Lecture Notes in Computer Science 6047

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

Jin Kwak Robert H. Deng Yoojae Won
Guilin Wang (Eds.)

Information Security Practice and Experience

6th International Conference, ISPEC 2010
Seoul, Korea, May 12-13, 2010
Proceedings

Springer

Volume Editors

Jin Kwak
Soonchunhyang University
Department of Information Security Engineering
646 Eupnae-ri, Shinchang-myun, Asan-si, Chungcheongnam-do, 336-745, Korea
E-mail: jkwak@sch.ac.kr

Robert H. Deng
Singapore Management University
School of Information Systems
469 Bukit Timah Road, 259756, Singapore
E-mail: robertdeng@smu.edu.sg

Yoojae Won
Korea Internet and Security Agency
Internet and Security Policy Division
Daedong B/D, Garak-dong 79-3, Songpa-gu, Seoul, 138-950, Korea
E-mail: yjwon@kisa.or.kr

Guilin Wang
University of Birmingham
School of Computer Science
Birmingham, B15 2TT, UK
E-mail: g.wang@cs.bham.ac.uk

Library of Congress Control Number: 2010925440

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, J.1, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-12826-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-12826-4 Springer Berlin Heidelberg New York

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

Preface

The 6th International Conference on Information Security Practice and Experience (ISPEC 2010) was held in Seoul, Korea, May 12–13, 2010.

The ISPEC conference series is an established forum that brings together researchers and practitioners to provide a confluence of new information security technologies, including their applications and their integration with IT systems in various vertical sectors. In previous years, ISPEC has taken place in Singapore (2005), Hangzhou, China (2006), Hong Kong, China (2007), Sydney, Australia (2008), and Xi'an, China (2009). For all sessions, as this one, the conference proceedings were published by Springer in the *Lecture Notes in Computer Science* series.

In total, 91 papers from 18 countries were submitted to ISPEC 2010, and 28 were selected for inclusion in the proceedings (acceptance rate 30%). The accepted papers cover multiple topics of information security and applied cryptography. Each submission was anonymously reviewed by at least three reviewers. We are grateful to the Program Committee, which was composed of more than 56 well-known security experts from 16 countries; we heartily thank them as well as all external reviewers for their time and valued contributions to the tough and time-consuming reviewing process.

The conference was hosted by Soonchunhyang University, Korea, supported by Korea Internet & Security Agency (KISA), Korea; Electronics and Telecommunications Research Institute (ETRI), Korea, in Corporation with Korea Institute of Information Security & Cryptography (KIISC), Korea, and sponsored by Korea Communications Commission (KCC), Korea. We sincerely thank the Honorary Chair and the General Chairs of ISPEC 2010 for their strong support. We also thank the System Management Chair for managing the conference website, and the Organizing Chair and Committee for dealing with local issues.

There are many people who contributed to the success of ISPEC 2010. We would like to thank all authors from around the world for submitting and presenting their papers. We are deeply grateful to the Program Committee members for their fair review. It would have been impossible to organize ISPEC 2010 without the hard work of all our Chairs and Committees. Finally, we would like to thank all the participants for their contribution to ISPEC 2010.

May 2010

Jin Kwak
Robert H. Deng
Yoojae Won
Guilin Wang

ISPEC 2010

6th International Conference
on Information Security Practice and Experience

Seoul, Korea
May 12–13, 2010

Hosted by

Soonchunhyang University, Korea

Supported by

Korea Internet & Security Agency (KISA), Korea
Electronics and Telecommunications Research Institute (ETRI), Korea

In Corporation with

Korea Institute of Information Security & Cryptography (KIISC), Korea

Sponsored by

Korea Communications Commission (KCC), Korea

Honorary Chair

Heejung Kim	Korea Internet & Security Agency (KISA), Korea

General Chairs

Heung Youl Youm	Soonchunhyang University, Korea
Jong in Im	Korea University, Korea
Feng Bao	Institute for Infocomm Research (I^2R), Singapore

Program Chairs

Jin Kwak	Soonchunhyang University, Korea
Robert H. Deng	Singapore Management University, Singapore
Yoojae Won	Korea Internet & Security Agency (KISA), Korea

Program Committee

Joonsang Baek	Institute for Infocomm Research (I^2R), Singapore
Kefei Chen	Shanghai Jiaotong University, China
Liqun Chen	Hewlett-Packard Laboratories, UK

Hyoung-Kee Choi	Sungkyunkwan University, Korea
Debbie Cook	Telcordia, USA
Xuhua Ding	Singapore Management University, Singapore
Clemente Galdi	Università di Napoli "Federico II", Italy
David Galindo	University of Luxembourg, Luxembourg
Dong-Guk Han	Kookmin University, Korea
N. Jaisankar	VIT University, India
Stefan Katzenbeisser	Technical University of Darmstadt, Germany
Hyong-Shik Kim	Chungnam National University, Korea
Jeasung Kim	Korea Internet & Security Agency (KISA), Korea
Rack-Hyun Kim	Soonchunhyang University, Korea
Xuejia Lai	Shanghai Jiao Tong University, China
Deok Gyu Lee	ETRI, Korea
Sunyoung Lee	Soonchunhyang University, Korea
Yunho Lee	Sungkyunkwan University, Korea
Tieyan Li	Institute for Infocomm Research (I^2R), Singapore
Yingjiu Li	Singapore Management University, Singapore
Benoît Libert	Universite Catholique de Louvain, Belgium
Chae Hoon Lim	Sejong University, Korea
Dongdai Lin	SKLOIS, Chinese Academy of Sciences, China
Masahiro Mambo	University of Tsukuba, Japan
Atsuko Miyaji	JAIST, Japan
Yi Mu	University of Wollongong, Australia
Nhut Nguyen	Samsung Telecommunications America, USA
SooHyun Oh	Hoseo University, Korea
Daniel Page	University of Bristol, UK
Namje Park	UCLA, USA
Raphael C.-W. Phan	Loughborough University, UK
C. Pandu Rangan	Indian Institute of Technology Madras, India
Mark Ryan	University of Birmingham, UK
Jorge Villar Santos	UPC, Spain
Hee Suk Seo	Korea University of Technology and Education, Korea
SeongHan Shin	AIST, Japan
Alice Silverberg	University of California, Irvine, USA
Kyungho Son	Korea Internet & Security Agency (KISA), Korea
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University Hakodate, Japan
Toshiaki Tanaka	KDDI R&D Laboratories Inc., Japan
Zhiguo Wan	Tsinghua University, China
Huaxiong Wang	Nanyang Technological University, Singapore
Lina Wang	Wuhan University, China

Duncan Wong	City University of Hong Kong, Hong Kong
Yongdong Wu	Institute for Infocomm Research (I^2R), Singapore
Chaoping Xing	Nanyang Technological University, Singapore
Wei Yan	Trendmicro, USA
Chung-Huang Yang	National Kaohsiung Normal University, Taiwan
Wansuck Yi	Korea Internet & Security Agency (KISA), Korea
Yunlei Zhao	Fudan University, China
Fangguo Zhang	Sun Yat-Sen University, China
Rui Zhang	AIST, Japan
Jianying Zhou	Institute for Infocomm Research (I^2R), Singapore
Bo Zhu	Concordia University, Canada
Huafei Zhu	Institute for Infocomm Research (I^2R), Singapore

Publication Chair

Guilin Wang	University of Birmingham, UK

Organizing Committee Chair

Ji Hong Kim	Semyung University, Korea

Organizing Committee

JaeCheol Ha	Hoseo University, Korea
Jongsoo Jang	ETRI, Korea
Hyuncheol Jeong	KISA, Korea
DaeHun Nyang	Inha University, Korea
Dong Gue Park	Soonchunhyang University, Korea
Gwangsoo Rhee	Sookmyung Women's University, Korea
Jeong-Mo Yang	Joongbu University, Korea
Kangbin Yim	Soonchunhyang University, Korea

System Management Chairs

Min Hong	Soonchunhyang University, Korea
Sang-Soo Yeo	Mokwon Univeristy, Korea

External Reviewers

Jianhong Chen
Xiaofeng Chen
Donghyun Choi
Hyunwoo Choi
Sherman Chow
C. Clough
Ton van Deursen
Oriol Farras
Ge Fu
Woong Go
Zheng Gong
Hui-Ting Hsieh
Qiong Huang
JoungYoun Hwang
Moonyoung Hwang
Jaehoon Jang
Heasuk Jo
HeeSeok Kim
Jongsung Kim
Junsub Kim
Woo Kwon Koo
Noboru Kunihiro
Hidenori Kuwakado
Taekyoung Kwon
Fabien Laguillaumie
Junzuo Lai
Byunghee Lee
Dongbum Lee
Jesang Lee
Kwangwoo Lee
Youngsook Lee
Yan Li
Joseph Liu
Yiyuan Luo
Xianping Mao
Takahiro Matsuda
Chihiro Ohyama
Daesick Park
Mathieu Renauld
Francesco Sica
Chunhua Su
Koutarou Suzuki
Qiang Tang
Isamu Teranishi
Jie Wang
Yongtao Wang
Baodian Wei
Jian Weng
Kuo-Hui Yeh
Dongu Yeo
TaeYoung Youn
Mingwu Zhang
Benwen Zhu
Bo Zhu

Table of Contents

Cryptanalysis

Algorithms and Implementations (I)

Algorithms and Implementations (II)

Network Security

Access Control

Identity Management

Trust Management

Public Key Cryptography

Security Applications