

**Ilsun You
Taek-Young Youn (Eds.)**

LNCS 13720

Information Security Applications

**23rd International Conference, WISA 2022
Jeju Island, South Korea, August 24–26, 2022
Revised Selected Papers**



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>


Il sun You · Taek-Young Youn (Eds.)

Information Security Applications

23rd International Conference, WISA 2022
Jeju Island, South Korea, August 24–26, 2022
Revised Selected Papers

Editors

Ilsun You
Soonchunhyang University
Asan-Si, Korea (Republic of)

Taek-Young You 
Dankook University
Yongin, Korea (Republic of)

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-25658-5

ISBN 978-3-031-25659-2 (eBook)

<https://doi.org/10.1007/978-3-031-25659-2>

© Springer Nature Switzerland AG 2023

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 revised and selected papers which were submitted to and presented at the 23rd World Conference on Information Security Applications (WISA 2022) which was held at Jeju Island, Korea, during August 24–26, 2022. WISA 2022 provided an international forum for sharing original research results among specialists in various theories and practical applications.

We received 76 submissions, covering all areas of information security, and finally selected 30 papers to be presented at the conference. Among them, only 25 papers (32.9% of submitted papers) were selected for publication in this LNCS volume. We thank the authors for submitting meaningful papers to WISA 2022. We also thank the authors for their patience and cooperation during the back-and-forth process of comments and revisions requested by the editor and the reviewers. We were specially honored to have the two keynote talks by Willy Susilo (University of Wollongong), on “Cloud Computing Security,” and Yi-Bing Lin (Miin Wu SOC Chair Professor) on “5G Private Network Security and Applications.”

The conference was hosted by the Korea Institute of Information Security and Cryptography (KIISC) and sponsored by the Ministry of Science, ICT and Future Planning (MSIP) and National Intelligence Service (NIS), and co-sponsored by the Electronics & Telecommunications Research Institute (ETRI), the Korea Internet & Security Agency (KISA), the National Security Research Institute (NSR), and KONAI. The program chairs, Ilsun You (Kookmin University) and Taek-Young Youn, prepared a valuable program along with the Program Committee members listed here. The excellent arrangements for the conference venue were led by the WISA 2022 general chair, Okyeon Yi (Kookmin University), and organizing chairs, Jung Taek Seo (Gachon University) and Ki-Woong Park (Sejong University). Many people contributed to the success of WISA 2022. We would like to express our deepest appreciation to each of the WISA Program Committee and Organizing Committee members. Thanks to their invaluable support and sincere dedication, WISA 2022 was a success. Finally, we thank the Springer team for assistance with the LNCS proceedings.

September 2022

Ilsun You
Taek-Young Youn

Jong Kim	POSTECH, South Korea
Jongkil Kim	University of Wollongong, Australia
TaeGuen Kim	Soonchunhyang University, South Korea
Hyun Kwon	Korea Military Academy, South Korea
Yonghwi Kwon	University of Virginia, USA
Kyu Hyung Lee	University of Georgia, USA
Siqi Ma	University of New South Wales, Australia
David Mohaisen	University of Central Florida, USA
Masakatsu Nishigaki	Shizuoka University, Japan
Jason Nurse	University of Kent, UK
Younghee Park	San Jose State University, USA
Marcus Peinado	Microsoft, USA
Hyun Sook Rhee	Samsung Electronics, South Korea
Junghwan Rhee	University of Central Oklahoma, USA
Ulrich Rührmair	Ruhr University Bochum, Germany
Kouichi Sakurai	Kyushu University, Japan
Seog Chung Seo	Kookmin University, South Korea
Seung-Hyun Seo	Hanyang University, South Korea
Junji Shikata	Yokohama National University, Japan
Sang Uk Shin	Pukyong National University, South Korea
Seonghan Shin	AIST, Japan
Amril Syalim	University of Indonesia, Indonesia
Gang Tan	Pennsylvania State University, USA
Simon Woo	Sungkyunkwan University, South Korea
Toshihiro Yamauchi	Okayama University, Japan
Naoto Yanai	Osaka University, Japan
Meng Yu	Roosevelt University, USA

Organizing Committee

JongWook Baek	Gachon University, South Korea
Namkyun Baik Busan	University of Foreign Studies, South Korea
Jungsoo Park	Soongsil University, South Korea
Hangbae Chang	Chung-Ang University, South Korea
Byeongcheol Choi	ETRI, South Korea
Daeseon Choi	Soongsil University, South Korea
Hyojin Cho	Soongsil University, South Korea
KwangHee Choi	KISA, South Korea
Won Seok Choi	Hansung University, South Korea
Dongguk Han	Kookmin University, South Korea
Jaechel Ha	Hoseo University, South Korea
Manpyo Hong	Ajou University, South Korea
Seokhie Hong	Korea University, South Korea

Souhwan Jung	Soongsil University, South Korea
Yousung Kang	ETRI, South Korea
ChangHoon Kim	Daegu University, South Korea
Geonwoo Kim	ETRI, South Korea
Howon Kim	Pusan National University, South Korea
Hwanguk Kim	Sangmyung University, South Korea
Jin Cheol Kim	KEPCO-KDN, South Korea
Jongsung Kim	Kookmin University, South Korea
Sungmin Kim	Sungshin Women's University, South Korea
Tae-Sung Kim	Chungbuk National University, South Korea
Kibom Kim	NSR, South Korea
WonHo Kim	NSR, South Korea
Woo-Nyon Kim	NSR, South Korea
Hun Yeong	Kwon Korea University, South Korea
Jin Kwak	Ajou University, South Korea
Daesung Moon	ETRI, South Korea
Changhoon Lee	Seoul National University of Science and Technology, South Korea
Dong Hoon Lee	Korea University, South Korea
Imyeong Lee	Soonchunhyang University, South Korea
Jong-Hyouk Lee	Sejong University, South Korea
Kyungho Lee	Korea University, South Korea
Manhee Lee	Hannam University, South Korea
SeokJoon Lee	Gachon University, South Korea
Sungjae Lee	KISA, South Korea
Donghwan Oh	KISA, South Korea
Heekuck Oh	Hanyang University, South Korea
Hyung-Geun Oh	NSR, South Korea
Jin Young Oh	KISA, South Korea
Yunheung Paek	Seoul National University, South Korea
Kyung-Hyune Rhee	Pukyong National University, South Korea
HwaJung Seo	Hansung University, South Korea
Kyungho Son	Kangwon National University, South Korea
Jungsuk Song	Korea Institute of Science & Technology Information, South Korea
Jaechol Ryou	Chungnam National University, South Korea
Yoojae Won	Chungnam National University, South Korea

Contents

Cryptography

Collision-Resistant and Pseudorandom Hash Function Using Tweakable Block Cipher	3
<i>Shoichi Hirose</i>	
Provably Secure Password-Authenticated Key Exchange Based on SIDH	16
<i>Theo Fanuela Prabowo and Chik How Tan</i>	
Group Signatures with Designated Traceability over Openers' Attributes in Bilinear Groups	29
<i>Hiroaki Anada, Masayuki Fukumitsu, and Shingo Hasegawa</i>	
Grover on SPARKLE	44
<i>Yujin Yang, Kyungbae Jang, Hyunji Kim, Gyeongju Song, and Hwajeong Seo</i>	

Network Security

Quality-of-Service Degradation in Distributed Instrumentation Systems Through Poisoning of 5G Beamforming Algorithms	63
<i>Borja Bordel, Ramón Alcarria, Joaquin Chung, Rajkumar Kettimuthu, Tomás Robles, and Iván Armuelles</i>	
An Effective Approach for Stepping-Stone Intrusion Detection Using Packet Crossover	77
<i>Lixin Wang, Jianhua Yang, and Austin Lee</i>	
Software-Defined Network Based Secure Internet-Enabled Video Surveillance System	89
<i>Mathew Del Castillo, Harvey Hermosa, Philip Virgil Astillo, Gaurav Choudhary, and Nicola Dragoni</i>	
TLS Goes Low Cost: When TLS Meets Edge	102
<i>Intae Kim, Willy Susilo, Joonsang Baek, Jongkil Kim, and Yang-Wai Chow</i>	
5G-AKA, Revisited	114
<i>SeongHan Shin</i>	

Privacy Enhancing Technique

Membership Privacy for Asynchronous Group Messaging 131
Keita Emura, Kaisei Kajita, Ryo Nojima, Kazuto Ogawa, and Go Ohtake

On Membership Inference Attacks to Generative Language Models Across
 Language Domains 143
*Myung Gyo Oh, Leo Hyun Park, Jaekuk Kim, Jaewoo Park,
 and Taekyoung Kwon*

A Joint Framework to Privacy-Preserving Edge Intelligence in Vehicular
 Networks 156
Muhammad Firdaus and Kyung-Hyune Rhee

Vulnerability Analysis

Recovering Yaw Rate from Signal Injection Attack to Protect RV’s
 Direction 171
Hyunsu Cho, Sunwoo Lee, Wonsuk Choi, and Dong Hoon Lee

A Survey on Sensor False Data Injection Attacks and Countermeasures
 in Cyber-Physical and Embedded Systems 185
Jinhong Choi and Yeongjin Jang

DAZZLE- ATTACK: Anti-Forensic Server-side Attack via Fail-Free
 Dynamic State Machine 204
*Bora Lee, Kyungchan Lim, JiHo Lee, Chijung Jung, Doowon Kim,
 Kyu Hyung Lee, Haehyun Cho, and Yonghwi Kwon*

vkTracer: Vulnerable Kernel Code Tracing to Generate Profile of Kernel
 Vulnerability 222
Hiroki Kuzuno and Toshihiro Yamauchi

Security Engineering

ARMing-Sword: Scabbard on ARM 237
*Hyeokdong Kwon, Hyunjun Kim, Minjoo Sim, Siwoo Eum, Minwoo Lee,
 Wai-Kong Lee, and Hwajeong Seo*

Optimized Implementation of Quantum Binary Field Multiplication
 with Toffoli Depth One 251
*Kyungbae Jang, Wonwoong Kim, Sejin Lim, Yeajun Kang, Yujin Yang,
 and Hwajeong Seo*

Time-Optimal Design of Finite Field Arithmetic for SIKE on Cortex-M4 265
Mila Anastasova, Reza Azarderakhsh, and Mehran Mozaffari Kermani

Analysis of Radioactive Decay Based Entropy Generator in the IoT Environments 277
Taewan Kim, Seyoon Lee, Seunghwan Yun, Jongbum Kim, and Okyeon Yi

Security Management

A Novel Metric for Password Security Risk Against Dictionary Attacks 291
Binh Le Thanh Thai and Hidema Tanaka

Towards Evaluating the Security of Human Computable Passwords Using Neural Networks 303
Issei Murata, Pengju He, Yujie Gu, and Kouichi Sakurai

Markov Decision Process for Automatic Cyber Defense 313
Xiaofan Zhou, Simon Yusuf Enoch, and Dong Seong Kim

Influence Through Cyber Capacity Building: Network Analysis of Assistance, Cooperation, and Agreements Among ASEAN Plus Three Countries 330
Yu-kyung Kim, Myong-hyun Go, and Kyungho Lee

Chameleon DNN Watermarking: Dynamically Public Model Ownership Verification 344
Wei Li, Xiaoyu Zhang, Shen Lin, Xinbo Ban, and Xiaofeng Chen

Author Index 357