Lecture Notes in Computer Science 5824

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Springer

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

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)

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	Sony Corporation, Japan
Gergei Bana	Technical University of Lisbon, Portugal
Alexandra Boldyreva	Georgia Institute of Technology, USA
Zhenfu Cao	Shanghai Jiao Tong University, China
Christian S. Collberg	University of Arizona, USA
Bart De Decker	K.U.Leuven, Belgium
Chang Ee-Chien	National University of Singapore, Singapore
Eiichiro Fujisaki	NTT, Japan
Steven Furnell	University of Plymouth, UK
Juan A. Garay	AT&T Labs - Research, USA
Philippe Golle	Palo Alto Research Center, USA
Dieter Gollmann	TU Hamburg, Germany
Tetsu Iwata	Nagoya University, Japan
Mariusz H. Jakubowski	Microsoft, USA
Marc Joye	Thomson R&D, France
Angelos D. Keromytis	Columbia University, USA and Symantec Research Labs, France
Seungjoo Kim	Sungkyunkwan University, Korea
Takeshi Koshiba	Saitama University, Japan
Michiharu Kudo	IBM Japan, Japan
Noboru Kunihiro	University of Tokyo, Japan
Dong Hoon Lee	Korea University, Korea
Javier Lopez	University of Malaga, Spain
Mark Manulis	TU Darmstadt, Germany
Kanta Matsuura	University of Tokyo, Japan
Alfred Menezes	University of Waterloo, Canada
Atsuko Miyaji	JAIST, Japan
Hirofumi Muratani	Toshiba, Japan
David Naccache	ENS, France

Mridul Nandi	NIST, USA
Masakatsu Nishigaki	Shizuoka University, Japan
Kai Rannenberg	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	Kwangsu 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

Authentication