

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

Kanta Matsuura Eiichiro Fujisaki (Eds.)

Advances in Information and Computer Security

Third International Workshop on Security, IWSEC 2008
Kagawa, Japan, November 25-27, 2008
Proceedings



Springer

Volume Editors

Kanta Matsuura
Institute of Industrial Science
The University of Tokyo
Tokyo, Japan
E-mail: kanta@iis.u-tokyo.ac.jp

Eiichiro Fujisaki
NTT Laboratories
Yokosuka-shi, Japan
E-mail: fujisaki.eiichiro@lab.ntt.co.jp

Library of Congress Control Number: 2008939387

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	3-540-89597-3 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-89597-8 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 2008
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12557493 06/3180 5 4 3 2 1 0

Preface

The Third International Workshop on Security (IWSEC 2008) was held at Kagawa International Conference Hall, Kagawa, Japan, November 25–27, 2008. The workshop was co-sponsored jointly by CSEC, a special interest group on computer security of IPSJ (Information Processing Society of Japan) and ISEC, a technical group on information security of the IEICE (The Institute of Electronics, Information and Communication Engineers). The excellent Local Organizing Committee was led by the IWSEC 2008 General Co-chairs, Masato Terada and Kazuo Ohta.

This year, there were 94 paper submissions from all over the world. We would like to thank all the authors who submitted papers to IWSEC 2008. Each paper was reviewed at least three reviewers. In addition to the members of the Program Committee, many external reviewers joined the review process of papers 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 appreciate its developers.

After all the review phases, 18 papers were accepted for publication in this volume of *Advances in Information and Computer Security*. In the workshop, the contributed papers were supplemented by one invited talk from eminent researcher Alfred Menezes (the Centre for Applied Cryptographic Research, The University of Waterloo).

There are many people who contributed to the success of IWSEC 2008. We wish to express our deep appreciation for their contribution to information and computer security.

November 2008

Kanta Matsuura
Eiichiro Fujisaki

IWSEC 2008

Third International Workshop on Security

Co-sponsored by

CSEC (Special Interest Group on Computer Security of 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

Masato Terada	Hitachi Ltd., Japan
Kazuo Ohta	University of Electro-Communications, 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	Institute of Information Security, Japan
Doug Tygar	University of California, Berkeley, USA

Program Committee Co-chairs

Kanta Matsuura	The University of Tokyo, Japan
Eiichiro Fujisaki	NTT Labs, Japan

Local Organizing Committee

Co-chairs

Yuji Suga	Internet Initiative Japan Inc., Japan
Takao Okubo	Fujitsu Laboratories Ltd., Japan
Minoru Kuribayashi	Kobe University, Japan

Award Co-chairs

Mira Kim	Institute of Information Security, Japan
Hiroshi Doi	Institute of Information Security, Japan

Finance, Registration, and Liaison Co-chairs

Keisuke Takemori	KDDI R&D Laboratories Inc., Japan
Ryuya Uda	Tokyo University of Technology, Japan
Kazuhiro Ono	Mitsubishi Electric, Japan

Publicity Co-chairs

Koji Chida	NTT Labs, Japan
Kunihiko Miyazaki	Hitachi Ltd., Japan

System Co-chairs

Naoto Sone	Naruto University of Education, Japan
Toshihiro Tabata	Okayama University, Japan

Publication co-Chairs

Tsuyoshi Takagi	Future University Hakodate, Japan
Isao Echizen	National Institute of Informatics, Japan

Program Committee

Michel Abdalla	ENS & CNRS, France
Koichiro Akiyama	Toshiba Corporation, Japan
Jesus Almansa	NTT Labs, Japan
Tomoyuki Asano	Sony Corporation, Japan
Feng Bao	Institute for Infocomm Research, Singapore
Kevin Butler	Pennsylvania State University, USA
Ee-Chien Chang	National University of Singapore, Singapore
Ed Dawson	Queensland University of Technology, Australia
Bart De Decker	K. U. Leuven, Belgium
Hiroshi Doi	Institute of Information Security, Japan
Steven Furnell	University of Plymouth, UK
Soichi Furuya	Hitachi, Ltd., Japan
David Galindo	University of Malaga, Spain
Philippe Golle	Palo Alto Research Center, USA
Shoichi Hirose	University of Fukui, Japan
Keiichi Iwamura	Tokyo University of Science, Japan
Tetsu Iwata	Nagoya University, Japan

Angelos D. Keromytis	Columbia University, USA
Aggelos Kiayias	University of Connecticut, USA
Hiroaki Kikuchi	Tokai University, Japan
Mira Kim	Institute of Information Security, Japan
Michiharu Kudo	IBM Japan, Japan
Noboru Kunihiro	The University of Tokyo, Japan
Kwok-Yan Lam	Tsinghua University, China
Dong Hoon Lee	Korea University, Korea
Javier Lopez	University of Malaga, Spain
Mark Manulis	UCL Crypto Group, Belgium
Wenbo Mao	EMC Research China, China
Keith Martin	Royal Holloway, University of London, UK
Mitsuru Matsui	Mitsubishi Electric, Japan
Atsuko Miyaji	Japan Advanced Institute of Science and Technology, Japan
Toru Nakanishi	Okayama University, Japan
Phong Nguyen	ENS, France
Masakatsu Nishigaki	Shizuoka University, Japan
Wakaha Ogata	Tokyo Institute of Technology, Japan
Takeshi Okamoto	Tsukuba University of Technology, Japan
Tatsuaki Okamoto	NTT Labs, Japan
Kazumasa Omote	University of Tsukuba, Japan
Kenneth G. Paterson	Royal Holloway, University of London, UK
Raphael Phan	Loughborough University, UK
Kai Rannenberg	Frankfurt University, Germany
Kyung-Hyune Rhee	Pukyong National University, Korea
Rei Safavi-Naini	University of Calgary, Canada
Kouichi Sakurai	Kyushu University, Japan
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University Hakodate, Japan
Keiji Takeda	Carnegie Mellon CyLab Japan, Japan
Toshiaki Tanaka	KDDI R&D Laboratories Inc., Japan
Ryuya Uda	Tokyo University of Technology, Japan
Serge Vaudenay	EPFL, Switzerland
Teemupekka Virtanen	Helsinki University of Technology, Finland
Guilin Wang	University of Birmingham, UK
Cliff Wang	Army Research Office, USA
Hajime Watanabe	National Institute of Advanced Science and Technology, Japan
Sung-Ming Yen	National Central University, Taiwan
Hiroshi Yoshiura	University of Electro-Communications, Japan
Yuliang Zheng	University of North Carolina at Charlotte, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

External Reviewers

Andreas Albers
 Yusuke Atomori
 Nuttapong Attrapadung
 Joonsang Baek
 Quan Bai
 Shane Balfe
 Jean-Luc Beuchat
 Charles Bouillaguet
 Kyu Young Choi
 Yvonne Cliff
 Jason Crampton
 Yang Cui
 André Deuker
 Pierre-Alain Fouque
 Georg Fuchsbauer
 Meng Ge
 Keisuke Hakuta
 Goichiro Hanaoka
 Yoshikazu Hanatani
 Ryotaro Hayashi
 Julio C. Hernandez-Castro
 Harunaga Hiwatari
 Naofumi Homma
 Xinyi Huang
 Tibor Jager
 Lars Janssen
 Christian Kahl
 Yasuharu Katsuno
 Bum Han Kim
 Masafumi Kusakawa
 Jeong Ok Kwon
 Gyesik Lee
 Kwang Su Lee
 Adrian Leung
 Gaëtan Leurent
 Jun Li

Benoit Libert
 Tatsuyuki Matsushita
 Luke McAven
 Hirofumi Muratani
 Akito Niwa
 Satoshi Obana
 Kazuto Ogawa
 Koji Okada
 Raphael Overbeck
 Sylvain Pasini
 Maura Paterson
 Kun Peng
 Jsaon Reid
 Hyun Sook Rhee
 Denis Royer
 Sandra Rueda
 Minoru Saeki
 Mike Scott
 Jinyang Shi
 Joshua Schiffman
 Kouichi Shimizu
 SeongHan Shin
 Zhexuan Song
 Chunhua Su
 Hung-Min Sun
 Daisuke Suzuki
 Katsuyuki Takashima
 Shigenori Uchiyama
 Martin Vuagnoux
 Yuji Watanabe
 Ou Yang
 Tomoko Yonemura
 Maki Yoshida
 Katsunari Yoshioka
 Rui Zhang
 Jan Zibuschka

Table of Contents

Cryptography

On Generating Elements of Orders Dividing $p^{2k} \pm p^k + 1$	1
<i>Maciej Grześkowiak</i>	
Chosen Ciphertext Secure Public Key Encryption with a Simple Structure	20
<i>Goichiro Hanaoka, Hideki Imai, Kazuto Ogawa, and Hajime Watanabe</i>	
Remarks on the Attack of Fouque et al. against the ℓ IC Scheme	34
<i>Naoki Ogura and Shigenori Uchiyama</i>	

Signature and Signcryption

Efficient Batch Verification of Short Signatures for a Single-Signer Setting without Random Oracles	49
<i>Fuchun Guo, Yi Mu, and Zhide Chen</i>	
Signcryption Scheme in Multi-user Setting without Random Oracles	64
<i>Chik How Tan</i>	
Simple and Efficient Group Signature Scheme Assuming Tamperproof Devices	83
<i>Takuya Yoshida and Koji Okada</i>	

Software Security

The Superdiversifier: Peephole Individualization for Software Protection	100
<i>Matthias Jacob, Mariusz H. Jakubowski, Prasad Naldurg, Chit Wei (Nick) Saw, and Ramarathnam Venkatesan</i>	
Detecting Java Theft Based on Static API Trace Birthmark	121
<i>Heewan Park, Seokwoo Choi, Hyun-il Lim, and Taisook Han</i>	
Online Network Forensics for Automatic Repair Validation	136
<i>Michael E. Locasto, Matthew Burnside, and Angelos D. Keromytis</i>	
Return Value Predictability Profiles for Self-healing	152
<i>Michael E. Locasto, Angelos Stavrou, Gabriela F. Cretu, Angelos D. Keromytis, and Salvatore J. Stolfo</i>	

Privacy Protection and Contents Protection

Involuntary Information Leakage in Social Network Services	167
<i>Ieng-Fat Lam, Kuan-Ta Chen, and Ling-Jyh Chen</i>	
Privacy Preserving Computations without Public Key Cryptographic Operation	184
<i>Koji Chida and Katsumi Takahashi</i>	
A Novel Framework for Watermarking: The Data-Abstracted Approach	201
<i>Cyril Bazin, Jean-Marie Le Bars, and Jacques Madelaine</i>	

Invited Talk

The Elliptic Curve Discrete Logarithm Problem: State of the Art	218
<i>Alfred Menezes</i>	

Authentication and Access Control

An Application of the Boneh and Shacham Group Signature Scheme to Biometric Authentication	219
<i>Julien Bringer, Hervé Chabanne, David Pointcheval, and Sébastien Zimmer</i>	
Analysis of a Biometric Authentication Protocol for Signature Creation Application	231
<i>Anongporn Salaiwarakul and Mark D. Ryan</i>	
Efficient Secure Labeling Method under Dynamic XML Data Streams	246
<i>Dong Chan An, So Mi Park, and Seog Park</i>	

Implementation

Bitstream Encryption and Authentication Using AES-GCM in Dynamically Reconfigurable Systems	261
<i>Yohei Hori, Akashi Satoh, Hirofumi Sakane, and Kenji Toda</i>	
The Long-Short-Key Primitive and Its Applications to Key Security	279
<i>Matthew Cary, Matthias Jacob, Mariusz H. Jakubowski, and Ramarathnam Venkatesan</i>	

Author Index	299
--------------------	-----