Lecture Notes in Computer Science 3935

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

Dongho Won Seungjoo Kim (Eds.)

Information Security and Cryptology – ICISC 2005

8th International Conference
Seoul, Korea, December 1-2, 2005
Revised Selected Papers

Springer

Volume Editors

Dongho Won
Seungjoo Kim
Sungkyunkwan University
School of Information and Communication Engineering
Information Security Group
300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do 440-746, Korea
E-mail: {dhwon, skim}@security.re.kr

Library of Congress Control Number: 2006924114

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 3-540-33354-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-33354-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11734727 06/3142 5 4 3 2 1 0

Preface

The 8th International Conference on Information Security and Cryptology was organized by the Korea Institute of Information Security and Cryptology (KIISC) and sponsored by the Ministry of Information and Communication of Korea (MIC). This conference aims at providing a forum for the presentation of new results in research, development, and application in information security and cryptology. This is also intended to be a place where research information can be exchanged.

The conference received 192 submissions from 29 countries, and the Program Committee selected 32 (from 15 countries) of these for presentation. The conference program includes two invited lectures by David Naccache on "National Security, Forensics and Mobile Communications" and by Shigeo Tsujii on "Information Security as Interdisciplinary Science Based on Ethics".

We would like to thank the many researchers from all over the world who submitted their work to this conference. The submission review process had two phases. In the first phase, Program Committee members compiled reports and entered them, via Web interface, into Web Review software. In the second phase, committee members used the software to browse each other's reports, discuss, and update their own reports. We are extremely grateful to the Program Committee members for their enormous investment of time and effort in the difficult and delicate process of review and selection. Moreover, we would like to thank all the authors who submitted papers to ICISC 2005 and the authors of accepted papers for their preparation of camera-ready manuscripts. Last but not least, we thank our students, Junghyun Nam, Yunho Lee, Jin Kwak, Younggyo Lee, and Seokhyang Cho, who helped us during the whole process of preparation for the conference.

February 2006

Dongho Won
Seungjoo Kim

Organization

General Chair

Dae Ho Kim	NSRI, Korea

Program Committee Co-chairs

Dongho Won	Sungkyunkwan University, Korea
Seungjoo Kim	Sungkyunkwan University, Korea

Program Committee

Giuseppe Ateniese	The Johns Hopkins University, USA
Tuomas Aura	Microsoft Research, UK
Alex Biryukov	Katholieke Universiteit Leuven, Belgium
John Black	University of Colorado, USA
Liqun Chen	Hewlett-Packard Labs, UK
Jung Hee Cheon	Seoul National University, Korea
Kyo-il Chung	ETRI, Korea
Jean-Sebastien Coron	University of Luxembourg, Luxembourg
Ed Dawson	Queensland University of Technology, Australia
Alexander W. Dent	Royal Holloway, UK
Anand Desai	NTT MCL, USA
Yevgeniy Dodis	New York University, USA
Gerhard Eschelbeck	Qualys, USA
Serge Fehr	CWI, The Netherlands
Pierre-Alain Fouque	École Normale Supérieure, France
Eiichiro Fujisaki	NTT Labs, Japan
Juan A. Garay	Bell Laboratories, USA
Marc Girault	France Telecom, France
Philippe Golle	Palo Alto Research Center, USA
Dieter Gollmann	TU Hamburg, Germany
SangGeun Hahn	KAIST, Korea
Yongfei Han	ONETS, China
Goichiro Hanaoka	University of Tokyo, Japan
Markus Jakobsson	Indiana University of Pennsylvania, USA
Marc Joye	Gemplus Card International, France
Jonathan Katz	University of Maryland, USA
Hiroaki Kikuchi	University of Tokai, Japan
Hyoung-Joong Kim	Kangwon National University, Korea
Kwangjo Kim	Information and Communications University, Korea

Kaoru Kurosawa	Ibaraki University, Japan
Taekyoung Kwon	Sejong University, Korea
Young-Bin Kwon	Chung-Ang University, Korea
Chi Sung Laih	National Cheng Kung University, Taiwan
Kwok-Yan Lam	Tsinghua University, China
Dong Hoon Lee	Korea University, Korea
Sang-Ho Lee	Ewha Womans University, Korea
Arjen Lenstra	Lucent Technologies' Bell Laboratories, USA, and Eindhoven University of Technology, The Netherlands
Yingjiu Li	Singapore Management University, Singapore
Helger Lipmaa	Cybernetica AS & University of Tartu, Estonia
Javier Lopez	University of Malaga, Spain
Masahiro Mambo	University of Tsukuba, Japan
Keith Martin	Royal Holloway, University of London, UK
Mitsuru Matsui	Mitsubishi Electric Corporation, Japan
Chris Mitchell	Royal Holloway, University of London, UK
Atsuko Miyaji	JAIST, Japan
SangJae Moon	Kyungpook National University, Korea
Yi Mu	University of Wollongong, Australia
Jesper Buus Nielsen	Aarhus University, Denmark
DaeHun Nyang	Inha University, Korea
Rolf Oppliger	eSECURITY technologies, Switzerland
Carles Padro	Technical University of Catalonia, Spain
Raphael Chung-Wei PHAN	Swinburne University of Technology, Malaysia
Josef Pieprzyk	Macquarie University, Australia
Vincent Rijmen	Graz University of Technology, Austria
Rei Safavi-Naini	University of Wollongong, Australia
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	Indian Statistical Institute, India
Nigel Smart	University of Bristol, UK
JungHwan Song	Hanyang University, Korea
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University, Hakodate, Japan
Wen-Guey Tzeng	National Chiao Tung University, Taiwan
Guilin Wang	Institute for Infocomm Research, Singapore
William Whyte	NTRU Cryptosystems, USA
Michael Wiener	Cryptographic Clarity, Canada
Chuan-Kun Wu	Chinese Academy of Sciences, China
Shouhuai Xu	The University of Texas at San Antonio, USA
Sung-Ming Yen	National Central University, Taiwan
Yongjin Yeom	NSRI, Korea
Moti Yung	Columbia University, USA

Organizing Committee Chair

Heekuck Oh	Hanyang University, Korea

Organizing Committee

Dowon Hong	ETRI, Korea
Daewoon Jeon	KIISC, Korea
Ji Hong Kim	Semyung University, Korea
Jung-Tae Kim	Mokwon University, Korea
Kyung Sim Kim	KIISC, Korea
Young Sub Koo	MIC, Korea
HyungWoo Lee	Hanshin University, Korea
Sangjin Lee	Korea University, Korea
Dong Gue Park	Soonchunhyang University, Korea
Sangwoo Park	NSRI, Korea
Kyung Hyune Rhee	Pukyong National University, Korea
Sang Uk Shin	Pukyong National University, Korea
Yoojae Won	KISA, Korea

External Reviewers

Joe Choo	Masayuki Abe	Caroline Kudla
Christophe Doche	Heng Swee Huay	Orr Dunkelman
Krystian Matusiewicz	Emily Shen	John Kelsey
Ron Steinfeld	Siu-Leung Chung	Stefan Lucks
Huaxiong Wang	Hongwei Sun	Jorge Nakahara Jr
Christian Rechberger	Martijn Stam	Frederic Valette
Norbert Pramstaller	Dan Page	Ju-Sung Kang
Florian Mendel	Pooya Farshim	Jehong Park
Sanjit Chatterjee	John Malone-Lee	Choong-Hoon Lee
Chien-Ning Chen	David Galindo	DongHoon Lee
Hsi-Chung Lin	Kumar Viswanath	Woong Hee Kim
Xinyi Huang	Steven Galbraith	Yung Hur
Fabien Laguillaumie	Kenny Paterson	Sang Woon Jang
Katja Schmidt-Samoa	John Malone-Lee	ChangKyun Kim
DongGuk Han	Carlos Cid	Hyunrok Lee
Michel Abdalla	Geraint Price	Zeen Kim
Dario Catalano	Maura Paterson	Vo Duc Liem
Sebastien Zimmer	Rui Zhang	Dang Nguyen Duc
Tetsu Iwata	Nuttapong Attrapadung	Jaemin Park
Takeshi Koshiba	Yang Cui	Sungcheol Heo
Hiroki Koga	SeongHan Shin	Youngjoon Seo

Sponsoring Institutions

MIC (Ministry of Information and Communication), Korea
IITA (Institute of Information Technology Assessment), Korea
Solmaze Co., Ltd., Korea
K-Bell Co., Ltd., Korea
HAN Infocomm Co., Ltd., Korea

Table of Contents

System/Network Security

Block/Stream Ciphers (I)

Block/Stream Ciphers (II)

Efficient Implementations

Digital Rights Management

Public Key Cryptography