

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Sehun Kim Moti Yung
Hyung-Woo Lee (Eds.)

Information Security Applications

8th International Workshop, WISA 2007
Jeju Island, Korea, August 27-29, 2007
Revised Selected Papers

Volume Editors

Sehun Kim

KAIST, Department of Industrial Engineering

373-1, Guseong-dong, Yuseong-gu, Daejeon, 305-701, Korea

E-mail: shkim@kaist.ac.kr

Moti Yung

Google Inc.

Columbia University, Computer Science Department

RSA Laboratories

S.W.Mudd Building, New York, NY10027, USA

E-mail: moti@cs.columbia.edu

Hyung-Woo Lee

Hanshin University

School of Computer Engineering

411, Yangsan-dong, Osan, Gyunggi, 447-791, Korea

E-mail: hwlee@hs.ac.kr

Library of Congress Control Number: 2007942182

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, C.3, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-540-77534-X Springer Berlin Heidelberg New York

ISBN-13 978-3-540-77534-8 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12210664 06/3180 5 4 3 2 1 0

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
Moti Yung
Hyung-Woo Lee

KAIST, Korea
Columbia University, USA
Hanshin University, Korea

Members

Gildas Avoine
Lejla Batina
Mike Burmester
Ki-Joon Chae
Myeonggil Choi
Bruno Crispo
Sven Dietrich
Helena Handschu
Heng Swee Huay
Maria Isabel Gonzalez Vasco
Kil-Hyun Jeong
Gildas Avoine
Soon-Won Jung
Stefan Katzenbeisser
Seungjoo Kim
Seokwoo Kim
Brian King
Hong Seung Ko

MIT, CSAIL, USA
University of Leuven, Belgium
Florida State University, USA
Ewha University, Korea
Inje University, Korea
University of Trento, Italy
CERT, CMU, USA
Spansion, France
Multimedia University, Malaysia
Universidad Rey Juan Carlos, Spain
Jangan College, Korea
MIT, CSAIL, USA
NITGEN, Korea
Philips Research, Netherlands
Sungkyunkwan University, Korea
Hansei University, Korea
Indiana University at Purdue, USA
Kyoto College of Graduate Studies for
Informatics, Japan

Dong Hoon Lee
Pil Joong Lee
Chae-Hun Lim
Dongdai Lin
Mose Liskov
Michael Locasto
Havier Lopez
Masahiro Mambo
Jung Chan Na
Shozo Naito

CIST, Korea University, Korea
POSTECH, Korea
Sejong University, Korea
SKLIS, Chinese Academy of Sciences, China
William and Mary College, USA
Columbia, USA
University of Malaga, Spain
Tsukuba, Japan
ETRI, Korea
Kyoto College of Graduate Studies for
Informatics, Japan

Yoram Ofek
Heekuck Oh
Susan Pancho-Festin
In-Jae Park
Duong Hieu Phan,
Raphael C.-W. Phan
Vassilis Prevelakis

University of Trento, Italy
Hanyang University, Korea
University of the Philippines, Phillipines
Dream Security, Korea
University College London, UK
EPFL, Switzerland
Drexel University, USA

C. Pandu Rangan	IIT Madras, India
Kyung-Hyune Rhee	Pukyong National University, Korea
Pankaj Rohatgi	IBM Resaerch, USA
Ahmad-Reza Sadeghi	Ruhr University, Bochum, Germany
Kouichi Sakurai	Kyushu University, Japan
Radu Sion	SUNY, Stony Brook, USA
Ki-Wook Sohn	NSRI, Korea
Francois-Xavier Standaert	Louvaine University, Belgium
Yannis Stamatiou	University of Ioannina, Greece
Koutarou Suzuki	NTT Labs, Japan
Huaxiong Wang	Nanyang Technological University, Singapore
Duncan Wong	City University, Hong Kong
Heung-Youl Youm	Soonchunhyang University, Korea
Rui Zhang	AIST, Japan
Jianying Zhou	Inst. for Infocomm Research, Singapore

Table of Contents

Public Key Crypto Applications

Universal η_T Pairing Algorithm over Arbitrary Extension Degree	1
<i>Masaaki Shirase, Yuto Kawahara, Tsuyoshi Takagi, and Eiji Okamoto</i>	
Convertible Undeniable Proxy Signatures: Security Models and Efficient Construction	16
<i>Wei Wu, Yi Mu, Willy Susilo, and Xinyi Huang</i>	
Secret Signatures: How to Achieve Business Privacy Efficiently?	30
<i>Byoungcheon Lee, Kim-Kwang Raymond Choo, Jeongmo Yang, and Seungjae Yoo</i>	

Biometrics/Information Hiding

Implementation of BioAPI Conformance Test Suite Using BSP Testing Model	48
<i>Jihyeon Jang, Stephen J. Elliott, and Hakil Kim</i>	
Information Hiding in Software with Mixed Boolean-Arithmetic Transforms	61
<i>Yongxin Zhou, Alec Main, Yuan X. Gu, and Harold Johnson</i>	
Geometrically Invariant Image Watermarking in the DWT Domain	76
<i>Shijun Xiang and Hyoung-Joong Kim</i>	

Secure Hardware

Implementation of LSM-Based RBAC Module for Embedded System . . .	91
<i>Jae-Deok Lim, Sung-Kyong Un, Jeong-Nyeo Kim, and ChoelHoon Lee</i>	
Iteration Bound Analysis and Throughput Optimum Architecture of SHA-256 (384, 512) for Hardware Implementations	102
<i>Yong Ki Lee, Herwin Chan, and Ingrid Verbauwhede</i>	
A Compact Architecture for Montgomery Elliptic Curve Scalar Multiplication Processor	115
<i>Yong Ki Lee and Ingrid Verbauwhede</i>	

Secure Systems

Windows Vault: Prevention of Virus Infection and Secret Leakage with Secure OS and Virtual Machine	128
<i>Yoshiki Sameshima, Hideaki Saisho, Tsutomu Matsumoto, and Norihisa Komoda</i>	
An Architecture Providing Virtualization-Based Protection Mechanisms Against Insider Attacks	142
<i>Frederic Stumpf, Patrick Röder, and Claudia Eckert</i>	
Detecting Motifs in System Call Sequences	157
<i>William O. Wilson, Jan Feyereisl, and Uwe Aickelin</i>	

Wireless and Mobile Security

Comparative Studies in Key Disagreement Correction Process on Wireless Key Agreement System	173
<i>Toru Hashimoto, Takashi Itoh, Masazumi Ueba, Hisato Iwai, Hideichi Sasaoka, Kazukuni Kobara, and Hideki Imai</i>	
Breaking 104 Bit WEP in Less Than 60 Seconds	188
<i>Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin</i>	
Efficient Implementation of the Pairing on Mobilephones Using BREW	203
<i>Motoi Yoshitomi, Tsuyoshi Takagi, Shinsaku Kiyomoto, and Toshiaki Tanaka</i>	

Application Security/Secure Systems

Security Analysis of MISTY1	215
<i>Hidema Tanaka, Yasuo Hatano, Nobuyuki Sugio, and Toshinobu Kaneko</i>	
A Generic Method for Secure SBox Implementation	227
<i>Emmanuel Prouff and Matthieu Rivain</i>	
On the Security of a Popular Web Submission and Review Software (WSaR) for Cryptology Conferences	245
<i>Swee-Won Lo, Raphael C.-W. Phan, and Bok-Min Goi</i>	

Access Control/DB Security

Authorization Constraints Specification of RBAC	266
<i>Lilong Han, Qingtan Liu, and Zongkai Yang</i>	

Dynamic Access Control Research for Inter-operation in Multi-domain Environment Based on Risk	277
<i>Zhuo Tang, Ruixuan Li, Zhengding Lu, and Zhumu Wen</i>	
A Compositional Multiple Policies Operating System Security Model ...	291
<i>Lei Xia, Wei Huang, and Hao Huang</i>	

Smart Cards/Secure Systems

Longer Randomly Blinded RSA Keys May Be Weaker Than Shorter Ones	303
<i>Colin D. Walter</i>	
Differential Power Analysis of HMAC Based on SHA-2, and Countermeasures.....	317
<i>Robert McEvoy, Michael Tunstall, Colin C. Murphy, and William P. Marnane</i>	
Provably Secure Countermeasure Resistant to Several Types of Power Attack for ECC	333
<i>JaeCheol Ha, JeaHoon Park, SangJae Moon, and SungMing Yen</i>	

Anonymity and P2P Security

Risk & Distortion Based K -Anonymity	345
<i>Shenkun Xu and Xiaojun Ye</i>	
Optimizing Quality Levels and Development Costs for Developing an Integrated Information Security System	359
<i>Myeonggil Choi and Sangmun Shin</i>	
ICRep: An Incentive Compatible Reputation Mechanism for P2P Systems	371
<i>Junsheng Chang, Huaimin Wang, Gang Yin, and Yangbin Tang</i>	
Author Index	387