Lecture Notes in Computer Science 5461

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

Pil Joong Lee Jung Hee Cheon (Eds.)

Information Security and Cryptology – ICISC 2008

11th International Conference
Seoul, Korea, December 3-5, 2008
Revised Selected Papers

Springer

Volume Editors

Pil Joong Lee
Pohang University of Science and Technology (POSTECH)
Department of Electronic and Electrical Engineering
San 31 Hyoja-dong, Nam-gu, Pohang, Kyungbuk 790-784, Korea
E-mail: pjl@postech.ac.kr

Jung Hee Cheon
Seoul National University, Department of Mathematical Sciences
599 Gwanakno, Gwanak-gu, Seoul 151-742, Korea
E-mail: jhcheon@snu.ac.kr

Library of Congress Control Number: Applied for

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-00729-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-00729-3 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12631810 06/3180 5 4 3 2 1 0

Preface

ICISC 2008, the 11th International Conference on Information Security and Cryptology, was held in Seoul, Korea, during December 3–5, 2008. It was organized by the Korea Institute of Information Security and Cryptology (KIISC). The aim of this conference was to provide a forum for the presentation of new results in research, development, and applications in the field of information security and cryptology. It also served as a place for research information exchange.

The conference received 131 submissions from 28 countries, covering all areas of information security and cryptology. The review and selection processes were carried out in two stages by the Program Committee (PC) of 62 prominent researchers via online meetings, using the We-Submission-and-Review software written by Shai Halevi, IBM. First, at least three PC members blind-reviewed each paper, and papers co-authored by the PC members were reviewed by at least five PC members. Second, individual review reports were revealed to PC members, followed by detailed interactive discussion on each paper. Through this process, the PC finally selected 26 papers from 14 countries. The acceptance rate was 19.8%. The authors of selected papers had a few weeks to prepare for their final versions based on the comments received from more than 136 external reviewers. These revised papers were not subject to editorial review and the authors bear full responsibility for their contents.

The conference featured one tutorial and two invited talks. The tutorial was given by Masayuki Abe from NTT. The invited speakers for two talks were Vincent Rijmen from K.U.L. & Graz University of Tech and Jong-Deok Choi from Samsung Electronics.

There are many people who contributed to the success of ICISC 2008. We would like to thank all the authors who submitted papers to this conference. We are deeply grateful to all 62 members of the PC members. It was a truly nice experience to work with such talented and hard-working researchers. We wish to thank all the external reviewers for assisting the PC in their particular areas of expertise. Thanks to Shai Halevi for allowing us to use their convenient software. Finally, we would like to thank all the participants of the conference who made this event an intellectually stimulating one through their active contribution.

December 2008

Pil Joong Lee
Jung Hee Cheon

ICISC 2008

The 11th Annual International Conference
on Information Security

December 3–5, 2008
Sungkyunkwan University, Seoul, Korea

Organized by
Korea Institute of Information Security and Cryptology (KIISC)
http://www.kiisc.or.kr

In cooperation with
Ministry of Knowledge Economy (MKE)
http://www.mke.go.kr

General Chair

Hong-sub Lee	KIISC, Korea

Program Co-chairs

Pil Joong Lee	POSTECH, Korea
Jung Hee Cheon	Seoul National University, Korea

Program Committee

Joonsang Baek	Institute for Infocomm Research, Singapore
Liqun Chen	Hewlett-Packard Laboratories, UK
Nicolas T. Courtois	University College London, UK
Michel Cukier	University of Maryland, USA
Frederic Cuppens	Telecom Bretagne, France
Bart De Decker	Katholieke Universiteit Leuven, Belgium
Mario Marques Freire	University of Beira Interior, Portugal
Philippe Golle	Palo Alto Research Center, USA
Guang Gong	University of Waterloo, Canada
Vipul Goyal	UCLA, USA
Kil-Chan Ha	Sejong University, Korea
Eduardo B. Fernandez	Florida Atlantic University, USA
Dowon Hong	ETRI, Korea
Jin Hong	Seoul National University, Korea
Seokhie Hong	Korea University, Korea
Stanislaw Jarecki	University of California, Irvine, USA
Jaeyeon Jung	Intel Research, USA

Kwangjo Kim	ICU, Korea
Yongdae Kim	University of Minnesota, Twin Cities, USA
Christopher Kruegel	University of California, Santa Barbara, USA
Taekyoung Kwon	Sejong University, Korea
Byoungcheon Lee	Joongbu University, Korea
Dong Hoon Lee	Korea University, Korea
Mun-Kyu Lee	Inha University, Korea
Yingjiu Li	Singapore Management University, Singapore
Chae Hoon Lim	Sejong University, Korea
Javier Lopez	University of Malaga, Spain
Keith Martin	Royal Holloway, University of London, UK
Sjouke Mauw	University of Luxembourg, Luxembourg
Atsuko Miyaji	JAIST, Japan
SangJae Moon	Kyungpook National University, Korea
David Naccache	Ecole Normale Superieure, France
Jesper Buus Nielsen	Aarhus University, Denmark
DaeHun Nyang	Inha University, Korea
Tatsuaki Okamoto	NTT, Japan
Rolf Oppliger	eSECURITY Technologies, Switzerland
Paolo D'Arco	University of Salerno, Italy
Je Hong Park	ETRI, Korea
Sangjoon Park	Sungkyunkwan University, Korea
Sangwoo Park	ETRI, Korea
Jacques Patarin	Versailles University, France
Raphael C.-W. Phan	Loughborough University, UK
Bart Preneel	Katholieke Universiteit Leuven,Belgium
Jean-Jacques Quisquater	UCL, Belgium
Vincent Rijmen	K.U.L., Belgium and Graz University of Technology, Austria
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany
Kouichi Sakurai	Kyushu University, Japan
Mahmoud Salmasizadeh	Sharif University of Technology, Iran
Palash Sarkar	Indian Statistical Institute, India
JungHwan Song	Hanyang University, Korea
Rainer Steinwandt	Florida Atlantic University, USA
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University Hakodate, Japan
Yukiyasu Tsunoo	NEC Corporation, Japan
Jozef Vyskoc	VaF s.r.o., Slovakia
Sung-Ming Yen	National Central University, Taiwan
Jeong Hyun Yi	Samsung, Korea
Hyunsoo Yoon	KAIST, Korea
Dae Hyun Yum	POSTECH, Korea
Moti Yung	Google Inc. and Columbia University, USA
Fangguo Zhang	Google Inc. and Columbia University, USA
Alf Zugenmaier	DoCoMo Euro-Labs, Germany

Organizing Chair

Seungjoo Kim	Sungkyunkwan University, Korea

Organizing Committee

Dong Kyue Kim	Hanyang University. Korea
Ki Young Moon	ETRI, Korea
Chang-Seop Park	Dankook University, Korea
Young Ik Eom	Sungkyunkwan University, Korea
Heekuck Oh	Hanyang University, Korea
Dong Hoon Lee	Korea University, Korea
Im-Yeong Lee	Soonchunhyang University, Korea

External Reviewers

Frederik Armknecht
Maryam Rajabzadeh Assar
Man Ho Au
Jean-Philippe Aumasson
Fabien Autrel
Behnam Bahrak
Shane Balfe
Lejla Batina
Aurelie Bauer
Robin Berthier
Jean-Luc Beuchat
Annalisa De Bonis
Antoon Bosselaers
Yacine Bouzida
Wouter Castryck
Dario Catalano
Donghoon Chang
Ku Young Chang
Byong-Deok Choi
Jae Tark Choi
Jeong Woon Choi
Sherman Chow
Danielle Chrun
Carlos Cid
Ed Condon
Nora Cuppens-Boulahia
M. Prem Laxman Das
Ton van Deursen
Gwenael Doerr
Dang Nguyen Duc
Thomas Eisenbarth
Yehia Elrakaiby
Jonathan Etrog
Kazuhide Fukushima
Xinxin Fan
Joaquin Garcia-Alfaro
Benedikt Gierlichs
Henri Gilbert
Yoshiaki Hori
JaeCheul Ha
Daewan Han
Honggang Hu
Xinyi Huang
Junbeom Hur
Jung Yeon Hwang
Sebastiaan Indesteege
Hoda Jannati
Keith Jarrin
Ikrae, Jeong
Nam-su Jho
Takeshi Kawabata
Chano Kim
Jihye Kim
Jongsung Kim
Takayuki Kimura
Divyan M. Konidala
Heejin Park
Hiroyasu Kubo
Jeong Ok Kwon
Jorn Lapon
HoonJae Lee
Ji-Seon Lee
JongHyup Lee
Jun Ho Lee
Jung-Keun Lee
Kwangsu Lee
Minsoo Lee
Youngsook Lee
Jin Li
Wei-Chih Lien
Hsi-Chung Lin
Kuan-Jen Lin
Hans Loehr
Carolin Lunemann
Florian Mendel
Hideyuki Miyake
Abedelaziz Mohaisen
Amir Moradi
Tomislav Nad
Vincent Naessens
Akira Nozawa
Satoshi Obana
Chihiro Ohyama

Katsuyuki Okeya
Claudio Orlandi
Kyosuke Osaka
Omkant Pandey
Jun Pang
Chanil Park
Hyun-A Park
YongSu Park
Young-Ho Park
Axel Poschmann
Roberto De Prisco
Sasa Radomirovic
Christian Rechberger
Mohammad Reza Reyhanitabar
Chunhua Su
Minoru Saeki
Teruo Saito
Somitra Kumar Sanadhya
Riccardo Scandariato
Martin Schläffer
Jae Woo Seo
Maki Shigeri
Masaaki Shirase
Haya Shulman
Masakazu Soshi
Miroslava Sotakova
Takahiko Syouji
Tamer
Julien Thomas
Joe-Kai Tsay
Etsuko Tsujihara
Frederik Vercauteren
Pieter Verhaeghe
Ivan Visconti
Camille Vuillaume
Christian Wachsmann
Yamin Wen
Jian Weng
Bo-Ching Wu
Chi-Dian Wu
Lingling Xu
OkYeon Yi
Yves Younan
Ng Ching Yu
Aaram Yun
Chang-An Zhao
Xingwen Zhao
Tieyan Li

Sponsoring Institutions

BCQRE
Chungnam National University Internet Intrusion Response Technology Research Center (CNU IIRTRC), Korea
Electronics and Telecommunications Research Institute (ETRI), Korea
IglooSecurity, Korea
Korea Electronics Technology Institute (KETI), Korea
Korea Information Security Agency (KISA), Korea
BK21 Information Security in Ubiquitous Environment, Korea
Mobile Network Security Technology Research Center (MSRC), Korea
LG-CNS, Korea
LOTTE Data Communication Company, Korea
SNU-BK21 Mathematical Sciences Division, Korea
Sungkyunkwan University Authentication Technology Research Center (SKKU ARTC), Korea

Table of Contents

Public Key Encryption

Key Management and Secret Sharing

Privacy and Digital Rights

Digital Signature and Voting

Side Channel Attack

Hash and MAC

Primitives and Foundations

Block and Stream