Lecture Notes in Computer Science 4296

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

Min Surp Rhee Byoungcheon Lee (Eds.)

Information Security and Cryptology – ICISC 2006

9th International Conference
Busan, Korea, November 30 - December 1, 2006
Proceedings

Springer

Volume Editors

Min Surp Rhee
Dankook University
San 29, Anseo-dong, Cheonan-shi
Chungnam, 330-714, Korea
E-mail: msrhee@dankook.ac.kr

Byoungcheon Lee
Joongbu University
101 Daehak-Ro, Chubu-Myeon, Guemsan-Gun
Chungnam, 312-702, Korea
E-mail: sultan@joongbu.ac.kr

Library of Congress Control Number: 2006936103

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 3-540-49112-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-49112-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11927587 06/3142 5 4 3 2 1 0

Preface

ICISC 2006, the Ninth International Conference on Information Security and Cryptology was held in Busan, Korea, during November 30 - December 1, 2006. It was organized by the Korea Institute of Information Security and Cryptology (KIISC) in cooperation with the Ministry of Information and Communication (MIC), Korea. The aim of this conference was to provide a forum for the presentation of new results in research, development, and application in information security and cryptology. It also intended to be a place where research information can be exchanged.

Started in 1998, ICISC has grown into an important international conference in the information security and cryptology area with an established reputation. Based on this maturity, we tried an important change in the publication policy this year. Until last year, pre-proceedings were distributed at the conference and proceedings in Springer's *Lecture Notes in Computer Science* (LNCS) were published after the conference. This year ICISC proceedings were published in LNCS before the conference and distributed to the participants at the conference. We appreciate Springer for their full support and help in making this possible.

The conference received 129 submissions from 17 countries, covering all areas of information security and cryptology. The review and selection processes were carried out in two stages by the Program Committee of 57 prominent researchers via online meetings through the iChair Web server. First, each paper was blind reviewed by at least three PC members, 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 Program Committee finally selected 26 papers from 12 countries. The authors of selected papers had a few weeks to prepare final versions of their papers, aided by comments from the reviewers. The proceedings contain the revised versions of the accepted papers. However, most of these final revisions were not subject to any further editorial review.

The conference program included two invited talks from eminent researchers in information security and cryptology. Serge Vaudenay from EPFL gave an interesting talk on RFID privacy entitled "RFID Privacy Based on Public-Key Cryptography." Palash Sarkar from the Indian Statistical Institute talked on "Generic Attacks on Symmetric Ciphers," which showed various time-memory trade-off attacks on symmetric cipher algorithms.

We would like to thank everyone who contributed to the success of this conference. First, thanks to all the authors who submitted papers to this conference. Second, thanks to all 57 members of the Program Committee listed overleaf. It was a truly nice experience to work with such talented and hard-working researchers. Third, thanks to all the external reviewers for assisting the Program Committee in their particular areas of expertise. Fourth, we would like to thanks

all the participants of the event who made this event an intellectually stimulating one through their active contribution. We also would like to thank the iChair developers in EPFL for allowing us to use their software. Finally, we are delighted to acknowledge the partial financial support provided by Redgate, SECUi.COM, MarkAny, and EK Manpower.

November 2006

Min Surp Rhee
Byoungcheon Lee

Organization

General Chair

JooSeok Song	Yonsei University, Korea

Program Co-chairs

Min Surp Rhee	Dankook University, Korea
Byoungcheon Lee	Joongbu University, Korea

Program Committee

Giuseppe Ateniese	The Johns Hopkins University, USA
Joonsang Baek	Institute for Infocomm Research, Singapore
Alex Biryukov	University of Luxembourg, Luxembourg
John Black	University of Colorado, USA
Jean-Sebastien Coron	University of Luxembourg, Luxembourg
Jung Hee Cheon	Seoul National University, Korea
Kyo-il Chung	ETRI, Korea
Ed Dawson	Queensland University of Technology, Australia
Yevgeniy Dodis	New York University, USA
Serge Fehr	CWI Amsterdam, Netherlands
Pierre-Alain Fouque	Ecole Normale Superieure, France
Marc Girault	France Telecom, France
Philippe Golle	Palo Alto Research Center, USA
Dieter Gollmann	Hamburg University of Technology, Germany
Yongfei Han	ONETS, China
Goichiro Hanaoka	AIST, Japan
Marc Joye	Gemplus, France
Jonathan Katz	University of Maryland, USA
Hiroaki Kikuchi	Tokai University, Japan
Hwankoo Kim	Hoseo University, Korea
Kwangjo Kim	ICU, Korea
Kaoru Kurosawa	Ibaraki University, Japan
Taekyoung Kwon	Sejong University, Korea
Chi Sung Laih	Kun Shan University, Taiwan
Kwok-Yan Lam	Tsinghua University, China
Dong Hoon Lee	Korea University, Korea
Pil Joong Lee	POSTECH, Korea
Sang-Ho Lee	Ewha Womans University, Korea
Arjen Lenstra	EPFL, Switzerland
Yingjiu Li	Singapore Management University, Singapore

Helger Lipmaa	Cybernetica AS and 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
Rei Safavi-Naini	Wollongong University, 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
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	Indian Statistical Institute, India
Nigel Smart	University of Bristol, UK
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University - Hakodate, Japan
Serge Vaudenay	EPFL, Switzerland
Guilin Wang	Institute for Infocomm Research, Singapore
William Whyte	NTRU Cryptosystems, USA
Michael Wiener	Cryptographic Clarity, Canada
Dongho Won	Sungkyunkwan University, Korea
Sung-Ming Yen	National Central University, Taiwan
Yongjin Yeom	NSRI, Korea
Fangguo Zhang	Sun Yat-sen University, China
Alf Zugenmaier	DoCoMo Euro-Labs, Germany

Organizing Chair

Kyung-Hyune Rhee	Pukyong National University, Korea

Organizing Committee

Chang Kyu Kim	Dong-eui University, Korea
Heekuck Oh	Hanyang University, Korea
Im-Yeong Lee	Soonchunhyang University, Korea
Sang-Uk Shin	Pukyong National University, Korea
Weon Shin	Tongmyong University, Korea
HoonJae Lee	Dongseo University, Korea
Dong Kyue Kim	Hanyang University, Korea

External Reviewers

Imad Aad
Imad Abbadi
Michelle Abdalla
Toru Akishita
Patrick Amon
Thomas Baigneres
Simon Blackburn
Marina Blanton
Brian Carrier
Michael Cheng
Sangrae Cho
Seokhyang Cho
Yong-Je Choi
Sherman Chow
Andrew Clark
Yang Cui
John Daugman
Alain Durand
Andrzej Drygajlo
Dang Nguyen Duc
Gerardo Fernandez
Matthieu Finiasz
Aline Gouget
Matthew Green
JaeCheol Ha
Genebeck Hahn
Javier Herranz
Susan Hohenberger
Jungdae Hong
Yoshiaki Hori
Jeffrey Horton
Xinyi Huang
John Ioannidis
Toshiyuki Isshiki
Tetsuya Izu
Jingak Jang
Ik rae Jeong
Seny Kamara
Jeonil Kang
Eike Kiltz
Hyung Chan Kim
Jonghyun Kim
Tae Hyun Kim
Youngsoo Kim
Shinsaku Kiyomoto
Tetsutaro Kobayashi
Divyan M. Konidala
Noboru Kunihiro
Nam-Suk Kwarc
Sven Lachmund
Julien Laganier
Vinh The Lam
HoonJae Lee
Jin Li
Wanqing Li
Hsi-Chung Lin
JongHyup Lee
MunKyu Lee
Soo-hyung Lee
Yunho Lee
Jiqiang Lu
Liang Lu
Tal Malkin
Kanta Matsuura
Breno de Medeiros
Kunihiko Miyazaki
George Mohay
Jean Monnerat
Dae Sung Moon
Kazuto Ogawa
Takeshi Okamoto
Dan Page
Jung Hyung Park
Sangjoon Park
Tae Jun Park
Sylvain Pasini
Geong Sen Poh
Rodrigo Roman
Louis Salvail
Farzad Salim
Christian Schaefer
Jae Woo Seo
Nicholas Sheppard
Jong Hoon Shin
SeongHan Shin
Douglas Sicker
Hongwei Sun
Clark Thomborson
Dongvu Tonien
Eran Tromer
Yoshifumi Ueshige
Masashi Une
Frederik Vercauteren
Duc Liem Vo
Martin Vuagnoux
Camille Vuillaume
Thomas Walter
Baodian Wei
Chung-Huang Yang
Yeon Hyeong Yang
Eunsun Yoo
Sung-Soo Yoon
Dae Hyun Yum
Rui Zhang
Chang'an Zhao
Sebastien Zimmer

Sponsoring Institutions

Redgate, Korea	http://www.redgate.co.kr/
SECUi.COM, Korea	http://www.secui.com/
MarkAny, Korea	http://www.markany.com/
EK Manpower, Korea	http://www.ekmanpower.co.kr/

Table of Contents

Network Security and Access Control

Mobile Communications Security

Forensics

Copyright Protection

Biometrics

Hash Functions – II

Public Key Cryptosystems

Digital Signatures