Lecture Notes in Computer Science 6829

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

Kyung-Hyune Rhee DaeHun Nyang (Eds.)

Information Security and Cryptology - ICISC 2010

13th International Conference
Seoul, Korea, December 1-3, 2010
Revised Selected Papers

Springer

Volume Editors

Kyung-Hyune Rhee
Pukyong National University
Department of IT Convergence Application Engineering
599-1 Daeyeon 3-Dong Namgu, Busan 608-737, Republic of Korea
E-mail: khrhee@pknu.ac.kr

DaeHun Nyang
INHA University
Department of Computer Science and Information Technology
253 Yonghyun-dong, Nam-gu, Incheon 402-751, Republic of Korea
E-mail: nyang@inha.ac.kr

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-24208-3 e-ISBN 978-3-642-24209-0
DOI 10.1007/978-3-642-24209-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011936884

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

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

ICISC 2010, the 13th International Conference on Information Security and Cryptology, was held in Seoul, Korea, during December 1–3, 2010. 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 intended to be a place where research information can be exchanged.

The conference received 99 submissions from 27 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 64 prominent experts 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 PC finally selected 28 papers from 16 countries. The acceptance rate was 28.2%. The authors of selected papers had a few weeks to prepare for their final versions based on the comments received from the 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 delivered by Tatsuaki Okamoto from NTT Information Sharing Platform Laboratories. The invited speakers were Sakir Sezer from ECIT SoC Research Division and Giuseppe Ateniese from The Johns Hopkins University.

There are many people who contributed to the success of ICISC 2010. We would like to thank all the authors who submitted papers to this conference. We are deeply grateful to all 64 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 also like to thank the iChair developers for allowing us to use their 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 and all organizing members who nicely managed the conference.

December 2010

Kyung-Hyune Rhee
DaeHun Nyang

Organization

ICISC 2010, The 13^{th} Annual International Conference on Information Security and Cryptology, was held during December 1–3, 2010, at Chung-Ang University, Seoul, Korea, and organized by Korea Institute of Information Security and Cryptology (KIISC) (http://www.kiisc.or.kr) in cooperation with the Ministry of Public Administration and Security (MOPAS) (http://www.mopas.go.kr)

General Chair

Jong In Lim	KIISC, Korea

Program Co-chairs

Kyung-Hyune Rhee	Pukyong National University, Korea
DaeHun Nyang	INHA university, Korea

Program Committee

Joonsang Baek	Institute for Infocomm Research, Singapore
Alex Biryukov	University of Luxembourg, Luxembourg
Seongtaek Chee	Attached Institute of ETRI, Korea
Jung Hee Cheon	Seoul National University, Korea
Yongwha Chung	Korea University, Korea
Paolo Milani Comparetti	Vienna University of Technology, Austria
Frëdëric 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
Louis Granboulan	EADS Innovation Works, France
Matthew Green	Independent Security Evaluators, USA
JaeCheol Ha	Hoseo University, Korea
Dong-Guk Han	Kookmin University, Korea
Martin Hell	Lunds Universitet, Sweden
Deukjo Hong	Attached Institute of ETRI, Korea
Jin Hong	Seoul National University, Korea
Seokhie Hong	Korea University, Korea
Jung Yeon Hwang	ETRI, Korea
David Jao	University of Waterloo, Canada

Ju-Sung Kang	Kookmin University, Korea
Ho-Won Kim	Pusan University, Korea
Jihye Kim	Seoul National University, Korea
Seungjoo Kim	Sungkyunkwan University, Korea
Taekyoung Kwon	Sejong University, Korea
Xuejia Lai	Shanghai Jiao Tong University, China
Byoungcheon Lee	Joongbu University, Korea
Im-Yeong Lee	Soonchunyang University, Korea
Mun-Kyu Lee	Inha University, Korea
Pil Joong Lee	Pohang University of Science and Technology, Korea
Mark Manulis	TU Darmstadt, Germany
Keith Martin	Royal Holloway, University of London, UK
Sjouke Mauw	University of Luxembourg, Luxembourg
Atsuko Miyaji	JAIST, Japan
Jose A. Montenegro	University of Malaga, Spain
David Naccache	ENS, France
Heekuck Oh	Hanyang University, Korea
Rolf Oppliger	eSECURITY Technologies, Switzerland
Raphael C.-W. Phan	Loughborough University, UK
Bart Preneel	K.U. Leuven, Belgium
Vincent Rijmen	K.U.Leuven and TU Graz, Belgium and Austria
Bimal Roy	Indian Statistical Institute, India
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	Indian Statistical Institute, India
Kyung-Ah Shim	NIMS, Korea
Sang-Uk Shin	Pukyong University, Korea
Hong-Yeop Song	Yonsei 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
Jorge Villar	Universitat Politecnica de Catalunya, Spain
Sung-Ming Yen	National Central University, Taiwan
Jeong Hyun Yi	Soongsil University, Korea
Kangbin Yim	Soonchunyang University, Korea
Myungkeun Yoon	Kookmin University, Korea
Dae Hyun Yum	Pohang University of Science and Technology, Korea
Fangguo Zhang	Sun Yat-sen University, China
Jianying Zhou	I2R, Singapore

Organizing Committee Chair

Sehyun Park	Chung-Ang University, Seoul, Korea

Organizing Committee Vice-Chair

Eul Gyu Im	Hanyang University, Seoul, Korea

Organizing Committee

Jong-Soo Jang	ETRI, Korea
Dong-Kyue Kim	Hanyang University, Korea
Daesung Kwon	Attached Institute of ETRI, Korea
Im-Yeong Lee	Soonchunhyang University, Korea
Mun-Kyu Lee	Inha University, Korea
Yongsu Park	Hanyang University, Korea
Jungtaek Seo	Attached Institute of ETRI, Korea
Kyung-Ah Shim	NIMS, Korea
Yoo-jae Won	KISA, Korea
Jeong Hyun Yi	Soongsil University, Korea

External Reviewers

Anna Lisa Ferrara
Antonio Muñoz
Benedikt Gierlichs
Bin Zhang
Bo Zhu
Bonwook Koo
Cheol-Min Park
Chunhua Su
Claudio Soriente
Daeseon Choi
Daesung Kwon
Eun Sung Lee
Gunil Ma
Hakan Seyalioglu
Hans Loehr
Hee-Seok Kim
HongTae Kim
Hsi-Chung Lin
Hugo Jonker
Hyeong-Chan Lee
Hyun-Dong So
Hyung Tae Lee
Hyun-Min Kim
Isaac Agudo
Ivica Nikolic
Jae Ahn Hyun
Jae Hong Seo
Jae Woo Seo
Jangseung Kim
Jeonil Kang
Jheng-Hong Tu
Ji Young Chun
Jihye Kim
Joaquin Garcia-Alfaro
Johann Großschädl
Joseph K. Liu
Jun Pang
Jung Youl Park
Kai Yuen Cheong
Kazuhiko Minematsu
Kazumasa Omote
Kenneth Matheis

Lingling Xu
Luca Davi
Maki Shigeri
Martin Ågren
Ming Duan
Mingwu Zhang
Minkyu Kim
Moonsung Lee
MyungKeun Yoon
Myungsun Kim
Nicky Mouha
Özgür Dagdelen
Paul Stankovski
Pedro Peris-Lopez
Pieter Verhaeghe
Ping Wang
Qiping Lin
Ralf-Philipp Weinmann
Rishiraj Bhattacharyya
Ruei-Hau Hsu
Ryoji Ohta
Sangrae Cho
Sasa Radomirovic
Sebastian Faust
Seog Chung Seo
Somindu C. Ramanna
Sanjay Bhattacherjee
Subhabrata Samajder
Sung-Kyung Kim
Sungwook Eom
Sung-Wook Lee
Taechan Kim
Takashi Nishide
Takeshi Kawabata
Taku Hayashi
Tamer AbuHmed
Teruo Saito
Thomas Baigneres
Thomas Schneider
Ton van Deursen
Vincent Naessens
Wei-Chih Lien
Xingwen Zhao
Xinyi Huang
Yanjiang Yang
Yasufumi Hashimoto
Yeonkyu Kim
Ying Qiu
Young-In Cho
YoungJae Maeng
Young-Ran Lee
YoungSeob Cho
Younho Lee
Youn-Taek Young
Yu Sasaki
Kenji Ohkuma
Zayabaatar
Zheng Gong

Sponsoring Institutions

National Security Research Institute (NSRI)
Electronics and Telecommunications Research Institute (ETRI)
Korea Internet & Security Agency (KISA)
Korean Federation of Science and Technology Societies (KOFST)
Chung-Ang University Home Network Research Center (CAU HNRC)
Chungnam National University Internet Intrusion Response Technology Research Center (CNU IIRTRC)
Korea University Center for Information Security Technologies (KU CIST)

Table of Contents

Cryptanalysis

Cryptographic Algorithms

Implementation

Network and Mobile Security

Symmetric Key Cryptography

Cryptographic Protocols

Side Channel Attack