

2016 11th Asia Joint Conference on Information Security (AsiaJCIS 2016)

**Fukuoka, Japan
4 – 5 August 2016**



**IEEE Catalog Number: CFP1633T-POD
ISBN: 978-1-5090-2286-1**

**Copyright © 2016 by the Institute of Electrical and Electronics Engineers, Inc
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

******This publication is a representation of what appears in the IEEE Digital Libraries. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP1633T-POD
ISBN (Print-On-Demand):	978-1-5090-2286-1
ISBN (Online):	978-1-5090-2285-4

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2016 11th Asia Joint Conference on Information Security

AsiaJCIS 2016

Table of Contents

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

IoT Security

Securing Smart Meters Data for AMI Using RBAC	1
<i>Ezedin Barka, Nedaa Al Hussien, and Khaled Shuaib</i>	
Home Network Security: Modelling Power Consumption to Detect and Prevent Attacks on Homenet Routers	9
<i>Bilhanan Silverajan, Markku Vajaranta, and Antti Kolehmainen</i>	
Implementation Experiences and Design Challenges for Resilient SDN Based Secure WAN Overlays	17
<i>Markku Vajaranta, Joona Kannisto, and Jarmo Harju</i>	

Privacy and Anonymity

NFC-based Mobile Payment Protocol with User Anonymity	24
<i>Shang-Wen Chen and Raylin Tso</i>	
Partial Server Side Parameter Selection in Private Information Retrieval	31
<i>Thomas Vannet and Noboru Kunihiro</i>	
An Identity Preserving Access Control Scheme with Flexible System Privilege Revocation in Cloud Computing	39
<i>Rohit Ahuja, Sraban Kumar Mohanty, and Kouichi Sakurai</i>	
Efficient Privacy-Preserving Logistic Regression with Iteratively Re-weighted Least Squares	48
<i>Hiroaki Kikuchi, Hideo Yasunaga, Hiroki Matsui, and Chun-I Fan</i>	

Honeypot

Observing Hidden Service Directory Spying with a Private Hidden Service Honeynet	55
<i>Juha Nurmi, Joona Kannisto, and Markku Vajaranta</i>	
Wamber: Defending Web Sites on Hosting Services with Self-Learning Honeypots	60
<i>Satomi Saito, Satoru Torii, Katsunari Yoshioka, and Tsutomu Matsumoto</i>	
How to Design Practical Client Honeypots Based on Virtual Environment	67
<i>Jin-Hak Park, Jang-Won Choi, and Jung-Suk Song</i>	

Network-Based Attack Detection

Defense Joint Attacks Based on Stochastic Discrete Sequence Anomaly Detection	74
<i>Chia-Mei Chen, Gu-Hsin Lai, and Pong-Yu Young</i>	
A Machine Learning Based Approach for Detecting DRDoS Attacks and Its Performance Evaluation	80
<i>Yuxuan Gao, Yaokai Feng, Junpei Kawamoto, and Kouichi Sakurai</i>	
Classifier Ensemble Design with Rotation Forest to Enhance Attack Detection of IDS in Wireless Network	87
<i>Bayu Adhi Tama and Kyung-Hyune Rhee</i>	
Migrant Attack: A Multi-resource DoS Attack on Cloud Virtual Machine Migration Schemes	92
<i>Jia-Rung Yeh, Hsu-Chun Hsiao, and Ai-Chun Pang</i>	
SDNort: A Software Defined Network Testing Framework Using Openflow	100
<i>Po-Wen Chi, Ming-Hung Wang, Che-Wei Lin, Jing-Wei Guo, Chin-Laung Lei, and Nen-Fu Huang</i>	

Cryptography and Data Security

($\{1,3\},n$) Hierarchical Secret Sharing Scheme Based on XOR Operations for a Small Number of Indispensable Participants	108
<i>Koji Shima and Hiroshi Doi</i>	
New Conditional Differential Cryptanalysis for NLFSR-based Stream Ciphers and Application to Grain v1	115
<i>Yuhei Watanabe, Yosuke Todo, and Masakatu Morii</i>	
Design of Arithmetic Building Blocks for Cryptographic Systems	124
<i>Mostafa Abd-El-Barr and Aisha Al-Noori</i>	

Novel Design of Fair Exchange Protocol for Semi-trusted Server and Its Application in Cloud Environment	130
<i>Chih-Hung Wang and Chien-Ming Wang</i>	
An Improvement Data Hiding Scheme Based on Formula Fully Exploiting Modification Directions and Pixel Value Differencing Method	136
<i>Wen-Chung Kuo, Jyun-Jia Li, Chun-Cheng Wang, Lih-Chyau Wu, and Yu-Chih Huang</i>	
Fighting Malware	
Integration of Multi-modal Features for Android Malware Detection Using Linear SVM	141
<i>Tao Ban, Takeshi Takahashi, Shanqing Guo, Daisuke Inoue, and Koji Nakao</i>	
Evaluation of a Brute Forcing Tool that Extracts the RAT from a Malicious Document File	147
<i>Mamoru Mimura, Yuhei Otsubo, and Hidehiko Tanaka</i>	
Comparing Malware Samples for Unpacking: A Feasibility Study	155
<i>Ryoichi Isawa, Masakatu Morii, and Daisuke Inoue</i>	
Author Index	161