

Ho-won Kim · Dooho Choi (Eds.)

# Information Security Applications

16th International Workshop, WISA 2015  
Jeju Island, Korea, August 20–22, 2015  
Revised Selected Papers

# Contents

## Hardware Security

M-ORAM: A Matrix ORAM with Log $N$ Bandwidth Cost . . . . .	3
<i>Steven Gordon, Atsuko Miyaji, Chunhua Su, and Karin Sumongkayothin</i>	
Process Variation Evaluation Using RO PUF for Enhancing SCA-Resistant Dual-Rail Implementation . . . . .	16
<i>Wei He, Dirmanto Jap, and Alexander Herrmann</i>	
Compact Implementations of LEA Block Cipher for Low-End Microprocessors . . . . .	28
<i>Hwajeong Seo, Zhe Liu, Jongseok Choi, Taehwan Park, and Howon Kim</i>	
Compact Implementations of LSH. . . . .	41
<i>Taehwan Park, Hwajeong Seo, Zhe Liu, Jongseok Choi, and Howon Kim</i>	
Detection of Rogue Devices in WLAN by Analyzing RF Features and Indoor Location of the Device . . . . .	54
<i>Hyeokchan Kwon, Kwang-Il Lee, Gaeil An, Byung-Ho Chung, and Jeong-Nyeo Kim</i>	

## Cryptography

Security Analysis on RFID Mutual Authentication Protocol . . . . .	65
<i>You Sung Kang, Elizabeth O'Sullivan, Dooho Choi, and Maire O'Neill</i>	
How Much Randomness Can Be Extracted from Memoryless Shannon Entropy Sources? . . . . .	75
<i>Maciej Skorski</i>	
Two Types of Special Bases for Integral Lattices . . . . .	87
<i>Renzhang Liu and Yanbin Pan</i>	
Keyword Updatable PEKS . . . . .	96
<i>Hyun Sook Rhee and Dong Hoon Lee</i>	
On Partitioning Secret Data Based on Concept of Functional Safety . . . . .	110
<i>Seira Hidano and Shinsaku Kiyomoto</i>	
Unbounded Hierarchical Identity-Based Encryption with Efficient Revocation . . . . .	122
<i>Geumsook Ryu, Kwangsu Lee, Seunghwan Park, and Dong Hoon Lee</i>	

Publishing Graph Data with Subgraph Differential Privacy. . . . .	134
<i>Binh P. Nguyen, Hoa Ngo, Jihun Kim, and Jong Kim</i>	
An Improved Analysis of Broadcast Attacks on the GGH Cryptosystem . . . .	146
<i>Maoning Wang</i>	
<b>Side Channel Attacks and Countermeasures</b>	
Secure Binary Field Multiplication . . . . .	161
<i>Hwajeong Seo, Chien-Ning Chen, Zhe Liu, Yasuyuki Nogami, Taehwan Park, Jongseok Choi, and Howon Kim</i>	
An Improved Second-Order Power Analysis Attack Based on a New Refined Expecter: - Case Study on Protected AES -. . . . .	174
<i>Hyunjin Ahn, Neil Hanley, Maire O'Neill, and Dong-Guk Han</i>	
Various Threat Models to Circumvent Air-Gapped Systems for Preventing Network Attack . . . . .	187
<i>Eunchong Lee, Hyunsoo Kim, and Ji Won Yoon</i>	
An Improved Masking Scheme for S-Box Software Implementations. . . . .	200
<i>Sungjun Ahn and Dooho Choi</i>	
<b>Security and Threat Analysis</b>	
Open Sesame! Hacking the Password . . . . .	215
<i>Hwajeong Seo, Zhe Liu, Gyuwon Seo, Taehwan Park, Jongseok Choi, and Howon Kim</i>	
BurnFit: Analyzing and Exploiting Wearable Devices . . . . .	227
<i>Dongkwan Kim, Suwan Park, Kibum Choi, and Yongdae Kim</i>	
Security Analysis of FHSS-type Drone Controller . . . . .	240
<i>Hocheol Shin, Kibum Choi, Youngseok Park, Jaeyeong Choi, and Yongdae Kim</i>	
Encryption is Not Enough: Inferring User Activities on KakaoTalk with Traffic Analysis. . . . .	254
<i>Kyungwon Park and Hyoungshick Kim</i>	
<b>IoT Security</b>	
Challenges in Deploying CoAP Over DTLS in Resource Constrained Environments . . . . .	269
<i>Hyeokjin Kwon, Jiye Park, and Namhi Kang</i>	

A Study of OAuth 2.0 Risk Notification and Token Revocation from Resource Server . . . . .	281
<i>Jungsoo Park, Jinouk Kim, Minho Park, and Souhwan Jung</i>	
Cyber Security Considerations for Designing IoT-Based Control Systems . . .	288
<i>Kwangho Kim</i>	
Frying PAN: Dissecting Customized Protocol for Personal Area Network . . .	300
<i>Kibum Choi, Yunmok Son, Jangjun Lee, Suryeon Kim, and Yongdae Kim</i>	
Structured Design Approach for an Optimal Programmable Synchronous Security Processor. . . . .	313
<i>Mahmoud El-Hadidi, Hany El-Sayed, Heba Aslan, and Karim Osama</i>	
On Zero Knowledge Argument with PQT Soundness . . . . .	326
<i>Guifang Huang and Hongda Li</i>	
<b>Network Security</b>	
Performance Analysis of Multiple Classifier System in DoS Attack Detection . . . . .	339
<i>Bayu Adhi Tama and Kyung Hyune Rhee</i>	
Changes of Cybersecurity Legal System in East Asia: Focusing on Comparison Between Korea and Japan . . . . .	348
<i>Kwangho Kim, Sangdon Park, and Jongin Lim</i>	
Applying Recurrent Neural Network to Intrusion Detection with Hessian Free Optimization . . . . .	357
<i>Jihyun Kim and Howon Kim</i>	
<b>Application Security</b>	
Cost-Effective Modeling for Authentication and Its Application to Activity Tracker . . . . .	373
<i>Hiroya Susuki and Rie Shigetomi Yamaguchi</i>	
Fully Batch Processing Enabled Memory Integrity Verification Algorithm Based on Merkle Tree . . . . .	386
<i>Se Hwan Kim, Yonggon Kim, Ohmin Kwon, and Hyunsoo Yoon</i>	
Automatic Security Classification with Lasso . . . . .	399
<i>Paal E. Engelstad, Hugo Hammer, Kyrre Wahl Kongsgård, Anis Yazidi, Nils Agne Nordbotten, and Aleksander Bai</i>	
Constructing Efficient PAKE Protocols from Identity-Based KEM/DEM . . . .	411
<i>Kyu Young Choi, Jihoon Cho, Jung Yeon Hwang, and Taekyoung Kwon</i>	

How to Demonstrate Our Presence Without Disclosing Identity? Evidence  
from a Grouping-Proof Protocol . . . . . 423  
*Yunhui Zhuang, Gerhard P. Hancke, and Duncan S. Wong*

**Author Index** . . . . . 437