

2015 10th Asia Joint Conference on Information Security

(AsiaJCIS 2015)

Kaohsiung City, Taiwan
24 – 26 May 2015



IEEE Catalog Number: CFP1533T-POD
ISBN: 978-1-4799-1990-1

2015 10th Asia Joint Conference on Information Security

AsiaJCIS 2015

Table of Contents

Message from General Co-chairs	viii
Message from Program Co-chairs.....	ix
Conference Organization	x
Program Committee.....	xii
Acknowledgments.....	xiv

Anonymity and Privacy

An Enhanced Secure Anonymous Authentication Scheme Based on Smart Cards and Biometrics for Multi-server Environments	1
<i>Wen-Chung Kuo, Hong-Ji Wei, Yu-Hui Chen, and Jiin-Chiou Cheng</i>	
On the Traceability of the Accountable Anonymous Channel	6
<i>Tomoaki Kosugi, Tomoki Hayafuji, and Masahiro Mambo</i>	
Privacy-Preserved Key Agreement with User Authentication	12
<i>Chien-Lung Hsu and Tzu-Wei Lin</i>	

Data Security

Encrypted Data Deduplication in Cloud Storage	18
<i>Chun-I Fan, Shi-Yuan Huang, and Wen-Che Hsu</i>	
Attribute-Based Proxy Re-encryption with Dynamic Membership	26
<i>Chun-I Fan, Chien-Nan Wu, Chun-Hung Chen, Yi-Fan Tseng, and Cheng-Chun Feng</i>	
An Efficient Detection Algorithm for Copy-Move Forgery	33
<i>Chen-Ming Hsu, Jen-Chun Lee, and Wei-Kuei Chen</i>	

Mobile and Wireless Security

The Cryptanalysis of WPA & WPA2 in the Rule-Based Brute Force Attack, an Advanced and Efficient Method	37
<i>Chia-Mei Chen and Tien-Ho Chang</i>	
De-synchronization Attack on Quadratic Residues-Based RFID Ownership Transfer	42
<i>Hung-Yu Chien</i>	
Intelligent Display Auto-Lock Scheme for Mobile Devices	48
<i>Nai-Wei Lo, Chi-Kai Yu, and Chao Yang Hsu</i>	
Hash-Based Anonymous Secure Routing Protocol in Mobile Ad Hoc Networks	55
<i>Nai-Wei Lo, Meng-Chih Chiang, and Chao Yang Hsu</i>	
Secure and Lightweight Authentication Protocol for NFC Tag Based Services	63
<i>Jonghyun Baek and Heung Youl Youm</i>	

Privacy Preserving Analysis

Discovery of De-identification Policies Considering Re-identification Risks and Information Loss	69
<i>He-Ming Ruan, Ming-Hwa Tsai, Yen-Nun Huang, Yen-Hua Liao, and Chin-Laung Lei</i>	
Privacy Preserved Rule-Based Risk Analysis through Secure Multi-party Computation	77
<i>Yu Liu, Nasato Goto, Akira Kanaoka, and Eiji Okamoto</i>	
Privacy-Preserving Epidemiological Analysis for a Distributed Database of Hospitals	85
<i>Hiroaki Kikuchi, Hideki Hashimoto, and Hideo Yasunaga</i>	

Secure Payment

A Secure and Efficient Smartphone Payment Scheme in IoT/Cloud Environments	91
<i>Jheng-Jia Huang, Wen-Sheng Juang, and Chun-I Fan</i>	
Delegation-Based Roaming Payment Protocol with Location and Purchasing Privacy Protection	97
<i>Chih Hung Wang and Hsiao Chien Sung</i>	
Secure Electronic Coupons	104
<i>Chin-Chen Chang, Iuon-Chang Lin, and Yi-Lun Chi</i>	

Symmetric Key Encryption and Digital Signature

Preliminary Design of a Novel Lightweight Authenticated Encryption Scheme Based on the Sponge Function	110
<i>Hakju Kim and Kwangjo Kim</i>	
Constructions of Fail-Stop Signatures for Multi-signer Setting	112
<i>Nobuaki Kitajima, Naoto Yanai, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto</i>	
A Provable Watermark-Based Copyright Protection Scheme	124
<i>Pei-Yih Ting, Shao-Da Huang, Tzong-Sun Wu, and Han-Yu Lin</i>	

System Security

iF2: An Interpretable Fuzzy Rule Filter for Web Log Post-Compromised Malicious Activity Monitoring	130
<i>Chih-Hung Hsieh, Yu-Siang Shen, Chao-Wen Li, and Jain-Shing Wu</i>	
Malware Function Classification Using APIs in Initial Behavior	138
<i>Naoto Kawaguchi and Kazumasa Omote</i>	
An Approach to Predict Drive-by-Download Attacks by Vulnerability Evaluation and Opcode	145
<i>Takashi Adachi and Kazumasa Omote</i>	
A Proposal for Detecting Distributed Cyber-Attacks Using Automatic Thresholding	152
<i>Yaokai Feng, Yoshiaki Hori, and Kouichi Sakurai</i>	
Author Index	160