Table of Contents

Greetings from General Co-chairs ...........................................................................................................viii
Greetings from Program Co-chairs ...........................................................................................................ix
Organizing Committee .................................................................................................................................x
Acknowledgments .....................................................................................................................................xiii

Cryptographic Protocol
Detect Zero by Using Symmetric Homomorphic Encryption .................................................................1
D.J. Guan, Chen-Yu Tsai, and E.S. Zhuang
Secure Certificateless Signature Scheme Supporting Batch Verification ..............................................8
Chun-I Fan, Pei-Hsiu Ho, Jheng-Jia Huang, and Yi-Fan Tseng

Authentication
On Zero-Knowledge Identification Based on Q-ary Syndrome Decoding ..............................................12
Rong Hu, Kirill Morozov, and Tsuyoshi Takagi
An Efficient and Practical Fair Buyer-Anonymity Exchange Scheme Using Bilinear Pairings ................19
Wen-Sheng Juang
An Efficient and Provable Secure Security-Mediated Identity-Based Identification Scheme ..................27
Ji-Jian Chin, Rouzbeh Behnia, Swee-Huay Heng, and Raphael C.-Wei Phan

Network Security I
Cryptanalysis on RFID Authentications Using Minimum Disclosure Approach ....................................33
Hung Yu Chien
Adaptive Feature-Weighted Alert Correlation System Applicable in Cloud Environment ......................41
Chih-Hung Wang and Ji-Min Yang
Detecting and Preventing Drive-By Download Attack via Participative Monitoring of the Web

Takashi Matsunaka, Junpei Urakawa, and Ayumu Kubota

Search Engine Based Investigation on Misconfiguration of Zone Transfer

Yin Minn Pa Pa, Katsunari Yoshioka, and Tsutomu Matsumoto

Network Security II

Detecting HTTP-Based Botnet Based on Characteristic of the C & C Session Using by SVM

Kazuma Yamauchi, Yoshiaki Hori, and Kouichi Sakurai

Efficient Malware Packer Identification Using Support Vector Machines with Spectrum Kernel

Tao Ban, Ryoichi Isawa, Shanqing Guo, Daisuke Inoue, and Koji Nakao

Suspicious URL Filtering Based on Logistic Regression with Multi-view Analysis

Ke-Wei Su, Kuo-Ping Wu, Hahn-Ming Lee, and Te-En Wei

Preventing Abuse of Cookies Stolen by XSS

Hiroya Takahashi, Kenji Yasunaga, Masahiro Mambo, Kwangjo Kim, and Heung Youl Youn

Digital Forensics

Design and Implementation of Digital Forensic Software for iPhone

Chung-Nan Chen, Raylin Tso, and Chung-Huang Yang

Memory Forensics for Key Evidence Investigations in Case Illustrations

Ya-Ting Chang, Min-Ju Chung, Chin-Feng Lee, Cheng-Ta Huang, and Shiuh-Jeng Wang

Histogram-Based Reversible Information Hiding Improved by Prediction with the Variance to Enhance Image Quality

Chi-Yao Weng, Cheng-Hsing Yang, Chun-I Fan, Kuan-Liang Liu, and Hung-Min Sun

International Standard/Others

Formal Analysis of ISO/IEC 9798-2 Authentication Standard Using AVISPA

Sheikh Ziauddin and Bruno Martin

Present Cyber Threat Management (Methodologies to Mitigate Evolving Cyber-Attacks)

Bright Gameli Mawudor

Automatic Adding License Management Functionality for Android Applications

Ming-Chih Kao, Wen-Chung Kuo, and Yu-Hsuan Pan