# 2012 Seventh Asia Joint Conference on Information Security

# (Asia JCIS 2012)

## Tokyo, Japan
## 9 – 10 August 2012

IEEE Catalog Number: CFP1233T-PRT
ISBN: 978-1-4673-2261-4

# 2012 Seventh Asia Joint Conference on Information Security

# AsiaJCIS 2012

# Table of Contents

**Preface**............................................................vii

**Conference Committees and Reviewers**............................................................viii

---

## Session 1

Reversible Data Hiding for JPEG Based on EMD ............................................................1
*Wen-Chung Kuo and Shao-Hung Kuo*

An Efficient Lossless Data Hiding Scheme on VQ Index Coding ............................................................6
*Chin-Feng Lee, Ming-Chi Shih, and Cheng-Ta Huang*

Strong Tamper-Localization, Visual Secret Sharing Scheme Based on Exploiting Modification Direction ............................................................10
*Chin-Chen Chang, Ngoc-Tu Huynh, and Chia-Chun Lin*

## Session 2

SSL/TLS Status Survey in Japan - Transitioning against the Renegotiation Vulnerability and Short RSA Key Length Problem ............................................................17
*Yuji Suga*

Proposal of a Secure WEP Operation against Existing Key Recovery Attacks and its Evaluation ............................................................25
*Tsubasa Tsukaune, Yosuke Todo, and Masakatu Morii*

An Analysis of Security Patch Lifecycle Using Google Trend Tool ............................................................31
*Chien-Ting Kuo, He-Ming Ruan, Shih-Jen Chen, and Chin-Laung Lei*

Synthesis of Secure Passwords ............................................................35
*Tomoki Sato and Hiroaki Kikuchi*

## Session 3

Mobile Friendly and Highly Efficient Remote User Authenticated Key Agreement Protocol Featuring Untraceability ............................................................38
*Chin-Chen Chang, Hai-Duong Le, and Ching-Hsiang Chang*

PDAF: Proactive Distributed Authentication Framework for Regional Network ............................................................44
*Ruidong Li, Masaaki Ohnishi, Yasunori Owada, and Hiroaki Harai*

Fast-Refreshing Tree-Based Group Key Agreement for Mobile Ad Hoc Networks ....51
*Chung-Wei Chen, Shiuh-Jeng Wang, Yuh-Ren Tsai, and Hsing-Chung Chen*

Analysis of an eHealth Care System with Smart Card Based Authentication ....59
*Kuo-Hui Yeh, N.W. Lo, Tzong-Chen Wu, Ta-Chi Yang, and Horng-Twu Liaw*

**Session 4**

DroidMat: Android Malware Detection through Manifest and API Calls Tracing ....62
*Dong-Jie Wu, Ching-Hao Mao, Te-En Wei, Hahn-Ming Lee, and Kuo-Ping Wu*

A Study on Method to Analyze Application on Bada Using GUI without Source Code ....70
*Hanjae Jeong and Dongho Won*

Geographical Visualization of Malware Download for Anomaly Detection ....74
*Naoki Hiroguchi, Khamphao Sisaat, Hiroaki Kikuchi, and Surin Kittitornkun*

Multipurpose Network Monitoring Platform Using Dynamic Address Assignment ....79
*Masashi Eto, Daisuke Inoue, Mio Suzuki, and Koji Nakao*

**Session 5**

Survey on Cloud Data Integrity Proof Techniques ....85
*Solomon Guadie Worku, Zhong Ting, and Qin Zhi-Guang*

Data Integrity on Remote Storage for On-line Co-working ....92
*He-Ming Ruan, Yu-Shian Chen, and Chin-Laung Lei*

Attack Sequence Detection in Cloud Using Hidden Markov Model ....100
*Chia-Mei Chen, D.J. Guan, Yu-Zhi Huang, and Ya-Hui Ou*

Flaw and Configuration Analysis of Cloud Component Using First Order Logic ....104
*Ruo Ando*

**Author Index** ....109