# Contents

Does Query Blocking Improve DNS Privacy? Quantifying Privacy Under Partial Blocking Deployment ......................................................... 1  
  *Aziz Mohaisen, Ah Reum Kang, and Kui Ren*

Measuring and Analyzing Trends in Recent Distributed Denial of Service Attacks .................................................................................................. 15  
  *An Wang, Aziz Mohaisen, Wentao Chang, and Songqing Chen*

SD-OVS: SYN Flooding Attack Defending Open vSwitch for SDN ......................................................... 29  
  *Xinyu Liu, Beumjin Cho, and Jong Kim*

Slowloris DoS Countermeasure over WebSocket ...................................................... 42  
  *Jongseok Choi, Jong-gyu Park, Shinwook Heo, Namje Park, and Howon Kim*

Detecting Encrypted Traffic: A Machine Learning Approach ...................................................... 54  
  *Seunghun Cha and Hyoungshick Kim*

Features for Behavioral Anomaly Detection of Connectionless Network Buffer Overflow Attacks ...................................................... 66  
  *Ivan Homoliak, Ladislav Sulak, and Petr Hanacek*

A Behavior-Based Online Engine for Detecting Distributed Cyber-Attacks ...................................................... 79  
  *Yaokai Feng, Yoshiaki Hori, and Kouichi Sakurai*

Influence Evaluation of Centrality-Based Random Scanning Strategy on Early Worm Propagation Rate ...................................................... 90  
  *Su-kyung Kown, Bongsoo Jang, Byoung-Dai Lee, Younghae Do, Hunki Baek, and Yoon-Ho Choi*

Analysis on South Korean Cybersecurity Readiness Regarding North Korean Cyber Capabilities ...................................................... 102  
  *Jeong Yoon Yang, So Jeong Kim, and Il Seok Oh(Luke)*

A Practical Analysis of TLS Vulnerabilities in Korea Web Environment ...................................................... 112  
  *Jongmin Jeong, Hyunsoo Kwon, Hyungjune Shin, and Junbeom Hur*

Doppelganger in Bitcoin Mining Pools: An Analysis of the Duplication Share Attack ...................................................... 124  
  *Yujin Kwon, Dohyun Kim, Yunmok Son, Jaeyeong Choi, and Yongdae Kim*
Detecting Impersonation Attack in WiFi Networks Using Deep Learning Approach .............................................................. 136
    Muhamad Erza Aminanto and Kwangjo Kim

Pay as You Want: Bypassing Charging System in Operational Cellular Networks ......................................................... 148
    Hyunwook Hong, Hongil Kim, Byeongdo Hong, Dongkwan Kim, Hyunwoo Choi, Eunkyu Lee, and Yongdae Kim

Towards Automated Exploit Generation for Embedded Systems .................. 161
    Matthew Ruffell, Jin B. Hong, Hyungshick Kim, and Dong Seong Kim

Empirical Analysis of SSL/TLS Weaknesses in Real Websites: Who Cares? .............................................................. 174
    Sanghak Oh, Eunsoo Kim, and Hyungshick Kim

Development of Information Security Management Assessment Model for the Financial Sector ........................................ 186
    Eun Oh, Tae-Sung Kim, and Tae-Hee Cho

A Practical Approach to Constructing Triple-Blind Review Process with Maximal Anonymity and Fairness ....................... 198
    Jisoo Jung, Joo-Im Kim, and Ji Won Yoon

GIS Vector Map Perceptual Encryption Scheme Using Geometric Objects ... 210
    P.N. Giao, Suk-Hwan Lee, Kwang-Seok Moon, and Ki-Ryong Kwon

Efficient Scalar Multiplication for Ate Based Pairing over KSS Curve of Embedding Degree 18 ........................................ 221
    Md. Al-Amin Khandaker, Yasuyuki Nogami, Hwajeong Seo, and Sylvain Duquesne

LRCRYPT: Leakage-Resilient Cryptographic System (Design and Implementation) ........................................................ 233
    Xiaoqi Yu, Nairen Cao, Gongxian Zeng, Ruqing Zhang, and Siu-Ming Yiu

Revocable Group Signatures with Compact Revocation List Using Vector Commitments ............................................... 245
    Shahidatul Sadiah and Toru Nakanishi

The Quantum-Safe Revolution .................................................. 258
    Jean-Charles Faugère and Ludovic Perret

New Integral Characteristics of KASUMI Derived by Division Property ....... 267
    Nobuyuki Sugio, Yasutaka Igarashi, Toshinobu Kaneko, and Kenichi Higuchi
On Pseudorandomness in Stateless Sources .................................................. 280
Maciej Skorski

Algebraic Degree Estimation for Integral Attack by Randomized Algorithm ..................................................... 292
Haruhisa Kosuge and Hidema Tanaka

Applications of Soft Computing in Cryptology ................................. 305
Stjepan Picek

Parallel Implementations of LEA, Revisited ................................. 318
Hwajeong Seo, Taehwan Park, Shinwook Heo, Gyuwon Seo, Bongjin Bae, Zhi Hu, Lu Zhou, Yasuyuki Nogami, Youwen Zhu, and Howon Kim

Multi-precision Squaring for Public-Key Cryptography on Embedded Microprocessors, a Step Forward......................... 331
Hwajeong Seo, Taehwan Park, Shinwook Heo, Gyuwon Seo, Bongjin Bae, Lu Zhou, and Howon Kim

A Secure and Privacy Preserving Iris Biometric Authentication Scheme with Matrix Transformation ................................. 341
Abayomi Jegede, Nur Izura Udzir, Azizol Abdullah, and Ramlan Mahmod

Exploration of 3D Texture and Projection for New CAPTCHA Design .. 353
Simon S. Woo, Jingul Kim, Duoduo Yu, and Beomjun Kim

A Study on Feature of Keystroke Dynamics for Improving Accuracy in Mobile Environment .................................................. 366
Sung-Hoon Lee, Jong-Hyuk Roh, Soohyung Kim, and Seung-Hun Jin

Geocasting-Based Almanac Synchronization Method for Secure Maritime Cloud .................................................. 376
Donghyeok Lee and Namje Park

The Vessel Trajectory Mechanism for Marine Accidents Analysis .......... 388
Seung-hee Oh, Byung-gil Lee, and Byungho Chung

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