2019 14th Asia Joint Conference on Information Security (AsiaJCIS 2019)

Kobe, Japan
1 – 2 August 2019

IEEE Catalog Number: CFP1933T-POD
ISBN: 978-1-7281-2557-2

Copyright © 2019 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP1933T-POD
ISBN (Print-On-Demand):	978-1-7281-2557-2
ISBN (Online):	978-1-7281-2556-5

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

2019 14th Asia Joint Conference on Information Security (AsiaJCIS)

AsiaJCIS 2019

Table of Contents

Message from the General Chairs ix
Message from the Program Chairs x
Conference Organization xi
Technical Program Committee xiii
Acknowledgements xv

Session 1: Malware

Detecting Unknown Malware from ASCII Strings with Natural Language Processing Techniques 1
Ryo Ito (National Defense Academy) and Mamoru Mimura (National Defense Academy)

Measurement Study Towards a Unified Firmware Updating Scheme for Legacy IoT Devices 9
Bing-Kai Hong (National Taiwan University of Science and Technology), Jr-Wei Huang (National Taiwan University of Science and Technology), Tao Ban (National Institute of Information and Communications Technology), Ryoichi Isawa (National Institute of Information and Communications Technology), Shin-Ming Cheng (National Taiwan University of Science and Technology), Daisuke Inoue (National Institute of Information and Communications Technology), and Koji Nakao (National Institute of Information and Communications Technology)

Malware Classification using Early Stage Behavioral Analysis 16
Nitesh Kumar (Indian Institute of Technology, Kanpur, India), Subhasis Mukhopadhyay (Indian Institute of Technology, Kanpur, India), Mugdha Gupta (Indian Institute of Technology, Kanpur, India), Anand Handa (Indian Institute of Technology, Kanpur, India), and Sandeep K. Shukla (Indian Institute of Technology, Kanpur, India)

Filtering Malicious JavaScript Code with Doc2Vec on an Imbalanced Dataset 24
Mamoru Mimura (National Defense Academy) and Yuya Suga (National Defense Academy)

Session 2: Data Security

String commitment scheme with low output locality .32
Hideaki Miyaji (Osaka University), Akinori Kawachi (Mie University), and Atsuko Miyaji (Osaka University)

Privacy and Integrity Protection of Metering Data in Smart Grid .40
Yong Ding (Guilin University of Electronic Technology, Guilin, China; Cyberspace Security Research Center, Pengcheng Laboratory, Shenzhen, China), Bingyao Wang (Guilin University of Electronic Technology, Guilin, China), Yujue Wang (Guilin University of Electronic Technology, Guilin, China), Kun Zhang (National Information Cente, Beijing, China), and Huiyong Wang (Guilin University of Electronic Technology, Guilin, China)

Analysis of Division Property using MILP Method for Lightweight Blockcipher Piccolo .48
Hiroki Sato (National Defence Academy), Mamoru Mimura (National Defense Academy), and Hidema Tanaka (National Defense Academy)

Secure Online-Efficient Interval Test based on Empty-Set Check .56
Katsunari Shishido (Osaka University, Japan Advanced Institute of Science and Technology) and Atsuko Miyaji (Osaka University, Japan Advanced Institute of Science and Technology)

Session 3: Detection

Platform Design and Implementation for Flexible Data Processing and Building ML Models of IDS Alerts .64
Iksoo Shin (University of Science & Technology), Yunsoo Choi (Korea Institute of Science & Technology Information(KISTI)), Taewoong Kwon (Korea Institute of Science & Technology Information(KISTI)), Hyeakro Lee (Korea Institute of Science & Technology Information(KISTI)), and Jungsuk Song (Korea Institute of Science & Technology Information(KISTI))

Boosting Fuzzing Performance with Differential Seed Scheduling .72
Chung-Yi Lin (National Chiao Tung University) and Chun-Ying Huang (National Chiao Tung University)

Prediction of Crime Occurrence using Information Propagation Model and Gaussian Process .80
Shusuke Morimoto (Carnegie Mellon University), Hajime Kawamukai (University of Hyogo), and Kilho Shin (Gakushuin University)

Session 4: Application Security

Enabling Cybersecurity Incident Reporting and Coordinated Handling for Maritime Sector .88
Bilhanan Silverajan (Tampere University) and Petteri Vistiaho (Tampere University)

Counter Attack Against the Bus-Off Attack on CAN .96
Masaru Takada (Kobe University), Yuki Osada (Kobe University), and Masakatu Morii (Kobe University)

Prevention of Data Leakage due to Implicit Information Flows in Android Applications .103
Hiroki Inayoshi (Nagoya Institute of Technology), Shohei Kakei (Nagoya Institute of Technology), Eiji Takimoto (Ritsumeikan University), Koichi Mouri (Ritsumeikan University), and Shoichi Saito (Nagoya Institute of Technology)

Designing Authentication and Authorization System with Blockchain .111
Yuki Ezawa (Kobe University), Makoto Takita (University of Hyogo), Yoshiaki Shiraishi (Kobe University), Shohei Kakei (Nagoya Institute of Technology), Masanori Hirotomo (Saga University), Youji Fukuta (Kindai University), Masami Mohri (Gifu University), and Masakatu Morii (Kobe University)

Watermarking Technique Based on Harris-Laplace Feature Point Detector Capable of Resisting Geometric Attacks .119
Kuo-Lung Hung (Chao-Yang University of Technology) and Chih-Yu Yen (Chao-Yang University of Technology)

Session 5: Cryptography

Identification Scheme Based on the Binary Syndrome Decoding Problem Using High-Density Parity-Check Matrices .127
Masanori Hirotomo (Saga University), Haruka Ito (Saga University), Youji Fukuta (Kindai University), Masami Mohri (Gifu University), and Yoshiaki Shiraishi (Kobe University)

Signcryption from NTRU Lattices Without Random Oracles .134
Zi-Yuan Liu (National Chengchi University, Taipei, Taiwan), Raylin Tso (National Chengchi University, Taipei, Taiwan), Yi-Fan Tseng (National Chengchi University, Taipei, Taiwan), and Masahiro Mambo (Kanazawa University, Kakuma Kanazawa, Japan)

A Signature Scheme Based on the Syndrome Decoding Problem Using LDPC Codes .142
Toshiki Tsuchida (Kobe University), Masanori Hirotomo (Saga University), Haruka Ito (Saga University), Makoto Takita (University of Hyogo), Yoshiaki Shiraishi (Kobe University), Kenta Nomura (Kobe University), Masami Mohri (Gifu University), Youji Fukuta (Kindai University), and Masakatu Morii (Kobe University)

Subliminal Channels in the Code-based Ring Signature Scheme .146
Bingsen Wang (Sun Yat-sen University), Zhuoran Zhang (Sun Yat-sen University), and Fangguo Zhang (Sun Yat-sen University)

Session 6: Privacy Protection

Learnable Audio Encryption for Untrusted Outsourcing Machine Learning Services .151
Po-Wen Chi (National Taiwan Normal University) and Pin-Hsin Hsiao (National Taiwan Normal University)

Password Strength Measurement without Password Disclosure .157
Taku Sugai (Toho University), Toshihiro Ohigashi (Tokai University), Yoshio Kakizaki (Tokyo Denki University), and Akira Kanaoka (Toho University)

Privacy Risk Evaluation of Re-Identification of Pseudonyms . 165
Yuma Takeuchi (Kanazawa University), Shogo Kitajima (Kanazawa University), Kazuya Fukushima (Kanazawa University), and Masahiro Mambo (Kanazawa University)

Author Index 173