseph Liu	Monash University, Australia
Javier Lopez	University of Malaga, Spain
Rongxing Lu	University of New Brunswick, Canada
Xiapu Luo	Hong Kong Polytechnic University, Hong Kong
Mark Manulis	University of Surrey, UK
Weizhi Meng	Technical University of Denmark, Denmark
Khoa Nguyen	Nanyang Technological University, Singapore
Pankaj Pandey	Norwegian University of Science and Technology, Norway
Günther Pernul	Universität Regensburg, Germany
Josef Pieprzyk	CSIRO, Data61, Australia
Nikolaos Pitropakis	Edinburgh Napier University, UK
Reihaneh Safavi-Naini	University of Calgary, Canada
Georgios Spathoulas	Norwegian University of Science and Technology, Norway
Stavros Stavrou	Open University of Cyprus, Cyprus
Ron Steinfeld	Monash University, Australia
Shi-Feng Sun	Monash University, Australia
Willy Susilo	University of Wollongong, Australia
Qiang Tang	University of Sydney, Australia
Ding Wang	Nankai University, China
Avishai Wool	Tel Aviv University, Israel
Qianhong Wu	Beihang University, China
Toshihiro Yamauchi	Okayama University, Japan
Guomin Yang	University of Wollongong, Australia
Yong Yu	Shaanxi Normal University, China
Tsz Hon Yuen	University of Hong Kong, Hong Kong
Mingwu Zhang	Hubei University of Technology, China
Jianying Zhou	Singapore University of Technology and Design, Singapore

Additional Reviewers

Mohsen Ali
Marios Anagnostopoulos
Michael Bamiloshin
Thomas Baumer
Cailing Cai
Yanmei Cao
Eyasu Getahun Chekole
Long Chen
Yonghui Chen
Chengjun Lin
Liron David
Fuyang Deng
Vasiliki Diamantopoulou
Philip Empl
Ludwig Englbrecht
Sabrina Friedl
Sebastian Groll
Rami Haffar
Fadi Hassan
Shen Hua
Li Huilin
Najeeb Jebreel
Pallavi Kaliyar
Maria Karyda
Sascha Kern
Ashneet Khandpur Singh
Chhagan Lal
Minghang Li
Yumei Li
Trupil Limbasiya
Chao Lin
Eleonora Losiouk
Jiqiang Lu

Katerina Mavroeidi
Mohamed-Amine Merzouk
Reza Mohammadi
Antonio Muñoz
Vinod P. Nair
Jianting Ning
Jean-Yves Ouattara
Jing Pan
Shimin Pan
Pavlos Papadopoulos
Argyri Pattakou
Baodong Qin
Xianrui Qin
Tian Qiu
Yanli Ren
Rahul Saha
Jun Shen
Stavros Simou
Chunhua Su
Teik Guan Tan
Aggeliki Tsohou
Mingming Wang
Mingli Wu
Yi Xie
Lei Xu
S. J. Yang
Xu Yang
Yang Yang
Shang Zefua
Jixin Zhang
Yudi Zhang
Yuexin Zhang
Haibin Zheng

Contents

Cryptology

Integer LWE with Non-subgaussian Error and Related Attacks	3
<i>Tianyu Wang, Yuejun Liu, Jun Xu, Lei Hu, Yang Tao, and Yongbin Zhou</i>	
Layering Quantum-Resistance into Classical Digital Signature Algorithms	26
<i>Teik Guan Tan and Jianying Zhou</i>	
Cryptanalysis of RSA Variants with Primes Sharing Most Significant Bits	42
<i>Meryem Cherkaoui-Semmouni, Abderrahmane Nitaj, Willy Susilo, and Joseph Tonien</i>	
Cryptanalysis of Two White-Box Implementations of the SM4 Block Cipher	54
<i>Jiqiang Lu and Jingyu Li</i>	
A Non-interactive Multi-user Protocol for Private Authorised Query Processing on Genomic Data	70
<i>Sara Jafarbeiki, Amin Sakzad, Shabnam Kasra Kermanshahi, Ron Steinfeld, Raj Gaire, and Shangqi Lai</i>	
Bigdata-Facilitated Two-Party Authenticated Key Exchange for IoT	95
<i>Bowen Liu, Qiang Tang, and Jianying Zhou</i>	
Randomized Component Based Secure Secret Reconstruction in Insecure Networks	117
<i>Xinyan Wang and Fuyou Miao</i>	
Transparency Order of (n, m) -Functions—Its Further Characterization and Applications	139
<i>Yu Zhou, Yongzhuang Wei, Hailong Zhang, Luyang Li, Enes Pasalic, and Wenling Wu</i>	

Web and OS Security

Browserprint: An Analysis of the Impact of Browser Features on Fingerprintability and Web Privacy	161
<i>Seyed Ali Akhavan, Jordan Jueckstock, Junhua Su, Alexandros Kapravelos, Engin Kirda, and Long Lu</i>	

TridentShell: A Covert and Scalable Backdoor Injection Attack on Web Applications	177
<i>Xiaobo Yu, Weizhi Meng, Lei Zhao, and Yining Liu</i>	
Andromeda: Enabling Secure Enclaves for the Android Ecosystem	195
<i>Dimitris Deyannis, Dimitris Karnikis, Giorgos Vasiliadis, and Sotiris Ioannidis</i>	
Network Security	
FEX – A Feature Extractor for Real-Time IDS	221
<i>Andreas Schaad and Dominik Binder</i>	
Identifying Malicious DNS Tunnel Tools from DoH Traffic Using Hierarchical Machine Learning Classification	238
<i>Rikima Mitsuhashi, Akihiro Satoh, Yong Jin, Katsuyoshi Iida, Takahiro Shinagawa, and Yoshiaki Takai</i>	
Detection of Malware, Attacks and Vulnerabilities	
Hybroid: Toward Android Malware Detection and Categorization with Program Code and Network Traffic	259
<i>Mohammad Reza Norouzian, Peng Xu, Claudia Eckert, and Apostolis Zarras</i>	
A Novel Behavioural Screenlogger Detection System	279
<i>Hugo Sbai, Jassim Happa, and Michael Goldsmith</i>	
DEVA: Decentralized, Verifiable Secure Aggregation for Privacy-Preserving Learning	296
<i>Georgia Tsaloli, Bei Liang, Carlo Brunetta, Gustavo Banegas, and Aikaterini Mitrokotsa</i>	
DVul-WLG: Graph Embedding Network Based on Code Similarity for Cross-Architecture Firmware Vulnerability Detection	320
<i>Hao Sun, Yanjun Tong, Jing Zhao, and Zhaoquan Gu</i>	
Machine Learning for Security	
Detect and Remove Watermark in Deep Neural Networks via Generative Adversarial Networks	341
<i>Shichang Sun, Haoqi Wang, Mingfu Xue, Yushu Zhang, Jian Wang, and Weiqiang Liu</i>	

Targeted Universal Adversarial Perturbations for Automatic Speech Recognition	358
<i>Wei Zong, Yang-Wai Chow, Willy Susilo, Santu Rana, and Svetha Venkatesh</i>	
Voxstructor: Voice Reconstruction from Voiceprint	374
<i>Panpan Lu, Qi Li, Hui Zhu, Giuliano Sovernigo, and Xiaodong Lin</i>	
Word-Map: Using Community Detection Algorithm to Detect AGDs	398
<i>Futai Zou, Qianying Shen, and Yuzong Hu</i>	
Author Index	415