Preface

The 8th International Workshop on Information Security Applications (WISA 2007) was held on Jeju Island, Korea during August 27–29, 2007. The workshop was sponsored by the Korea Institute of Information Security and Cryptology (KIISC), the Electronics and Telecommunications Research Institute (ETRI) and the Ministry of Information and Communication (MIC).

WISA aims at providing a forum for professionals from academia and industry to present their work and to exchange ideas. The workshop covers all technical aspects of security applications, including cryptographic and non-cryptographic techniques.

We were very pleased and honored to serve as the Program Committee Co-chairs of WISA 2007. The Program Committee received 95 papers from 20 countries, and accepted 27 papers for the full presentation track. The papers were selected after an extensive and careful refereeing process in which each paper was reviewed by at least three members of the Program Committee.

In addition to the contributed papers, the workshop had three special talks. Moti Yung gave a tutorial talk, entitled “Somebody You Know: The Fourth Factor of Authentication.” Kihong Park and Nasir Memon gave invited talks, entitled “Reactive Zero-Day Attack Protection” and “Securing Biometric Templates,” respectively.

Many people deserve our gratitude for their generous contributions to the success of the workshop. We would like to thank all the people involved in the technical program and in organizing the workshop. We are very grateful to the Program Committee members and the external referees for their time and efforts in reviewing the submissions and selecting the accepted papers. We also express our special thanks to the Organizing Committee members for their hard work in organizing the workshop.

Last but not least, on behalf of all those involved in organizing the workshop, we would like to thank all the authors who submitted papers to this workshop. Without their submissions and support, WISA could not have been a success.

December 2007

Sehun Kim
Moti Yung
Hyung-Woo Lee
Organization

Advisory Committee

- Man-Young Rhee, Kyung Hee University, Korea
- Hideki Imai, Tokyo University, Japan
- Mun Kee Choi, ETRI, Korea
- Bart Preneel, Katholieke Universiteit Leuven, Belgium
- Kil-Hyun Nam, Korea National Defense University, Korea
- Sang-Jae Moon, Kyungpook National University, Korea
- Dong-Ho Won, Sungkyunkwan University, Korea
- Pil-Joong Lee, POSTECH, Korea
- Dae-Ho Kim, NSRI, Korea
- Joo-Seok Song, Yonsei University, Korea

General Co-chairs

- Min Surp Rhee, Dankook University, Korea
- Sung-Won Sohn, ETRI, Korea

Steering Committee

- Kyo-Il Chung, ETRI, Korea
- TaeKyoung Kwon, Sejong University, Korea
- Im-Yeong Lee, Soonchunhyang University, Korea
- Dong-Il Seo, ETRI, Korea
- OkYeon Yi, Kookmin University, Korea
- Jae-Kwang Lee, Hannam University, Korea

Organizing Committee

- Chair: Sang Choon Kim, Kangwon National University, Korea
- Finance: Taenam Cho, Woosuk University, Korea
- Publication: Ji-Young Lim, Korean Bible University, Korea
- Publicity: Gang Shin Lee, KISA, Korea
- Heuisu Ryu, Gyeongin National University of Education, Korea
- Registration: Yoonjeong Kim, Seoul Women’s University, Korea
- Treasurer: Jaehoon Nah, ETRI, Korea
- Local Arrangements: Khi Jung Ahn, Cheju National University, Korea
- Dohoon Lee, NSRI, Korea
Program Committee

Co-chairs
Sehun Kim  KAIST, Korea
Moti Yung  Columbia University, USA
Hyung-Woo Lee  Hanshin University, Korea

Members
Gildas Avoine  MIT, CSAIL, USA
Lejla Batina  University of Leuven, Belgium
Mike Burmester  Florida State University, USA
Ki-Joon Chae  Ewha University, Korea
Myeonggil Choi  Inje University, Korea
Bruno Crispo  University of Trento, Italy
Sven Dietrich  CERT, CMU, USA
Helena Handschu  Spansion, France
Heng Swee Huay  Multimedia University, Malaysia
Maria Isabel Gonzalez Vasco  Universidad Rey Juan Carlos, Spain
Kil-Hyun Jeong  Jangan College, Korea
Gildas Avoine  MIT, CSAIL, USA
Soon-Won Jung  NITGEN, Korea
Stefan Katzenbeisser  Philips Research, Netherlands
Seungjoo Kim  Sungkyunkwan University, Korea
Seokwoo Kim  Hansei University, Korea
Brian King  Indiana University at Purdue, USA
Hong Seung Ko  Kyoto College of Graduate Studies for Informatics, Japan
Dong Hoon Lee  CIST, Korea University, Korea
Pil Joong Lee  POSTECH, Korea
Chae-Hun Lim  Sejong University, Korea
Dongdai Lin  SKLIS, Chinese Academy of Sciences, China
Mose Liskov  William and Mary College, USA
Michael Locasto  Columbia, USA
Havier Lopez  University of Malaga, Spain
Masahiro Mambo  Tsukuba, Japan
Jung Chan Na  ETRI, Korea
Shozo Naito  Kyoto College of Graduate Studies for Informatics, Japan
Yoram Ofek  University of Trento, Italy
Heekuck Oh  Hanyang University, Korea
Susan Pancho-Festin  University of the Philippines, Phillipines
In-Jae Park  Dream Security, Korea
Duong Hieu Phan,  University College London, UK
Raphael C.-W. Phan  EPFL, Switzerland
Vassilis Prevelakis  Drexel University, USA
# Table of Contents

## Public Key Crypto Applications

Universal $\eta_T$ Pairing Algorithm over Arbitrary Extension Degree .......................... 1  
*Masaaki Shirase, Yuto Kawahara, Tsuyoshi Takagi, and Eiji Okamoto*

Convertible Undeniable Proxy Signatures: Security Models and Efficient Construction .................................................. 16  
*Wei Wu, Yi Mu, Willy Susilo, and Xinyi Huang*

Secret Signatures: How to Achieve Business Privacy Efficiently? ........................................ 30  
*Byoungcheon Lee, Kim-Kwang Raymond Choo, Jeongmo Yang, and Seungjae Yoo*

## Biometrics/Information Hiding

Implementation of BioAPI Conformance Test Suite Using BSP Testing Model .......................................................... 48  
*Jihyeon Jang, Stephen J. Elliott, and Hakil Kim*

Information Hiding in Software with Mixed Boolean-Arithmetic Transforms ............................................. 61  
*Yongxin Zhou, Alec Main, Yuan X. Gu, and Harold Johnson*

Geometrically Invariant Image Watermarking in the DWT Domain ........................................ 76  
*Shijun Xiang and Hyoung-Joong Kim*

## Secure Hardware

Implementation of LSM-Based RBAC Module for Embedded System .................................................. 91  
*Jae-Deok Lim, Sung-Kyong Un, Jeong-Nyeo Kim, and ChoeilHoon Lee*

Iteration Bound Analysis and Throughput Optimum Architecture of SHA-256 (384, 512) for Hardware Implementations ............................................. 102  
*Yong Ki Lee, Herwin Chan, and Ingrid Verbauwhede*

A Compact Architecture for Montgomery Elliptic Curve Scalar Multiplication Processor ........................................ 115  
*Yong Ki Lee and Ingrid Verbauwhede*
Secure Systems

Windows Vault: Prevention of Virus Infection and Secret Leakage with Secure OS and Virtual Machine

Yoshiki Sameshima, Hideaki Saisho, Tsutomu Matsumoto, and Norihisa Komoda

An Architecture Providing Virtualization-Based Protection Mechanisms Against Insider Attacks

Frederic Stumpf, Patrick Röder, and Claudia Eckert

Detecting Motifs in System Call Sequences

William O. Wilson, Jan Feyereisl, and Uwe Aickelin

Wireless and Mobile Security

Comparative Studies in Key Disagreement Correction Process on Wireless Key Agreement System

Toru Hashimoto, Takashi Itoh, Masazumi Ueba, Hisato Iwai, Hideichi Sasaoka, Kazukuni Kobara, and Hideki Imai

Breaking 104 Bit WEP in Less Than 60 Seconds

Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin

Efficient Implementation of the Pairing on Mobilephones Using BREW

Motoi Yoshitomi, Tsuyoshi Takagi, Shinsaku Kiyomoto, and Toshiaki Tanaka

Application Security/Secure Systems

Security Analysis of MISTY1

Hidema Tanaka, Yasuo Hatano, Nobuyuki Sugio, and Toshinobu Kaneko

A Generic Method for Secure SBox Implementation

Emmanuel Prouff and Matthieu Rivain

On the Security of a Popular Web Submission and Review Software (WSaR) for Cryptology Conferences

Swee-Won Lo, Raphael C.-W. Phan, and Bok-Min Goi

Access Control/DB Security

Authorization Constraints Specification of RBAC

Lilong Han, Qingtan Liu, and Zongkai Yang
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Access Control Research for Inter-operation in Multi-domain</td>
<td>277</td>
</tr>
<tr>
<td>Zhuo Tang, Ruixuan Li, Zhengding Lu, and Zhumu Wen</td>
<td></td>
</tr>
<tr>
<td>A Compositional Multiple Policies Operating System Security Model</td>
<td>291</td>
</tr>
<tr>
<td>Lei Xia, Wei Huang, and Hao Huang</td>
<td></td>
</tr>
<tr>
<td><strong>Smart Cards/Secure Systems</strong></td>
<td></td>
</tr>
<tr>
<td>Longer Randomly Blinded RSA Keys May Be Weaker Than Shorter Ones</td>
<td>303</td>
</tr>
<tr>
<td>Colin D. Walter</td>
<td></td>
</tr>
<tr>
<td>Differential Power Analysis of HMAC Based on SHA-2, and Countermeasures</td>
<td>317</td>
</tr>
<tr>
<td>Robert McEvoy, Michael Tunstall, Colin C. Murphy, and William P. Marnane</td>
<td></td>
</tr>
<tr>
<td>Provably Secure Countermeasure Resistant to Several Types of Power Attack for ECC</td>
<td>333</td>
</tr>
<tr>
<td>JaeCheol Ha, Jeahoon Park, SangJae Moon, and SungMing Yen</td>
<td></td>
</tr>
<tr>
<td><strong>Anonymity and P2P Security</strong></td>
<td></td>
</tr>
<tr>
<td>Risk &amp; Distortion Based $K$-Anonymity</td>
<td>345</td>
</tr>
<tr>
<td>Shenkun Xu and Xiaojun Ye</td>
<td></td>
</tr>
<tr>
<td>Optimizing Quality Levels and Development Costs for Developing an Integrated Information Security System</td>
<td>359</td>
</tr>
<tr>
<td>Myeonggil Choi and Sangmun Shin</td>
<td></td>
</tr>
<tr>
<td>ICRrep: An Incentive Compatible Reputation Mechanism for P2P Systems</td>
<td>371</td>
</tr>
<tr>
<td>Junsheng Chang, Huaimin Wang, Gang Yin, and Yangbin Tang</td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>387</td>
</tr>
</tbody>
</table>