2018 13th Asia Joint Conference on Information Security
AsiaJCIS 2018

Table of Contents

Message from the AsiaJCIS 2018 General Co-Chairs ................................................................. viii
Message from the AsiaJCIS 2018 Program Co-Chairs ................................................................. ix
AsiaJCIS 2018 Conference Organization ......................................................................................... x
AsiaJCIS 2018 Program Committee .............................................................................................. xii
AsiaJCIS 2018 Acknowledgments ................................................................................................... xiv

Session 1: Cyber Security

VISNU: A Novel Visualization Methodology of Security Events Optimized for a Centralized SOC ................................................................................................................................. 1
Taewoong Kwon (Korea Institute of Science and Technology Information),
Jung-suk Song (Korea Institute of Science and Technology Information),
Sangsu Choi (Korea Institute of Science and Technology Information),
Yunsoo Lee (Korea Institute of Science and Technology Information),
and Jinhak Park (Korea Institute of Science and Technology Information)

Protecting Struts 2 from OGNL Related Attacks by Using Servlet Filter ........................................ 8
Mariko Fujimoto (University of Tokyo), Wataru Matsuda (University of Tokyo), and Takuho Mitsunaga (University of Tokyo)

Time Series Analysis of Copy-and-Paste Impact on Android Application Security .............................. 15
Hironori Imai (Toho University) and Akira Kanaoka (Toho University)

Session 2: Cryptographic Protocols

Efficient Card-Based Cryptographic Protocols for the Millionaires' Problem Using Private Input Operations ......................................................................................................................... 23
Hibiki Ono (Kogakuin University) and Yoshifumi Manabe (Kogakuin University)

An Efficient Oblivious Transfer Protocol with Access Control ....................................................... 29
Yaqing Liao (Hubei University of Technology), Jing Zhou (Hubei University of Technology),
Yang Yang (Hubei University of Technology), and Ou Ruan (Hubei University of Technology)

Transformation between Attribute-Based Encryption and Key-Aggregate Cryptosystem .................... 35
Chun-I Fan (National Sun Yat-sen University), Yi-Fan Tseng (National Sun Yat-sen University),
Cheng-Yuan E (National Sun Yat-sen University), and Jheng-Jia Huang (National Sun Yat-sen University)
Session 3: Social Aspects

Toward a Resilient System: The Inspiration from Information Security Management Appliance ................................. 42
Ming Xu (Yunnan Police College), Yu Cheng (Yunnan Police College), and QiXin Yin (Yunnan Police College)

Helping Johnny to Search: Encrypted Search on Webmail System ................................................................. 47
Tatsuya Midorikawa (Toho University), Akihiro Tachikawa (Toho University), and Akira Kanaoka (Toho University)

An Algorithm Based on Influence to Predict Invisible Relationship ................................................................. 54
Junfeng Tian (Hebei University), LIZheng Xue (Hebei University), and Hongyun Cai (Hebei University)

Trust Elevation Scheme Based on Entropy-Specific Biometric Authentication Methods for the Financial Sector ........................................................................... 62
Ji Hye Kim (Soonchunhyang University), Mee Yeon Kim (Soonchunhyang University), and Heung Youl Youm (Soonchunhyang University)

Session 4: Low-Level Security

Power Attack and Protected Implementation on Lightweight Block Cipher SKINNY .................................................... 69
Jing Ge (Beijing Institute of Technology), Yifan Xu (Beijing Institute of Technology), Ruiqian Liu (Public Security Department of Henan Province), Enze Si (Beijing Institute of Technology), Ning Shang (Beijing Institute of Technology), and An Wang (Beijing Institute of Technology and Institute of Information Engineering, CAS)

Load Balancing Method Based on a Performance and Power Ratio ................................................................. 75
Junfeng Tian (Hebei University) and Yanwei Ma (Hebei University)

A Survey of Return-Oriented Programming Attack, Defense and Its Benign Use .................................................... 83
Jingyuan Wang (National University of Defence Technology), Peidai Xie (National University of Defence Technology), Yongjun Wang (National University of Defence Technology), and Zelin Rong (National University of Defence Technology)

Session 5: Analyzing Malicious Activities

Evaluating Disassembly-Code Based Similarity between IoT Malware Samples .................................................... 89
Ryoichi Isawa (National Institute of Information and Communications Technology), Tao Ban (National Institute of Information and Communications Technology), Ying Tie (Yokohama National University), Katsunari Yoshioka (Yokohama National University), and Daisuke Inoue (National Institute of Information and Communications Technology)

Development of White List Based Autonomous Evolution of Defense System for RAT Malware .................... 95
Tomohiro Shigemoto (Hitachi, Ltd.), Shota Fujii (Hitachi, Ltd.), Ichiro Kuriama (Hitachi, Ltd.), Tetsuro Kito (Hitachi, Ltd.), Hirofumi Nakakoji (Hitachi, Ltd.), Yasuhiro Fujii (Hitachi, Ltd.), and Hiroaki Kikuchi (Meiji University)
A Lightweight Host-Based Intrusion Detection Based on Process Generation Patterns  .................................. 102
Yu Tsuda (National Institute of Information and Communications Technology), Junji Nakazato (Fujitsu Laboratories Ltd.), Yaichiro Takagi (National Institute of Information and Communications Technology), Daisuke Inoue (National Institute of Information and Communications Technology), Koji Nakao (National Institute of Information and Communications Technology), and Kenjiro Terada (National Institute of Information and Communications Technology)

Constructing a Complete Timeline of a Security Incident by Aggregating Reports ............................. 109
Hiroki Kuzuno (SECOM), Shun Inagaki (SECOM), and Kenichi Magata (SECOM)

Author Index .................................................................................................................................................. 117