

Contents

Malware Detection

ADAM: Automated Detection and Attribution of Malicious Webpages	3
<i>Ahmed E. Kosba, Aziz Mohaisen, Andrew West, Trevor Tonn, and Huy Kang Kim</i>	
Detection of Heap-Spraying Attacks Using String Trace Graph.	17
<i>Jaehyeok Song, Jonghyuk Song, and Jong Kim</i>	
A Simple Yet Efficient Approach to Combat Transaction Malleability in Bitcoin.	27
<i>Ubaidullah Rajput, Fizza Abbas, Rasheed Hussain, Hasoo Eun, and Heekuck Oh</i>	

Mobile Security

Before Unrooting your Android Phone, Patching up Permission System First!	41
<i>Zhongwen Zhang</i>	
I've Got Your Number: Harvesting Users' Personal Data via Contacts Sync for the KakaoTalk Messenger	55
<i>Eunhyun Kim, Kyungwon Park, Hyounghick Kim, and Jaeseung Song</i>	
Analyzing Unnecessary Permissions Requested by Android Apps Based on Users' Opinions	68
<i>Jina Kang, Daehyun Kim, Hyounghick Kim, and Jun Ho Huh</i>	

Vulnerability Analysis

Reconstructing and Visualizing Evidence of Artifact from Firefox SessionStorage	83
<i>Shinichi Matsumoto, Yuya Onitsuka, Junpei Kawamoto, and Kouichi Sakurai</i>	
Analyzing Security of Korean USIM-Based PKI Certificate Service	95
<i>Shinjo Park, Suwan Park, Insu Yun, Dongkwan Kim, and Yongdae Kim</i>	

AMAL: High-Fidelity, Behavior-Based Automated Malware Analysis and Classification	107
<i>Aziz Mohaisen and Omar Alrawi</i>	

Systematically Breaking Online WYSIWYG Editors	122
<i>Ashar Javed and Jörg Schwenk</i>	

Applied Cryptography

New Integrated Long-Term Glimpse of RC4	137
<i>Ryoma Ito and Atsuko Miyaji</i>	

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

Network Security

Context Based Smart Access Control on BYOD Environments	165
<i>Dongwan Kang, Joohyung Oh, and Chaetae Im</i>	

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

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

Name Server Switching: Anomaly Signatures, Usage, Clustering, and Prediction	202
<i>Aziz Mohaisen, Mansurul Bhuiyan, and Yannis Labrou</i>	

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

Cryptography

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

Fair Multi-signature.	244
<i>Pairat Thorncharoensri, Willy Susilo, and Yi Mu</i>	

An Efficient Variant of Boneh-Gentry-Hamburg's Identity-Based Encryption Without Pairing	257
<i>Ibrahim Elashry, Yi Mu, and Willy Susilo</i>	
Joint Signature and Encryption in the Presence of Continual Leakage	269
<i>Fei Tang and Hongda Li</i>	
Hardware Security	
Wireless Key Exchange Using Frequency Impairments	283
<i>Jörn Müller-Quade and Antonio Sobreira de Almeida</i>	
Exploiting the Potential of GPUs for Modular Multiplication in ECC	295
<i>Fangyu Zheng, Wuqiong Pan, Jingqiang Lin, Jiwu Jing, and Yuan Zhao</i>	
The Unified Hardware Design for GCM and SGCM	307
<i>Yeoncheol Lee, Hwajeong Seo, and Howon Kim</i>	
Successful Profiling Attacks with Different Measurement Environments for Each Phase	321
<i>Yongdae Kim</i>	
Function Masking: A New Countermeasure Against Side Channel Attack . . .	331
<i>Taesung Kim, Sungjun Ahn, Seungkwang Lee, and Dooho Choi</i>	
Critical Infrastructure Security and Policy	
Multivariate Statistic Approach to Field Specifications of Binary Protocols in SCADA System	345
<i>Seungoh Choi, Yeop Chang, Jeong-Han Yun, and Woonyon Kim</i>	
Packet Loss Consideration for Burst-Based Anomaly Detection in SCADA Network	358
<i>Kyoung-Ho Kim, Jeong-Han Yun, Yeop Chang, and Woonyon Kim</i>	
Defining Security Primitives for Eliciting Flexible Attack Scenarios Through CAPEC Analysis	370
<i>Ji-Yeon Kim and Hyung-Jong Kim</i>	
Advanced Security Assessment for Control Effectiveness	383
<i>Youngin You, Sangkyo Oh, and Kyungho Lee</i>	
Study on the Effectiveness of the Security Countermeasures Against Spear Phishing	394
<i>Misun Song, JunSeok Seo, and Kyungho Lee</i>	
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