Lecture Notes in Computer Science 7839

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

Taekyoung Kwon Mun-Kyu Lee
Daesung Kwon (Eds.)

Information Security and Cryptology – ICISC 2012

15th International Conference
Seoul, Korea, November 28-30, 2012
Revised Selected Papers

Springer

Volume Editors

Taekyoung Kwon
Sejong University
Department of Computer Engineering
Seoul 143-747, Korea
E-mail: tkwon@sejong.edu

Mun-Kyu Lee
Inha University
School of Computer and Information Engineering
Incheon 402-751, Korea
E-mail: mklee@inha.ac.kr

Daesung Kwon
National Security Research Institute
Daejeon 306-600, Korea
E-mail: ds_kwon@ensec.re.kr

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-37681-8 e-ISBN 978-3-642-37682-5
DOI 10.1007/978-3-642-37682-5
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013935780

CR Subject Classification (1998): E.3, K.6.5, C.2, D.4.6, G.2.1, E.4, J.1

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 2012, the 15th International Conference on Information Security and Cryptology, was held in Seoul, Korea, during November 28–30, 2012. This year the conference was hosted by the KIISC (Korea Institute of Information Security and Cryptology) jointly with the NSRI (National Security Research Institute), in cooperation with the Ministry of Public Administration and Security (MOPAS).

The aim of this conference is to provide an international forum for the latest results of research, development, and applications in the field of information security and cryptology. This year we received 120 submissions from more than 20 countries and were able to accept 32 papers from 13 countries, with the acceptance rate of 26.7%. The review and selection processes were carried out by the Program Committee (PC) members, 88 prominent experts world-wide, via Springer's OCS system. First, each paper was blind reviewed by at least three PC members. Second, to resolve conflicts in the reviewer's decisions, the individual review reports were open to all PC members, and detailed interactive discussions on each paper ensued. For the LNCS post-proceedings, the authors of selected papers had a few weeks to prepare their final versions based on the comments received from the reviewers. We also recommended that authors should revise their papers based on the comments and recommendations they might have received from attendees upon their presentations at the conference.

The conference featured three invited talks: "Machine Learning on Encrypted Data" delivered by Kristin Lauter, Microsoft Research; "Another Look at Affine-Padding RSA Signatures" by David Naccache, Ecole Normale Superieure; and "New Meet-in-the-Middle Attacks in Symmetric Cryptanalysis" by Christian Rechberger, Technical University of Denmark. We thank the invited speakers for their kind acceptance and nice presentations.

We would like to thank all the authors who submitted their papers to ICISC 2012 and all 88 PC members. It was a truly nice experience to work with such talented and hard-working researchers. We also appreciate the external reviewers for assisting the PC members in their particular areas of expertise. Finally, we would like to thank all attendees for their active participation and the Organizing Committee Members, who nicely managed this conference. We look forward to next year's ICISC.

January 2013

Taekyoung Kwon
Mun-Kyu Lee
Daesung Kwon

ICISC 2012

The 15th Annual International Conference
on Information Security

November 28–30, 2012
Konkuk University, Seoul, Korea

Hosted by
Korea Institute of Information Security and Cryptology (KIISC)
National Security Research Institute (NSRI)

Supported by
Ministry of Public Administration and Security (MOPAS)
Electronics and Telecommunications Research Institute (ETRI)
Korea Internet & Security Agency (KISA)
The Korean Federation of Science and Technology Societies (KOFST)

General Chairs

Chang-Seop Park	KIISC and Dankook University, Korea
Seokyoul Kang	NSRI, Korea

Program Co-chairs

Taekyoung Kwon	Sejong University, Korea
Mun-Kyu Lee	Inha University, Korea
Daesung Kwon	NSRI, Korea

Program Committee

Frederik Armknecht	University of Mannheim, Germany
Joonsang Baek	KUSTAR, UAE
Alex Biryukov	University of Luxembourg, Luxembourg
Zhenfu Cao	Shanghai Jiao Tong University, China
Aldar C-F. Chan	Institute for Infocomm Research, Singapore
Ku-Young Chang	ETRI, Korea
Kefei Chen	Shanghai Jiaotong University, China
Jung Hee Cheon	Seoul National University, Korea
Yongwha Chung	Korea University, Korea
Nora Cuppens-Boulahia	TELECOM Bretagne, France

Paolo D'Arco	University of Salerno, Italy
Bart De Decker	IBBT-DistriNet, KU Leuven, Belgium
Rafael Dowsley	University of California, San Diego, USA
Shaojing Fu	National University of Defense Technology, China
David Galindo	University of Luxembourg, Luxembourg
Dieter Gollmann	Security in Distributed Applications
Louis Granboulan	EADS Innovation Works, France
Johann Groszschaed	University of Luxembourg, Luxembourg
JaeCheol Ha	Hoseo University, Korea
Dong-Guk Han	Kookmin University, Korea
Martin Hell	Lund University, Sweden
Swee-Huay Heng	Multimedia University, Malaysia
Deukjo Hong	NSRI, Korea
Dowon Hong	Kongju National University, Korea
Jin Hong	Seoul National University, Korea
Seokhie Hong	Korea University, Korea
Jiankun Hu	UNSW, Australia
Jung Yeon Hwang	ETRI, Korea
Eul Gyu Im	Hanyang University, Korea
David Jao	University of Waterloo, Canada
Hiroaki Kikuchi	Tokai University, Japan
Ji Hye Kim	Kookmin University, Korea
Howon Kim	Pusan National University, Korea
Huy Kang Kim	Korea University, Korea
Shinsaku Kiyomoto	KDDI R&D Laboratories Inc., Japan
Hyang-Sook Lee	Ewha Womans University, Korea
JongHyup Lee	Korea National University of Transportation, Korea
Jooyoung Lee	Sejong University, Korea
Pil Joong Lee	POSTECH, Korea
Su Mi Lee	Financial Security Agency, Korea
Dongdai Lin	Institute of Software, ISCAS, China
Mark Manulis	University of Surrey, UK
Sjouke Mauw	University of Luxembourg, Luxembourg
Atsuko Miyaji	JAIST, Japan
Yutaka Miyake	KDDI R&D Laboratories Inc., Japan
Abedelaziz Mohaisen	Verisign labs, USA
Jose A. Montenegro	Universidad de Malaga, Spain
Fidel Nemenzo	University of the Philippines, Philippines
DaeHun Nyang	Inha University, Korea
Heekuck Oh	Hanyang University, Korea
Tae (Tom) Oh	Rochester Institute of Technology, USA
Rolf Oppliger	eSECURITY Technologies, Switzerland
Daniel Page	University of Bristol, UK

Susan Pancho-Festin	University of the Philippines, Philippines
Omkant Pandey	Microsoft Research India, India / University of Texas, Austin, USA
Raphael C.-W. Phan	Multimedia University, Malaysia
Christian Platzer	Automation Systems Group at the Technical University of Vienna, Austria
Carla Ráfols	Ruhr-Universität Bochum, Germany
C. Pandu Rangan	Indian Institute of Technology Madras, India
Christian Rechberger	DTU, Denmark
Vincent Rijmen	Katholieke Universiteit Leuven, Belgium
Bimal Roy	Indian Statistical Institute, India
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	Indian Statistical Institute, India
Nitesh Saxena	University of Alabama, Birmingham, USA
Ji Sun Shin	Sejong University, Korea
Sang Uk Shin	Pukyong National University, Korea
Hong-Yeop Song	Yonsei University, Korea
Rainer Steinwandt	Florida Atlantic University, USA
Hung-Min Sun	National Tsing Hua University, Taiwan
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Kyushu University, Japan
Yukiyasu Tsunoo	NEC Corporation, Japan
Marion Videau	University of Lorraine / LORIA, France
Jorge Villar	Universitat Politecnica de Catalunya, Spain
Yongzhuang Wei	Guilin University of Electronic Technology, China
Wenling Wu	SKLOIS, Chinese Academy of Sciences, China
Toshihiro Yamauchi	Okayama University, Japan
Wei-Chuen Yau	Multimedia University, Malaysia
Ching-Hung Yeh	Far East University, Taiwan
Sung-Ming Yen	National Central University, Taiwan
Yongjin Yeom	Kookmin University, Korea
Jeong Hyun Yi	Soongsil University, Korea
Kazuki Yoneyama	NTT, Japan
Myungkeun Yoon	Kookmin University, Korea
Dae Hyun Yum	Myongji University, Korea
Aaram Yun	UNIST, Korea
Fangguo Zhang	Sun Yat-sen University, China

Organizing Chair

Dong Il Seo	ETRI, Korea

Organizing Committee

Heuisu Ryu	Gyeongin National University of Education, Korea
Hokun Moon	KT, Korea
Howon Kim	Pusan National University, Korea
Jason Kim	Korea Internet & Security Agency, Korea
Keecheon Kim	Konkuk University, Korea
Soohyun Oh	Hoseo University, Korea
Tae-Hoon Kim	SYWORKS, Korea
Young-Ho Park	Sejong Cyber University, Korea

Table of Contents

Cryptographic Protocol

Identity-Based Encryption

Efficient Implementation

Cloud Computing Security

Cryptanalysis II

Side Channel Analysis

Digital Signature

Privacy Enhancement

Erratum