Lecture Notes in Computer Science 5984

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

Donghoon Lee Seokhie Hong (Eds.)

Information Security and Cryptology – ICISC 2009

12th International Conference
Seoul, Korea, December 2-4, 2009
Revised Selected Papers

Springer

Volume Editors

Donghoon Lee
Seokhie Hong
CIST (Center for Information Security Technologies)
Korea University
5-1 Anam, Sungbuk Gu, Seoul, 136-713, Korea
E-mail: donghlee@korea.ac.kr, hsh@cist.korea.ac.kr

Library of Congress Control Number: 2010930429

CR Subject Classification (1998): E.3, K.6.5, C.2, D.4.6, G.2.1, E.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-14422-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-14422-6 Springer Berlin Heidelberg New York

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

ICISC 2009, the 12th International Conference on Information Security and Cryptology, was held in Seoul, Korea, during December 2–4, 2009. It was organized by the Korea Institute of Information Security and Cryptology (KIISC) and the Ministry of Public Administration and Security (MOPAS). 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 88 submissions from 22 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) comprising 57 prominent researchers via online meetings. 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, and detailed interactive discussion on each paper followed. Through this process, the PC finally selected 25 papers from 15 countries. The acceptance rate was 28.4%. The authors of selected papers had a few weeks to prepare for their final versions based on the comments received from more than 80 external reviewers. The conference featured one tutorial and one invited talk. The tutorial was given by Amit Sahai from the University of California and the talk was given by Michel Abdalla from École normale supérieure. There are many people who contributed to the success of ICISC 2009. We would like to thank all the authors who submitted papers to this conference. We are deeply grateful to all 57 members of the PC, especially to those who shepherded conditionally accepted papers. 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. We would like to thank all the participants of the conference who made this event an intellectually stimulating one through their active contribution. The support given to the ICISC 2009 workshop by the following sponsors is greatly appreciated: National Security Research Institute (NSRI), Electronics and Telecommunications Research Institute (ETRI), National Institute for Mathematical Sciences (NIMS), Korea Internet and Security Agency (KISA), Korea University BK21 Information Security in Ubiquitous Environment, Seoul National University Research Institute of Mathematics (SNU RIM), Korean Federation of Science and Technology Societies (KOFST), Chungnam National University Internet Intrusion Response Technology Research Center (IIRTRC), MarkAny, SG Advantech, AhnLab, LG CNS, and Korea University.

December 2009

Donghoon Lee
Seokhie Hong

Organization

ICISC 2009 was organized by the Korea Institute of Information Security and Cryptology (KIISC) and Ministry of Public Administration and Security (MOPAS)

Executive Committee

General Chair	Kwangjo Kim (KAIST, Korea)
Program Chair	Donghoon Lee (CIST, Korea University, Korea)
	Seokhie Hong (CIST, Korea University, Korea)
Organizing Chair	Taekyoung Kwon (Sejong University, Korea)

Program Committee

Joonsang Baek	I2R, Singapore
Alex Biryukov	University of Luxembourg, Luxembourg
Liqun Chen	HP Labs, UK
Jung Hee Cheon	Seoul National University, Korea
Paolo Milani Comparetti	Vienna University of Technology, Austria
Nicolas T. Courtois	University College London, UK
Frédéric Cuppens	Telecom Bretagne, France
Paolo D'Arco	University of Salerno, Italy
Bart De Decker	Katholieke Universiteit Leuven, Belgium
David Galindo	University of Luxembourg, Luxembourg
Philippe Golle	Palo Alto Research Center, USA
Vipul Goyal	UCLA, USA and MSR, India
Louis Granboulan	EADS Innovation Works, France
Matthew Green	Independent Security Evaluators, USA
Dong-Guk Han	Kookmin University, Korea
Martin Hell	Lund University, Sweden
Deukjo Hong	Attached Institute of ETRI, Korea
Jin Hong	Seoul National University, Korea
Nick Hopper	University of Minnesota, USA
David Jao	University of Waterloo, Canada
Jaeyeon Jung	Intel Labs, USA
Seungjoo Kim	Sungkyunkwan University, Korea
Xuejia Lai	Shanghai Jiao Tong University, China
Byoungcheon Lee	Joongbu University, Korea
Mun-Kyu Lee	Inha University, Korea
Pil Joong Lee	Pohang University of Science and Technology, Korea
Yingjiu Li	Singapore Management University, Singapore

Mark Manulis	Darmstadt University of Technology, Germany
Keith Martin	Royal Holloway, University of London, UK
Sjouke Mauw	University of Luxembourg, Luxembourg
Atsuko Miyaji	Japan Advanced Institute of Science and Technology, Japan
Jose A. Montenegro	University of Malaga, Spain
David Naccache	École normale supérieure, France
Jesper Buus Nielsen	Aarhus University, Denmark
DaeHun Nyang	Inha University, Korea
Rolf Oppliger	eSECURITY Technologies, Switzerland
Kihong Park	Purdue University, USA
Raphael C.-W. Phan	Loughborough University, UK
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Vincent Rijmen	Katholieke Universiteit Leuven, Belgium and Graz University of Technology, Austria
Bimal Roy	Indian Statistical Institute, India
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany
Reihaneh Safavi-Naini	University of Calgary, Canada
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	Indian Statistical Institute, India
Berry Schoenmakers	Eindhoven University of Technology, The Netherlands
Rainer Steinwandt	Florida Atlantic University, USA
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University Hakodate, Japan
Yukiyasu Tsunoo	NEC Corporation, Japan
Jorge Villar	Universitat Politecnica de Catalunya, Spain
Sung-Ming Yen	National Central University, Taiwan
Jeong Hyun Yi	Soongsil University, Korea
Dae Hyun Yum	Pohang University of Science and Technology, Korea
Fangguo Zhang	Sun Yat-sen University, China
Jianying Zhou	I2R, Singapore

Subreviewers

Tamer AbuHmed	Ming Duan
Jean-Philippe Aumasson	Sungwook Eom
Luigi Catuogno	Junfeng Fan
Yong-Je Choi	Caroline Fontaine
Kim-Kwang Raymond Choo	Ge Fu
Gouenou Coatrieux	Joaquin Garcia-Alfaro
Deepak Dalai	Ran Gelles
Ton van Deursen	Choudary Gorantla

Taeyoon Han
Jeongdae Hong
Xinyi Huang
Emeline Hufschmitt
Sebastiaan Indesteege
Daisuke Inoue
Hugo Jonker
Jeonil Kang
Emilia Käsper
Takeshi Kawabata
Dmitry Khovratovich
HyunMin Kim
Jangseong Kim
Jihye Kim
Kitae Kim
Minkyu Kim
So Jeong Kim
Sungkyung Kim
Woo Chun Kim
Youn Kyu Kim
Bonwook Koo
Barbara Kordy
Jung Keun Lee
Jin Li
Peter van Liesdonk
Hsi-Chung Lin
Joseph K. Liu
Yali Liu
Hans Loehr
Nicky Mouha
Sandra Marcello
Sascha Müller
Kris Narayan
Ching Yu Ng
Ivica Nikolic
Kazumasa Omote
Wolter Pieters
Saša Radomirović
Minoru Saeki
Teruo Saito
Thomas Schneider
Jae Woo Seo
Masaaki Shirase
Siamak F. Shahandashti
Maki Shigeri
HyunDong So
Jeong Eun Song
Masakazu Soshi
Takahiko Syouji
Toshiaki Tanaka
Isamu Teranishi
Etsuko Tsujihara
Frederik Vercauteren
Christian Wachsmann
Jhih-Wei Wang
Jian Weng
Chi-Dian Wu
Zhongming Wu
Yanjiang Yang
Yeon-Hyeong Yang
Tsz Hon Yuen
Jinmin Zhong
Zayabaatar
Bo Zhu

Table of Contents

Key Management and Key Exchange

Public Key Cryptography

Algebraic Cryptanalysis and Stream Cipher

Security Management and Efficient Implementation

Side Channel Attack

Privacy Enhanced Technology

Cryptographic Protocol

Cryptanalysis of Hash Function

Network Security