Contents

Malware Detection

ADAM: Automated Detection and Attribution of Malicious Webpages 3
Ahmed E. Kosba, Aziz Mohaisen, Andrew West, Trevor Tonn, and Huy Kang Kim

Detection of Heap-Spraying Attacks Using String Trace Graph 17
Jaehyeok Song, Jonghyuk Song, and Jong Kim

A Simple Yet Efficient Approach to Combat Transaction Malleability in Bitcoin 27
Ubaidullah Rajput, Fizza Abbas, Rasheed Hussain, Hasoo Eun, and Heekuck Oh

Mobile Security

Before Unrooting your Android Phone, Patching up Permission System First! 41
Zhongwen Zhang

I’ve Got Your Number: Harvesting Users’ Personal Data via Contacts Sync for the KakaoTalk Messenger 55
Eunhyun Kim, Kyungwon Park, Hyoungshick Kim, and Jaeseung Song

Analyzing Unnecessary Permissions Requested by Android Apps Based on Users’ Opinions 68
Jina Kang, Daehyun Kim, Hyoungshick Kim, and Jun Ho Huh

Vulnerability Analysis

Reconstructing and Visualizing Evidence of Artifact from Firefox SessionStorage 83
Shinichi Matsumoto, Yuya Onitsuka, Junpei Kawamoto, and Kouichi Sakurai

Analyzing Security of Korean USIM-Based PKI Certificate Service 95
Shinjo Park, Suwan Park, Insu Yun, Dongkwan Kim, and Yongdae Kim
AMAL: High-Fidelity, Behavior-Based Automated Malware Analysis and Classification .......................................................... 107
  Aziz Mohaisen and Omar Alrawi

Systematically Breaking Online WYSIWYG Editors .......................... 122
  Ashar Javed and Jörg Schwenk

Applied Cryptography

New Integrated Long-Term Glimpse of RC4 .............................. 137
  Ryoma Ito and Atsuko Miyaji

Improved Modular Multiplication for Optimal Prime Fields ............ 150
  Hwajeong Seo, Zhe Liu, Yasuyuki Nogami, Jongseok Choi, and Howon Kim

Network Security

Context Based Smart Access Control on BYOD Environments .......... 165
  Dongwan Kang, Joohyung Oh, and Chaetae Im

Scalable and Autonomous Mobile Device-Centric Cloud for Secured D2D Sharing .......................................................... 177
  Chao-Lieh Chen, Shen-Chien Chen, Chun-Ruei Chang, and Chia-Fei Lin

SecaaS Framework and Architecture: A Design of Dynamic Packet Control .... 190
  Ngoc-Tu Chau, Minh-Duong Nguyen, Seungwook Jung, and Souhwan Jung

Name Server Switching: Anomaly Signatures, Usage, Clustering, and Prediction ......................................................... 202
  Aziz Mohaisen, Mansurul Bhuiyan, and Yannis Labrou

A Trustless Broker Based Protocol to Discover Friends in Proximity-Based Mobile Social Networks .................................. 216
  Fizza Abbas, Ubaidullah Rajput, Rasheed Hussain, Hasoo Eun, and Heekuck Oh

Cryptography

Shared and Searchable Encrypted Data for Semi-trusted Servers with Controllable Sharing Property ..................................... 231
  Minkyu Joo and Pil Joong Lee

Fair Multi-signature ...................................................................... 244
  Pairat Thorncharoensri, Willy Susilo, and Yi Mu
An Efficient Variant of Boneh-Gentry-Hamburg’s Identity-Based Encryption
Without Pairing ................................................................. 257

Ibrahim Elashry, Yi Mu, and Willy Susilo

Joint Signature and Encryption in the Presence of Continual Leakage ....... 269
Fei Tang and Hongda Li

Hardware Security

Wireless Key Exchange Using Frequency Impairments ....................... 283
Jörn Müller-Quade and Antonio Sobreira de Almeida

Exploiting the Potential of GPUs for Modular Multiplication in ECC .... 295
Fangyu Zheng, Wuqiong Pan, Jingqiang Lin, Jiwu Jing, and Yuan Zhao

The Unified Hardware Design for GCM and SGCM .......................... 307
Yeoncheol Lee, Hwajeong Seo, and Howon Kim

Successful Profiling Attacks with Different Measurement Environments for Each Phase ........................................... 321
Yongdae Kim

Function Masking: A New Countermeasure Against Side Channel Attack ... 331
Taesung Kim, Sungjun Ahn, Seungkwang Lee, and Dooho Choi

Critical Infrastructure Security and Policy

Multivariate Statistic Approach to Field Specifications of Binary Protocols in SCADA System .................................................. 345
Seungoh Choi, Yeop Chang, Jeong-Han Yun, and Woonyon Kim

Packet Loss Consideration for Burst-Based Anomaly Detection in SCADA Network .................................................. 358
Kyoung-Ho Kim, Jeong-Han Yun, Yeop Chang, and Woonyon Kim

Defining Security Primitives for Eliciting Flexible Attack Scenarios Through CAPEC Analysis ........................................... 370
Ji-Yeong Kim and Hyung-Jong Kim

Advanced Security Assessment for Control Effectiveness .................. 383
Youngin You, Sangkyo Oh, and Kyungho Lee

Study on the Effectiveness of the Security Countermeasures Against Spear Phishing .................................................. 394
Misun Song, JunSeok Seo, and Kyungho Lee

Author Index ............................................................................ 405
Information Security Applications
15th International Workshop, WISA 2014, Jeju Island, Korea, August 25-27, 2014. Revised Selected Papers
Rhee, K.-H.; Yi, J.H. (Eds.)
2015, XIII, 406 p. 155 illus., Softcover
ISBN: 978-3-319-15086-4