

Contents

Does Query Blocking Improve DNS Privacy? Quantifying Privacy Under Partial Blocking Deployment	1
<i>Aziz Mohaisen, Ah Reum Kang, and Kui Ren</i>	
Measuring and Analyzing Trends in Recent Distributed Denial of Service Attacks	15
<i>An Wang, Aziz Mohaisen, Wentao Chang, and Songqing Chen</i>	
SD-OVS: SYN Flooding Attack Defending Open vSwitch for SDN	29
<i>Xinyu Liu, Beumjin Cho, and Jong Kim</i>	
Slowloris DoS Countermeasure over WebSocket.	42
<i>Jongseok Choi, Jong-gyu Park, Shinwook Heo, Namje Park, and Howon Kim</i>	
Detecting Encrypted Traffic: A Machine Learning Approach	54
<i>Seunghun Cha and Hyounghick Kim</i>	
Features for Behavioral Anomaly Detection of Connectionless Network Buffer Overflow Attacks	66
<i>Ivan Homoliak, Ladislav Sulak, and Petr Hanacek</i>	
A Behavior-Based Online Engine for Detecting Distributed Cyber-Attacks. . .	79
<i>Yaokai Feng, Yoshiaki Hori, and Kouichi Sakurai</i>	
Influence Evaluation of Centrality-Based Random Scanning Strategy on Early Worm Propagation Rate	90
<i>Su-kyung Kwon, Bongsoo Jang, Byoung-Dai Lee, Younghae Do, Hunki Baek, and Yoon-Ho Choi</i>	
Analysis on South Korean Cybersecurity Readiness Regarding North Korean Cyber Capabilities	102
<i>Jeong Yoon Yang, So Jeong Kim, and Il Seok Oh(Luke)</i>	
A Practical Analysis of TLS Vulnerabilities in Korea Web Environment	112
<i>Jongmin Jeong, Hyunsoo Kwon, Hyungjune Shin, and Junbeom Hur</i>	
Doppelganger in Bitcoin Mining Pools: An Analysis of the Duplication Share Attack.	124
<i>Yujin Kwon, Dohyun Kim, Yunmok Son, Jaeyeong Choi, and Yongdae Kim</i>	

Detecting Impersonation Attack in WiFi Networks Using Deep Learning Approach	136
<i>Muhamad Erza Aminanto and Kwangjo Kim</i>	
Pay as You Want: Bypassing Charging System in Operational Cellular Networks	148
<i>Hyunwook Hong, Hongil Kim, Byeongdo Hong, Dongkwan Kim, Hyunwoo Choi, Eunkyu Lee, and Yongdae Kim</i>	
Towards Automated Exploit Generation for Embedded Systems	161
<i>Matthew Ruffell, Jin B. Hong, Hyounghick Kim, and Dong Seong Kim</i>	
Empirical Analysis of SSL/TLS Weaknesses in Real Websites: Who Cares?	174
<i>Sanghak Oh, Eunsoo Kim, and Hyounghick Kim</i>	
Development of Information Security Management Assessment Model for the Financial Sector	186
<i>Eun Oh, Tae-Sung Kim, and Tae-Hee Cho</i>	
A Practical Approach to Constructing Triple-Blind Review Process with Maximal Anonymity and Fairness	198
<i>Jisoo Jung, Joo-Im Kim, and Ji Won Yoon</i>	
GIS Vector Map Perceptual Encryption Scheme Using Geometric Objects . . .	210
<i>P.N. Giao, Suk-Hwan Lee, Kwang-Seok Moon, and Ki-Ryong Kwon</i>	
Efficient Scalar Multiplication for Ate Based Pairing over KSS Curve of Embedding Degree 18	221
<i>Md. Al-Amin Khandaker, Yasuyuki Nogami, Hwajeong Seo, and Sylvain Duquesne</i>	
LRCRYPT: Leakage-Resilient Cryptographic System (Design and Implementation)	233
<i>Xiaoqi Yu, Nairen Cao, Gongxian Zeng, Ruoqing Zhang, and Siu-Ming Yiu</i>	
Revocable Group Signatures with Compact Revocation List Using Vector Commitments	245
<i>Shahidatul Sadiah and Toru Nakanishi</i>	
The Quantum-Safe Revolution	258
<i>Jean-Charles Faugère and Ludovic Perret</i>	
New Integral Characteristics of KASUMI Derived by Division Property	267
<i>Nobuyuki Sugio, Yasutaka Igarashi, Toshinobu Kaneko, and Kenichi Higuchi</i>	

On Pseudorandomness in Stateless Sources	280
<i>Maciej Skorski</i>	
Algebraic Degree Estimation for Integral Attack by Randomized Algorithm.	292
<i>Haruhisa Kosuge and Hidema Tanaka</i>	
Applications of Soft Computing in Cryptology	305
<i>Stjepan Picek</i>	
Parallel Implementations of LEA, Revisited	318
<i>Hwajeong Seo, Taehwan Park, Shinwook Heo, Gyuwon Seo, Bongjin Bae, Zhi Hu, Lu Zhou, Yasuyuki Nogami, Youwen Zhu, and Howon Kim</i>	
Multi-precision Squaring for Public-Key Cryptography on Embedded Microprocessors, a Step Forward.	331
<i>Hwajeong Seo, Taehwan Park, Shinwook Heo, Gyuwon Seo, Bongjin Bae, Lu Zhou, and Howon Kim</i>	
A Secure and Privacy Preserving Iris Biometric Authentication Scheme with Matrix Transformation	341
<i>Abayomi Jegede, Nur Izura Udzir, Azizol Abdullah, and Ramlan Mahmod</i>	
Exploration of 3D Texture and Projection for New CAPTCHA Design	353
<i>Simon S. Woo, Jingul Kim, Duoduo Yu, and Beomjun Kim</i>	
A Study on Feature of Keystroke Dynamics for Improving Accuracy in Mobile Environment	366
<i>Sung-Hoon Lee, Jong-Hyuk Roh, Soohyung Kim, and Seung-Hun Jin</i>	
Geocasting-Based Almanac Synchronization Method for Secure Maritime Cloud	376
<i>Donghyeok Lee and Namje Park</i>	
The Vessel Trajectory Mechanism for Marine Accidents Analysis.	388
<i>Seung-hee Oh, Byung-gil Lee, and Byungho Chung</i>	
Author Index	397

Information Security Applications

17th International Workshop, WISA 2016, Jeju Island,
Korea, August 25-27, 2016, Revised Selected Papers

Choi, D.; Guilley, S. (Eds.)

2017, XI, 398 p. 157 illus., Softcover

ISBN: 978-3-319-56548-4