Contents

Invited Paper

While Mobile Encounters with Clouds .................................................. 3
Man Ho Au, Kaitai Liang, Joseph K. Liu, and Rongxing Lu

Authentication Mechanism

Multi-device Anonymous Authentication .............................................. 21
Kamil Kluczniak, Jianfeng Wang, Xiaofeng Chen,
and Miroslaw Kutyłowski

A Mobile Device-Based Antishoulder-Surfing Identity Authentication
Mechanism ................................................................. 37
Jia-Ning Luo, Ming-Hour Yang, and Cho-Luen Tsai

Mutual Authentication with Anonymity for Roaming Service with Smart
Cards in Wireless Communications ........................................... 47
Chang-Shiun Liu, Li Xu, Limei Lin, Min-Chi Tseng, Shih-Ya Lin,
and Hung-Min Sun

Cloud Computing Security

Efficient Fine-Grained Access Control for Secure Personal Health Records
in Cloud Computing ............................................................. 65
Kai He, Jian Weng, Joseph K. Liu, Wanlei Zhou, and Jia-Nan Liu

An Energy-Efficient Task Scheduling Heuristic Algorithm Without Virtual
Machine Migration in Real-Time Cloud Environments ....................... 80
Yi Zhang, Liuhua Chen, Haiying Shen, and Xiaohui Cheng

An Infrastructure-Based Framework for the Alleviation of JavaScript
Worms from OSN in Mobile Cloud Platforms ............................... 98
Shashank Gupta and Brij B. Gupta

Data Mining for Security Application

Ld-CNNs: A Deep Learning System for Structured Text Categorization
Based on LDA in Content Security ........................................... 113
Jinshuo Liu, Yabo Xu, Juan Deng, Lina Wang, and Lanxin Zhang
Realtime DDoS Detection in SIP Ecosystems: Machine Learning Tools of the Trade .................................................. 126
Zisis Tsiatsikas, Dimitris Geneiatakis, Georgios Kambourakis, and Stefanos Gritzalis

Digital Signature

Two-in-One Oblivious Signatures Secure in the Random Oracle Model ...... 143
Raylin Tso

A New Transitive Signature Scheme ..................................... 156
Chao Lin, Fei Zhu, Wei Wu, Kaitai Liang, and Kim-Kwang Raymond Choo

Privacy-Preserving Technologies

Privacy-Preserving Profile Matching Protocol Considering Conditions .... 171
Yosuke Ishikuro and Kazumasa Omote

Privacy Preserving Credit Systems ...................................... 184
Sherman S.M. Chow, Russell W.F. Lai, Xiuhua Wang, and Yongjun Zhao

Evading System-Calls Based Intrusion Detection Systems .................. 200
Ishai Rosenberg and Ehud Gudes

Network Security and Forensic

HeapRevolver: Delaying and Randomizing Timing of Release of Freed Memory Area to Prevent Use-After-Free Attacks ......................... 219
Toshihiro Yamauchi and Yuta Ikegami

Timestamp Analysis for Quality Validation of Network Forensic Data ...... 235
Nikolai Hampton and Zubair A. Baig

Searchable Encryption

An Efficient Secure Channel Free Searchable Encryption Scheme with Multiple Keywords .................................................. 251
Tingting Wang, Man Ho Au, and Wei Wu

Searchable Symmetric Encryption Supporting Queries with Multiple-Character Wildcards ...................................... 266
Fangming Zhao and Takashi Nishide

A System of Shareable Keyword Search on Encrypted Data .................. 283
Wei-Ting Lu, Wei Wu, Shih-Ya Lin, Min-Chi Tseng, and Hung-Min Sun
Security Policy and Access Control

An Attribute-Based Protection Model for JSON Documents .................. 303
                     Prosunjit Biswas, Ravi Sandhu, and Ram Krishnan

The GURA_G Administrative Model for User and Group Attribute Assignment .............................................................. 318
                     Maanak Gupta and Ravi Sandhu

On the Relationship Between Finite Domain ABAM and PreUCON_A ........ 333
                     Asma Alshehri and Ravi Sandhu

Security Protocols

MD-\(\mathcal{V}_{\text{Matrix}}\): An Efficient Scheme for Publicly Verifiable Computation of Outsourced Matrix Multiplication .................................................. 349
                     Gang Sheng, Chunming Tang, Wei Gao, and Ying Yin

Expressive Rating Scheme by Signatures with Predications on Ratees .... 363
                     Hiroaki Anada, Sushmita Ruj, and Kouichi Sakurai

Symmetric Key Cryptography

A New Adaptable Construction of Modulo Addition with Scalable Security for Stream Ciphers ................................................................. 383
                     Min Hsuan Cheng, Reza Sedaghat, and Prathap Siddavaatam

Extension of Meet-in-the-Middle Technique for Truncated Differential and Its Application to RoadRunneR .................................................... 398
                     Qianqian Yang, Lei Hu, Siwei Sun, and Ling Song

System Security

DF-ORAM: A Practical Dummy Free Oblivious RAM to Protect Outsourced Data Access Pattern .......................... 415
                     Qiumao Ma, Wensheng Zhang, and Jinsheng Zhang

PMFA: Toward Passive Message Fingerprint Attacks on Challenge-Based Collaborative Intrusion Detection Networks .................. 433
                     Wenjuan Li, Weizhi Meng, Lam-For Kwok, and Horace Ho Shing Ip

Iris Cancellable Template Generation Based on Indexing-First-One Hashing ... 450
                     Yen-Lung Lai, Zhe Jin, Bok-Min Goi, Tong-Yuen Chai, and Wun-She Yap
Web Security

Detecting Malicious URLs Using Lexical Analysis .......................... 467
Mohammad Saiful Islam Mamun, Mohammad Ahmad Rathore,
Arash Habibi Lashkari, Natalia Stakhanova, and Ali A. Ghorbani

Gatekeeping Behavior Analysis for Information Credibility Assessment
on Weibo. ......................................................... 483
Bailin Xie, Yu Wang, Chao Chen, and Yang Xiang

Data Mining for Security Application (Short Paper)

Finding Anomalies in SCADA Logs Using Rare Sequential Pattern Mining ... 499
Anisur Rahman, Yue Xu, Kenneth Radke, and Ernest Foo

Provable Security (Short Paper)

Improved Security Proof for Modular Exponentiation Bits ............... 509
Kewei Lv, Wenjie Qin, and Ke Wang

Security Protocol (Short Paper)

Secure Outsourced Bilinear Pairings Computation for Mobile Devices .. 519
Tomasz Hyla and Jerzy Pejaś

The Design and Implementation of Multi-dimensional Bloom Filter
Storage Matrix ....................................................... 530
Fei Xu, Pinxin Liu, Jianfeng Yang, and Jing Xu

Author Index ...................................................... 539
Network and System Security
10th International Conference, NSS 2016, Taipei, Taiwan, September 28-30, 2016, Proceedings
Chen, J.; Piuri, V.; Su, C.; Yung, M. (Eds.)
2016, XIV, 540 p. 128 illus., Softcover
ISBN: 978-3-319-46297-4