

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

Alfred Kobsa

University of California, Irvine, CA, 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

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Kyo-Il Chung Kiwook Sohn Moti Yung (Eds.)

Information Security Applications

9th International Workshop, WISA 2008
Jeju Island, Korea, September 23-25, 2008
Revised Selected Papers

Volume Editors

Kyo-II Chung

Electronics and Telecommunications Research Institute (ETRI)

Information Security Research Division

161 Gajeong Dong, YuseongGu

Daejeon, 305-700, Korea

E-mail: kyoil@etri.re.kr

Kiwook Sohn

The Attached Institute of Electronics

and Telecommunications Research Institute (ETRI)

1 Yuseong-Post

Daejeon, 305-702, Korea

E-mail: kiwook@ensec.re.kr

Moti Yung

Google Inc.

Columbia University, Computer Science Department

1214 Amsterdam Avenue

New York, NY 10027, USA

E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2009920695

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 3-642-00305-2 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-00305-9 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.com

© Springer-Verlag Berlin Heidelberg 2009

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12612604 06/3180 5 4 3 2 1 0

Preface

The 9th International Workshop on Information Security Applications (WISA 2008) was held in Jeju Island, Korea during September 23–25, 2008. 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 Knowledge Economy (MKE).

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 have served as the Program Committee Co-chairs of WISA 2008. The Program Committee received 161 papers from 18 countries, and accepted 24 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. Anat Zeelim-Hovav gave an invited talk, entitled “Investing in Information Security: A Coin in a Wishing Well?” Tai-Myoung Chung and Dieter Gollmann gave invited talks entitled “Today and Tomorrow of Security and Privacy” and “SOA Security: Service-Oriented Access Control,” 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.

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

November 2008

Kyo-Il Chung
Kiwook Sohn
Moti Yung

Organization

Advisory Committee

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

General Co-chairs

Chaegy Kim	ETRI, Korea
Hong-Sub Lee	KIISC, Korea

Steering Committee

Hyun-Sook Cho	ETRI, Korea
Sang-Choon Kim	Kangwon National University, Korea
Hyung-Woo Lee	Hanshin University, Korea
Jae-Kwang Lee	Hannam University, Korea
Dong-Il Seo	ETRI, Korea
OkYeon Yi	Kookmin University, Korea

Organization Committee

Chair	Jae-Cheol Ryou	Chungnam National University, Korea
Finance	Seong-Gon Choi	Chungbuk National University, Korea
	Jintae Oh	ETRI, Korea
	Jaehwoon Lee	Dongguk University, Korea
Publication	Dong Gue Park	Soonchunhyang University, Korea
Publicity	Neungsoo Park	Konkuk University, Korea
	Kilsoo Chun	KISA, Korea
	Dohoon Lee	ETRI, Korea
Registration	Khi Jung Ahn	Cheju National University, Korea
Local Arrangements	Taenam Cho	Woosuk University, Korea

Program Committee

Co-chairs	Kyo-Il Chung	ETRI, Korea
	Kiwook Sohn	ETRI, Korea
	Moti Yung	Columbia University, USA
Members	C. Pandu Rangan	IIT Madras, India
	Hyoung-Kee Choi	Sungkyunkwan University, Korea
	Hyun Cheol Chung	BCNE Global.Co., Ltd., Korea
	Debbie Cook	Columbia University, USA
	Pierre Alain Fouque	ENS, France
	JaeCheol Ha	Hoseo University, Korea
	Hoh Peter In	Korea University, Korea
	Stefan Katzenbeisser	Philips Research, The Netherlands
	Howon Kim	Pusan National University, Korea
	Hyong Shik Kim	Chungnam National University, Korea
	Hyung Jong Kim	Seoul Women University, Korea
	Seok Woo Kim	Hansei University, Korea
	Seung Joo Kim	Sungkyunkwan University, Korea
	Yongdae Kim	University of Minnesota, USA
	Brian King	Indiana University - Purdue University Indianapolis, USA
	Chiu Yuen Koo	Google Inc., USA
	Hong Seung Ko	Kyoto College of Graduate Studies for Informatics, Japan
	Jin Kwak	Soonchunhyang University, Korea
	Deok Gyu Lee	ETRI, Korea
	Dong Hoon Lee	Korea University, Korea
	Pil Joong Lee	POSTECH, Korea
	Chae-Hoon Lim	Sejong University, Korea
	Ji-Young Lim	Korean Bible University, Korea
	Dongdai Lin	SKLIS, Chinese Academy of Sciences, China
	Soohyun Oh	Hoseo University, Korea
	Dan Page	Bristol University, UK
	Susan Pancho-Festin	University of the Philippines, Philippines
	Namje Park	ETRI, Korea
	Vassilis Prevelakis	Drexel University, USA
	Kyung-Hyune Rhee	Pukyong National University, Korea
	Pankaj Rohatgi	IBM Research, USA
	Daehyun Ryu	Hansei University, Korea
	Kouichi Sakurai	Kyushu University, Japan
	Chang-ho Seo	Kongju National University, Korea
	Tsuyoshi Takagi	Future University-Hakodate, Japan
	Jeong Hyun Yi	Soongsil University, Korea
	Heung-Youl Youm	Soonchunhyang University, Korea
	Rui Zhang	AIST, Japan
	Jianying Zhou	Inst. for Infocomm Research, Singapore

Table of Contents

Smart Card and Secure Hardware(1)

Using Templates to Attack Masked Montgomery Ladder Implementations of Modular Exponentiation	1
<i>Christoph Herbst and Marcel Medwed</i>	
Template Attacks on ECDSA	14
<i>Marcel Medwed and Elisabeth Oswald</i>	
Compact ASIC Architectures for the 512-Bit Hash Function Whirlpool	28
<i>Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, and Akashi Satoh</i>	

Wireless and Sensor Network Security(1)

Improved Constant Storage Self-healing Key Distribution with Revocation in Wireless Sensor Network	41
<i>Qingyu Xu and Mingxing He</i>	
Advances in Ultralightweight Cryptography for Low-Cost RFID Tags: Gossamer Protocol	56
<i>Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M.E. Tapiador, and Arturo Ribagorda</i>	
Securing Layer-2 Path Selection in Wireless Mesh Networks	69
<i>Md. Shariful Islam, Md. Abdul Hamid, Byung Goo Choi, and Choong Seon Hong</i>	

Public Key Crypto Applications

Public Key Authentication with Memory Tokens	84
<i>Camille Vuillaume, Katsuyuki Okeya, Erik Dahmen, and Johannes Buchmann</i>	
Certificate-Based Signatures: New Definitions and a Generic Construction from Certificateless Signatures	99
<i>Wei Wu, Yi Mu, Willy Susilo, and Xinyi Huang</i>	
Cryptanalysis of Mu et al.'s and Li et al.'s Schemes and a Provably Secure ID-Based Broadcast Signcryption (IBBSC) Scheme	115
<i>S. Sharmila Deva Selvi, S. Sree Vivek, Ragavendran Gopalakrishnan, Naga Naresh Karuturi, and C. Pandu Rangan</i>	

Privacy and Anonymity

Sanitizable and Deletable Signature	130
<i>Tetsuya Izu, Noboru Kunihiro, Kazuo Ohta, Makoto Sano, and Masahiko Takenaka</i>	
An Efficient Scheme of Common Secure Indices for Conjunctive Keyword-Based Retrieval on Encrypted Data	145
<i>Peishun Wang, Huaxiong Wang, and Josef Pieprzyk</i>	
Extension of Secret Handshake Protocols with Multiple Groups in Monotone Condition	160
<i>Yutaka Kawai, Shotaro Tanno, Takahiro Kondo, Kazuki Yoneyama, Noboru Kunihiro, and Kazuo Ohta</i>	

N/W Security and Intrusion Detection

Pseudorandom-Function Property of the Step-Reduced Compression Functions of SHA-256 and SHA-512	174
<i>Hidenori Kuwakado and Shoichi Hirose</i>	
A Regression Method to Compare Network Data and Modeling Data Using Generalized Additive Model	190
<i>Sooyoung Chae, Hosub Lee, Jaeik Cho, Manhyun Jung, Jongin Lim, and Jongsub Moon</i>	
A Visualization Technique for Installation Evidences Containing Malicious Executable Files Using Machine Language Sequence	201
<i>Jun-Hyung Park, Minsoo Kim, and Bong-Nam Noh</i>	

Application Security and Trust Management

Image-Feature Based Human Identification Protocols on Limited Display Devices	211
<i>Hassan Jameel, Riaz Ahmed Shaikh, Le Xuan Hung, Yuan Wei Wei, Syed Muhammad Khaliq-ur-rehman Raazi, Ngo Trong Canh, Sungyoung Lee, Heejo Lee, Yuseung Son, and Miguel Fernandes</i>	
Ternary Subset Difference Method and Its Quantitative Analysis	225
<i>Kazuhide Fukushima, Shinsaku Kiyomoto, Toshiaki Tanaka, and Kowichi Sakurai</i>	
Data Deletion with Provable Security	240
<i>Marek Klonowski, Michał Przykucki, and Tomasz Strumiński</i>	

Smart Card and Secure Hardware(2)

A Probing Attack on AES	256
<i>Jörn-Marc Schmidt and Chong Hee Kim</i>	

On Avoiding ZVP-Attacks Using Isogeny Volcanoes	266
<i>J. Miret, D. Sadornil, J. Tena, R. Tomàs, and M. Valls</i>	
Security Analysis of DRBG Using HMAC in NIST SP 800-90	278
<i>Shoichi Hirose</i>	

Wireless and Sensor Network Security(2)

Compact Implementation of SHA-1 Hash Function for Mobile Trusted Module	292
<i>Mooseop Kim, Jaecheol Ryou, and Sungik Jun</i>	
An Improved Distributed Key Management Scheme in Wireless Sensor Networks	305
<i>Jun Zhou and Mingxing He</i>	
Protection Profile for Connected Interoperable DRM Framework	320
<i>Donghyun Choi, Sungkyu Cho, Dongho Won, and Seungjoo Kim</i>	
Author Index	333