

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

Microsoft Research, Cambridge, 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

Tsuyoshi Takagi Masahiro Mambo (Eds.)

Advances in Information and Computer Security

4th International Workshop on Security, IWSEC 2009
Toyama, Japan, October 28-30, 2009
Proceedings

Volume Editors

Tsuyoshi Takagi

Future University Hakodate

School of Systems Information Science

116-2 Kamedanakano-cho, Hakodate, Hokkaido 041-8655, Japan

E-mail: takagi@fun.ac.jp

Masahiro Mambo

University of Tsukuba

Graduate School of Systems and Information Engineering

1-1-1 Tennodai, Tsukuba, Ibaraki 305-8573, Japan

E-mail: mambo@cs.tsukuba.ac.jp

Library of Congress Control Number: 2009935384

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, K.4.1, F.2.1, C.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-642-04845-5 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-04845-6 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: 12772520 06/3180 5 4 3 2 1 0

Preface

The Fourth International Workshop on Security (IWSEC 2009) was held at Toyama International Conference Center, Toyama, Japan, October 28–30, 2009. The workshop was co-organized by CSEC, a special interest group on computer security of the IPSJ (Information Processing Society of Japan) and ISEC, a technical group on information security of IEICE (The Institute of Electronics, Information and Communication Engineers). The excellent Local Organizing Committee was led by the IWSEC 2009 General Co-chairs, Kazuo Takaragi and Hiroaki Kikuchi.

IWSEC 2009 received 46 paper submissions from all over the world. We would like to thank all the authors who submitted papers. Each paper was reviewed by at least three reviewers. In addition to the Program Committee members, many external reviewers joined the review process in their particular areas of expertise. We were fortunate to have this energetic team of experts, and are grateful to all of them for their hard work. The hard work includes very active discussion; the discussion phase was almost as long as the initial individual reviewing. The review and discussion were supported by a very nice Web-based system, iChair. We thank its developers.

Following the review phases, 13 papers were accepted for publication in this volume of *Advances in Information and Computer Security*. Together with the contributed papers, the workshop featured an invited talk and a hash function panel both of which were respectively given and chaired by eminent researcher, Bart Preneel (Katholieke Universiteit Leuven). An abstract of the talk, titled “The Future of Cryptographic Algorithms,” is included in this volume. We deeply appreciate his contribution.

Many people contributed to the success of IWSEC 2009. We wish to express our deep appreciation for their contribution to information and computer security.

October 2009

Tsuyoshi Takagi
Masahiro Mambo

IWSEC 2009

Fourth International Workshop on Security

Co-organized by

CSEC (Special Interest Group on Computer Security of the Information
Processing Society of Japan)
and

ISEC (Technical Group on Information Security, Engineering Sciences Society,
of the Institute of Electronics, Information and Communication Engineers,
Japan)

General Co-chairs

Kazuo Takaragi	Hitachi Ltd., Japan
Hiroaki Kikuchi	Tokai University, Japan

Advisory Committee

Norihisa Doi	Chuo University, Japan
Akira Hayashi	Kanazawa Institute of Technology, Japan
Hideki Imai	Chuo University, Japan
Günter Müller	University of Freiburg, Germany
Yuko Murayama	Iwate Prefectural University, Japan
Eiji Okamoto	University of Tsukuba, Japan
Ryoichi Sasaki	Tokyo Denki University, Japan
Shigeo Tsujii	Chuo University, Japan
Doug Tygar	University of California, Berkeley, USA

Program Committee Co-chairs

Tsuyoshi Takagi	Future University Hakodate, Japan
Masahiro Mambo	University of Tsukuba, Japan

Local Organizing Committee

Venue and Excursion
Co-chairs

Takao Okubo (Fujitsu Laboratories Ltd., Japan)
Koutarou Suzuki (NTT Corp., Japan)

Award Co-chairs

Hiroshi Doi (Institute of Information Security,
Japan)
Mitsuru Tada (Chiba University, Japan)

VIII Organization

Finance, Registration,
and Liaison Co-chairs

Ryuya Uda (Tokyo University of Technology,
Japan)

Hisao Sakazaki (Hitachi Ltd., Japan)

Kazuhisa Sekine (NTT DoCoMo, Inc., Japan)

Publicity Co-chairs

Kunihiko Miyazaki (Hitachi Ltd., Japan)

Noboru Kunihiro (The University of Tokyo,
Japan)

System Co-chairs

Toshihiro Tabata (Okayama University, Japan)

Yasuharu Katsuno (IBM Tokyo Research
Laboratory, Japan)

Publication Co-chairs

Isao Echizen (National Institute of Infomatics,
Japan)

Toru Nakanishi (Okayama University, Japan)

Program Committee

Toru Akishita

Gergei Bana

Alexandra Boldyreva

Zhenfu Cao

Christian S. Collberg

Bart De Decker

Chang Ee-Chien

Eiichiro Fujisaki

Steven Furnell

Juan A. Garay

Philippe Golle

Dieter Gollmann

Tetsu Iwata

Mariusz H. Jakubowski

Marc Joye

Angelos D. Keromytis

Sony Corporation, Japan

Technical University of Lisbon, Portugal

Georgia Institute of Technology, USA

Shanghai Jiao Tong University, China

University of Arizona, USA

K.U.Leuven, Belgium

National University of Singapore, Singapore

NTT, Japan

University of Plymouth, UK

AT&T Labs - Research, USA

Palo Alto Research Center, USA

TU Hamburg, Germany

Nagoya University, Japan

Microsoft, USA

Thomson R&D, France

Columbia University, USA and Symantec

Research Labs, France

Seungjoo Kim

Takeshi Koshiba

Michiharu Kudo

Noboru Kunihiro

Dong Hoon Lee

Javier Lopez

Mark Manulis

Kanta Matsuura

Alfred Menezes

Atsuko Miyaji

Hirofumi Muratani

David Naccache

Sungkyunkwan University, Korea

Saitama University, Japan

IBM Japan, Japan

University of Tokyo, Japan

Korea University, Korea

University of Malaga, Spain

TU Darmstadt, Germany

University of Tokyo, Japan

University of Waterloo, Canada

JAIST, Japan

Toshiba, Japan

ENS, France

Mridul Nandi	NIST, USA
Masakatsu Nishigaki	Shizuoka University, Japan
Kai Rannenber	Goethe University Frankfurt, Germany
Reihaneh Safavi-Naini	University of Calgary, Canada
Ryuichi Sakai	Osaka Electro-Communication University, Japan
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	Indian Statistical Institute, India
Akashi Satoh	AIST, Japan
Takeshi Shimoyama	Fujitsu Laboratories, Japan
Willy Susilo	University of Wollongong, Australia
Michael Szydlo	Akamai, USA
Toshihiro Tabata	Okayama University, Japan
Katsuyuki Takashima	Mitsubishi Electric Corporation, Japan
Toshiaki Tanaka	KDDI R&D Laboratories Inc., Japan
Routo Terada	University of Sao Paulo, Brazil
Pim Tuyls	Intrinsic ID, The Netherlands
Vijay Varadharajan	Macquarie University, Australia
Guilin Wang	University of Birmingham, UK
Dai Watanabe	Hitachi, Japan
Chung-Huang Yang	National Kaohsiung Normal University, Taiwan
Sung-Ming Yen	National Central University, Taiwan
Maki Yoshida	Osaka University, Japan
Hiroshi Yoshiura	University of Electro-Communications, Japan
Fangguo Zhang	Sun Yat-sen University, China
Jianying Zhou	Institute for Infocomm Research, Singapore
Alf Zugenmaier	DOCOMO Euro-Labs, Germany

External Reviewers

Joonsang Baek	Shinsaku Kiyomoto	Denis Royer
Chien-Ning Chen	Yuichi Komano	Mehmet Tahir Sandikkaya
Jae Tark Choi	Woo Kwon Koo	Taizo Shirai
Kazuhide Fukushima	Jun Kurihara	Koen Simoens
Teddy Furon	Kwangsue Lee	Isamu Teranishi
Iftach Haitner	Wei-Chih Lien	Carmela Troncoso
Yoshikazu Hanatani	Joseph K. Liu	Markus Tschersich
Xinyi Huang	Takahiro Matsuda	Jheng-Hong Tu
Yasunori Ishihara	Luke McAven	Yamin Wen
Taichi Isogai	Ryo Nishimaki	Lingling Xu
Christian Kahl	Haruki Ohta	Tomoko Yonemura
Yuichi Kaji	Kazumasa Omote	
Hyung Chan Kim	Souradyuti Paul	

Table of Contents

Invited Talk

The Future of Cryptographic Algorithms (Extended Abstract)	1
<i>Bart Preneel</i>	

Block Cipher

Bit-Free Collision: Application to APOP Attack	3
<i>Lei Wang, Yu Sasaki, Kazuo Sakiyama, and Kazuo Ohta</i>	
Impossible Boomerang Attack for Block Cipher Structures	22
<i>Jiali Choy and Huihui Yap</i>	
Improved Distinguishing Attacks on HC-256	38
<i>Gautham Sekar and Bart Preneel</i>	

Cryptographic Protocols

A Generic Construction of Timed-Release Encryption with Pre-open Capability	53
<i>Yasumasa Nakai, Takahiro Matsuda, Wataru Kitada, and Kanta Matsuura</i>	
An Efficient Identity-Based Signcryption Scheme for Multiple Receivers	71
<i>S. Sharmila Deva Selvi, S. Sree Vivek, Rahul Srinivasan, and Chandrasekaran Pandu Rangan</i>	
Universal Designated Verifier Signatures with Threshold-Signers	89
<i>Pairat Thorncharoensri, Willy Susilo, and Yi Mu</i>	
Reducing Complexity Assumptions for Oblivious Transfer	110
<i>K.Y. Cheong and Takeshi Koshihba</i>	

Contents Protection and Intrusion Detection

Tamper-Tolerant Software: Modeling and Implementation	125
<i>Mariusz H. Jakubowski, Chit Wei (Nick) Saw, and Ramarathnam Venkatesan</i>	
An Error-Tolerant Variant of a Short 2-Secure Fingerprint Code and Its Security Evaluation	140
<i>Koji Nuida</i>	

Efficient Intrusion Detection Based on Static Analysis and Stack
Walks 158
Jingyu Hua, Mingchu Li, Kowichi Sakurai, and Yizhi Ren

Authentication

Strongly Secure Authenticated Key Exchange without NAXOS’
Approach 174
Minkyu Kim, Atsushi Fujioka, and Berkant Ustaoglu

ID-Based Group Password-Authenticated Key Exchange 192
Xun Yi, Raylin Tso, and Eiji Okamoto

A Proposal of Efficient Remote Biometric Authentication Protocol 212
*Taiki Sakashita, Yoichi Shibata, Takumi Yamamoto,
Kenta Takahashi, Wakaha Ogata, Hiroaki Kikuchi, and
Masakatsu Nishigaki*

Author Index 229