Lecture Notes in Computer Science 12583

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

Ilsun You (Ed.)

Information Security Applications

21st International Conference, WISA 2020 Jeju Island, South Korea, August 26–28, 2020 Revised Selected Papers

Springer

Editor
Ilsun You
Soonchunhyang University
Asan, Korea (Republic of)

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-65298-2 ISBN 978-3-030-65299-9 (eBook)
https://doi.org/10.1007/978-3-030-65299-9

LNCS Sublibrary: SL4 – Security and Cryptology

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Over the past decades, many advances in information technologies that include artificial intelligence (AI), 5G, blockchain, Internet of Things (IoT), and many more provided beneficial effects on various aspects of our lives. However, these advancements are accompanied with even more sophisticated threats to individuals, businesses, and government's most valuable data assets. Cybercriminals are also exploiting such technologies to find vulnerabilities and develop more sophisticated attacks. Therefore, it is of paramount importance to continuously study, inform, and develop new techniques to ensure information security.

World Conference on Information Security Application (WISA) is one of the main security research venues hosted by the Korea Institute of Information Security and Cryptography (KIISC) and sponsored by the Ministry of Science, ICT and Future Planning (MSIP), and co-sponsored by the Electronics & Telecommunication Research Institute (ETRI), the Korea Internet & Security Agency (KISA), and the National Security Research Institute (NSR). Especially in 2020, WISA celebrated the 31st anniversary for KIISC while going toward its new position as the best contributor to information security. Additionally, due to inevitable social changes caused by the COVID-19 pandemic, WISA took a new path in holding the 21st World Conference on Information Security Applications (WISA 2020). Despite the challenges, WISA continued to provide an open forum for exchanging and sharing common research interests through both live and recorded online presentations. The challenges lead to another opportunity for WISA to provide a platform for sharing results of on-going research, developments, and application on information security areas.

This volume is composed of the extended version of papers presented at WISA 2020, held at Jeju Island, South Korea during August 26–28, 2020. The primary focus of WISA 2020 is on systems and network security, including all other technical and practical aspects of security application. In particular, this year's conference invited researchers working on 5G/6G, AI, blockchain, V2X, and advanced IoT who are keen on bringing the latest open security challenges.

A total of 31 outstanding papers, covering areas such as AI and intrusion detection, steganography and malware, cryptography, cyber security, application, systems, and hardware security were accepted for presentation at WISA 2020. This year, WISA 2020 specially included poster presentations which composed of 39 posters. Moreover, invited keynote talks by Prof. Matt Bishop (University of California, USA), and Prof. Suman Jana (Columbia University, USA), as well as tutorial talks by Prof. Dan Dongseong Kim (The University of Queensland, Australia), and Dr. SeongHan Shin (National Institute of AIST, Japan) augmented the conference.

The great effort and countless dedication of the Organizing Committee and reviewers, support of the sponsor and co-sponsor, and active participation of all the participants led to another success story for WISA 2020. We would like to acknowledge the contribution of each individual Program Committee member. As well as our sincere gratitude to all the reviewers, authors, and participants around the world for their unending support.

October 2020 Ilsun You

Organization

General Chair

Souhwan Jung	Soongsil University, South Korea

Program Committee Chair

Ilsun You	Soonchunhyang University, South Korea

Program Committee

Pelin Angin	Middle East Technical University, Turkey
Joonsang Baek	University of Wollongong, Australia
Sang Kil Cha	KAIST, South Korea
Xiaofeng Chen	Xidian University, China
Jin-Hee Cho	Virginia Tech, USA
Dooho Choi	ETRI, South Korea
Swee-Huay Heng	Multimedia University, Malaysia
Hsu-Chun Hsiao	National Taiwan University, Taiwan
Qiong Huang	South China Agricultural University, China
Eul Gyu Im	Hanyang University, South Korea
Yeongjin Jang	Oregon State University, USA
Hiroaki Kikuchi	Meji University, Japan
Dongseong Kim	The University of Queensland, Australia
Jong Kim	POSTECH, South Korea
Jongkil Kim	University of Wollongong, Australia
Jonghoon Kwon	ETH Zurich, Switzerland
Byoungyoung Lee	Seoul National University, South Korea
Kyu Hyung Lee	University of Georgia, USA
Shengli Liu	Shanghai Jiao Tong University, China
Aziz Mohaisen	University of Central Florida, USA
Kirill Morozov	University of North Texas, USA
Masakatsu Nishigaki	Shizuoka University, Japan
Jason Nurse	University of Kent, UK
Kazumasa Omote	University of Tsukuba, Japan
Ki-Woong Park	Sejong University, South Korea
Marcus Peinado	Microsoft, USA
Junghwan Rhee	NEC Laboratories, USA
Ulrich Rührmair	LMU Munich, Germany
Kouichi Sakurai	Kyushu University, Japan
Junji Shikata	Yokohama National University, Japan
Dongwan Shin	New Mexico Tech, USA

Sang Uk Shin	Pukyong National University, South Korea
SeongHan Shin	AIST, Japan
Amril Syalim	University of Indonesia, Indonesia
Gang Tan	Penn State University, USA
Samuel Woo	Dankook University, South Korea
Toshihiro Yamauchi	Okayama University, Japan
Naoto Yanai	Osaka University, Japan
Siu Ming Yiu	The University of Hong Kong, Hong Kong
Taek-Young Youn	ETRI, South Korea
Mengyu Yu	Roosevelt University, USA

Organizing Committee Chair

Jung-Hyouk Lee	Sejong University, South Korea

Organizing Committee

Hyo-Beom Ahn	Kongju National University, South Korea
Soonjoung Byun	KISA, South Korea
Byung-Chul Choi	ETRI, South Korea
Yangseo Choi	ETRI, South Korea
KyengHwa Do	Konkuk University, South Korea
Dong-Guk Han	Kookmin University, South Korea
Hyoung Chun Kim	NSR, South Korea
Jin Cheol Kim	ETRI, South Korea
Jonghyun Kim	ETRI, South Korea
Jongsung Kim	Kookmin University, South Korea
JungHee Kim	KISA, South Korea
Tai Hyo Kim	Formal Works Inc., South Korea
Woo-Nyon Kim	NSR, South Korea
Young-Gab Kim	Sejong University, South Korea
Jin Kwak	Ajou University, South Korea
Changhoon Lee	Seoul National University of Science and Technology, South Korea
Deok Gyu Lee	Seowon University, South Korea
Manhee Lee	Hannam University, South Korea
Seoklae Lee	KISA, South Korea
Daesub Park	Sejong University, South Korea
Ki-Woong Park	Sejong University, South Korea
Youngho Park	Sejong Cyber University, South Korea
Jungtaek Seo	Soonchunhyang University, South Korea
Ji Sun Shin	Sejong University, South Korea
Kangbin Yim	Soonchunhyang University, South Korea
Joobeom Yun	Sejong University, South Korea

Contents

AI Security and Intrusion Detection

Spatially Localized Perturbation GAN (SLP-GAN) for Generating Invisible Adversarial Patches . . . 3
Yongsu Kim, Hyoeun Kang, Afifatul Mukaroh, Naufal Suryanto, Harashta Tatimma Larasati, and Howon Kim

Detecting Block Cipher Encryption for Defense Against Crypto Ransomware on Low-End Internet of Things . . . 16
Hyunji Kim, Jaehoon Park, Hyeokdong Kwon, Kyoungbae Jang, Seung Ju Choi, and Hwajeong Seo

CAPTCHAs Are Still in Danger: An Efficient Scheme to Bypass Adversarial CAPTCHAs . . . 31
Dongbin Na, Namgyu Park, Sangwoo Ji, and Jong Kim

Unsupervised Intrusion Detection System for Unmanned Aerial Vehicle with Less Labeling Effort. . . . 45
Kyung Ho Park, Eunji Park, and Huy Kang Kim

Entropy-Based Feature Grouping in Machine Learning for Android Malware Classification. . . . 59
Hyunseok Shim and Souhwan Jung

DLDDO: Deep Learning to Detect Dummy Operations . . . 73
JongHyeok Lee and Dong-Guk Han

Steganography and Malware

3-Party Adversarial Steganography . . . 89
Ishak Meraouche, Sabyasachi Dutta, and Kouichi Sakurai

Accessibility Service Utilization Rates in Android Applications Shared on Twitter . . . 101
Shuichi Ichioka, Estelle Pouget, Takao Mimura, Jun Nakajima, and Toshihiro Yamauchi

Novel Reversible Acoustic Steganography Based on Carrier Orthogonality. . . 112
Hung-Jr Shiu, Fang-Yie Leu, Chun-Ming Lai, and Yu-Chun Huang

Application, System, and Hardware Security

Compact Implementation of CHAM Block Cipher on Low-End Microcontrollers 127
Hyeokdong Kwon, Hyunji Kim, Seung Ju Choi, Kyoungbae Jang, Jaehoon Park, Hyunjun Kim, and Hwajeong Seo

The Gravy Value: A Set of Features for Pinpointing BOT Detection Method 142
Semi Park and Kyungho Lee

Impact of Optimized Operations $A \cdot B$, $A \cdot C$ for Binary Field Inversion on Quantum Computers 154
Kyoungbae Jang, Seung Ju Choi, Hyeokdong Kwon, Zhi Hu, and Hwajeong Seo

Virtualization Technologies in the Android Framework and Compatibility with SEAndroid 167
Jaehyeon Yoon, Tu Chau Ngoc, Hoang Nguyen Huy, and Souhwan Jung

Toward a Fine-Grained Evaluation of the Pwnable CTF. 179
Sung-Kyung Kim, Eun-Tae Jang, and Ki-Woong Park

A Statistical Approach Towards Fraud Detection in the Horse Racing 191
Moohong Min, Jemin Justin Lee, Hyunbeom Park, Hyojoung Shin, and Kyungho Lee

On the Cost-Effectiveness of TrustZone Defense on ARM Platform 203
Naiwei Liu, Meng Yu, Wanyu Zang, and Ravi Sandhu

Detection on GPS Spoofing in Location Based Mobile Games 215
Shing Ki Wong and Siu Ming Yiu

Push for More: On Comparison of Data Augmentation and SMOTE with Optimised Deep Learning Architecture for Side-Channel. 227
Yoo-Seung Won, Dirmanto Jap, and Shivam Bhasin

Cryptography

Identity-Based Unidirectional Proxy Re-encryption in Standard Model: A Lattice-Based Construction 245
Priyanka Dutta, Willy Susilo, Dung Hoang Duong, Joonsang Baek, and Partha Sarathi Roy

Efficient Algorithm for Computing Odd-Degree Isogenies on Montgomery Curves 258
Kenta Kodera, Chen-Mou Cheng, and Atsuko Miyaji

An Efficient Implementation of AES on 8-Bit AVR-Based Sensor Nodes . . . 276
YoungBeom Kim and Seog Chung Seo

Revisiting the Minrank Problem on Multivariate Cryptography 291
Yacheng Wang, Yasuhiko Ikematsu, Shuhei Nakamura, and Tsuyoshi Takagi

Paid and Anonymous Usage of Cloud Software 308
Kun Peng

Optimization of PBKDF2-HMAC-SHA256 and PBKDF2-HMAC-LSH256 in CPU Environments 321
Hojin Choi and Seog Chung Seo

Cryptanalysis of Two Fully Anonymous Attribute-Based Group Signature Schemes with Verifier-Local Revocation from Lattices 334
Yanhua Zhang, Ximeng Liu, Yupu Hu, Qikun Zhang, and Huiwen Jia

Advances in Network Security and Attack Defense

Analysis on Malicious Residential Hosts Activities Exploited by Residential IP Proxy Services. 349
Akihiro Hanzawa and Hiroaki Kikuchi

Insights into Attacks' Progression: Prediction of Spatio-Temporal Behavior of DDoS Attacks 362
Ahmed Abusnaina, Mohammed Abuhamad, DaeHun Nyang, Songqing Chen, An Wang, and David Mohaisen

Methods to Select Features for Android Malware Detection Based on the Protection Level Analysis. 375
Chaeeun Lee, Eunnarae Ko, and Kyungho Lee

Cyber Security

Filtering-Based Correlation Power Analysis (CPA) with Signal Envelopes Against Shuffling Methods. 389
Youngbae Jeon and Ji Won Yoon

Security Problems of 5G Voice Communication 403
Seongmin Park, HyungJin Cho, Youngkwon Park, Bomin Choi, Dowon Kim, and Kangbin Yim

Author Index 417