Lecture Notes in Computer Science 5451

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

Feng Bao Hui Li Guilin Wang (Eds.)

Information Security Practice and Experience

5th International Conference, ISPEC 2009
Xi'an, China, April 13-15, 2009
Proceedings

Springer

Volume Editors

Feng Bao
Institute for Infocomm Research (I^2R)
1 Fusionopolis Way, 19-01 Connexis (South Tower)
Singapore 138632, Singapore
E-mail: baofeng@i2r.a-star.edu.sg

Hui Li
Xidian University
School of Telecommunications Engineering
2 South Taibai Road, Xi'an, Shaanxi 710071, China
E-mail: xd.lihui@gmail.com

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

Library of Congress Control Number: Applied for

CR Subject Classification (1998): E.3, D.4.6, C.2.0, H.2.0, K.6.5, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-00842-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-00842-9 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12642663 06/3180 5 4 3 2 1 0

Preface

The 5th International Conference on Information Security Practice and Experience (ISPEC 2009) was held in Xi'an, China, April 13–15, 2009.

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), and Sydney, Australia (2008). For all sessions, as this one, the conference proceedings were published by Springer in the *Lecture Notes in Computer Science* series.

In total, 147 papers from 26 countries were submitted to ISPEC 2009, and 34 were finally selected for inclusion in the proceedings (acceptance rate 23%). 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 40 well-known security experts from 15 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.

In addition to the regular paper presentations, the program also featured four invited talks by Yupu Hu, from Xidian University, China; Youki Kadobayashi, from Nara Institute of Science and Technology, Japan; Mark Ryan, from the University of Birmingham, UK; and Gene Tsudik, from the University of California at Irvine, USA. We are grateful to them for accepting our invitation to speak at the conference.

The conference was organized and sponsored by Xidian University, China, co-organized by the School of Telecommunications Engineering, Xidian University, China; the Key Laboratory of Computer Networks and Information Security, Ministry of Education, China; and the National 111 Program of Introducing Talents of Discipline to Universities on Fundamental Theory and Technology of Modern Wireless Information Networks, China.

Special thanks are due to Ying Qiu for managing the review system, Libin Zhao for maintaining the conference website, and the Organizing Committee for dealing with local issues.

Last but not least, we would like to thank all the authors who submitted their papers to ISPEC 2009, and all the attendees from all over the world.

April 2009

Feng Bao
Hui Li
Guilin Wang

ISPEC 2009

5th International Conference
on Information Security Practice and Experience

Xi'an, China
April 13–15, 2009

Organized and Sponsored by

Xidian University, China

Co-organized by

School of Telecommunications Engineering, Xidian University, China.
Key Laboratory of Computer Networks and Information Security,
Ministry of Education, China.
National 111 Program of Introducing Talents of Discipline to
Universities on Fundamental Theory and Technology of
Modern Wireless Information Networks, China

General Chairs

Robert H. Deng	Singapore Management University, Singapore
Jianfeng Ma	Xidian University, China

Program Chairs

Feng Bao	I^2R, Singapore
Hui Li	Xidian University, China

Publication Chair

Guilin Wang	University of Birmingham, UK

Organizing Committee Chairs

Qingqi Pei	Xidian University, China
Xiaoyan Zhu	Xidian University, China
Yuanyuan Zuo	Xidian University, China

Program Committee

Kefei Chen	Shanghai Jiaotong University, China
Lily Chen	NIST, USA
Liqun Chen	HP Labs, UK
Dooho Choi	ETRI, Korea
Ed Dawson	QUT, Australia
Dengguo Feng	Chinese Academy of Sciences, China
Clemente Galdi	University of Naples "Federico II", Italy
David Galindo	ENS, France
Dieter Gollmann	TU Hamburg, Germany
Guang Gong	University of Waterloo, Canada
Javier Herranz	IIIA, Spain
Yupu Hu	Xidian University, China
Aggelos Kiayias	University of Connecticut, USA
Miroslaw Kutylowski	Wroclaw University of Technology, Poland
Jin Kwak	Soonchunhyang University, Korea
Xuejia Lai	Shanghai Jiaotong University, China
Benoît Libert	UCL, Belgium
Javier Lopez	University of Malaga, Spain
Michael Locasto	Dartmouth College, USA
Atsuko Miyaji	JAIST, Japan
Yi Mu	University of Wollongong, Australia
Elisabeth Oswald	University of Bristol, UK
Olivier Pereira	UCL, Belgium
Josef Pieprzyk	Macquarie University, Australia
Mark Ryan	University of Birmingham, UK
Sattar B. Sadkhan	University of Babylon, Iraq
Kouichi Sakurai	Kyushu University, Japan
Alice Silverberg	University of California at Irvine, USA
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University Hakodate, Japan
Toshiaki Tanaka	KDDI R&D Labs, Japan
Allan Tomlinson	Royal Holloway, UK
Jorge Villar	Universitat Politecnica de Catalunya, Spain
Guilin Wang	University of Birmingham, UK
Duncan Wong	City University of Hong Kong, China
Yongdong Wu	I^2R, Singapore
Chaoping Xing	NTU, Singapore
Heung Youl Youm	Soonchunhyang University, Korea
Fangguo Zhang	Sun Yat-Sen University, China
Rui Zhang	AIST, Japan
Huafei Zhu	I^2R, Singapore

External Reviewers

Toru Akishita
Nuttapong Attrapadung
Man Ho Au
Luigi Catuogno
Witold Charatonik
Jianhong Chen
Shengli Chen
Xiaofeng Chen
Tom Chothia
Jacek Cichon
Stefan Ciobaca
Baudoin Collard
Paolo D'Arco
Vanesa Daza
Hiroshi Doi
Ming Duan
Xinxin Fan
Hossein Ghodosi
Dong-Guk Han
Wei Han
Xuan Hong
Honggang Hu
Qiong Huang
Xinyi Huang
Vincenzo Iovino
Yuichi Kaji
John Kelsey
Ikkyun Kim
Juhan Kim
Namshik Kim
Fagen Li
Jin Li
Xiangxue Li
Zhijun Li
Joseph Liu
Yu Long
Krzysztof Majcher
Mark Manulis
Gogolewski Marcin
Andrew Moss
Mridul Nandi
Shivaramakrishnan Narayan
David Nowak
Kyunghee Oh
Takeshi Okamoto
Kazumasa Omote
Jose Antonio Onieva
Souradyuti Paul
Ray Perlner
Jason Reid
Chun Ruan
Germán Sáez
Masaaki Shirase
Leonie Simpson
Nigel Smart
Jason Smith
Ben Smyth
Marianne Swanson
Qiang Tang
Isamu Teranishi
Damien Vergnaud
Yongtao Wang
Bogdan Warinschi
Ralf-Philipp Weinmann
Wu Wei
Mi Wen
Yamin Wen
Stephen Wolthusen
Fubiao Xia
Jing Xu
Lingling Xu
Guomin Yang
Rehana Yasmin
Reza Z'Aba
Jinmin Zhong

Table of Contents

Public Key Encryption

Digital Signatures

System Security

Applied Cryptography

Multimedia Security and DRM

Security Protocols

Key Exchange and Management

Hash Functions and MACs

Cryptanalysis

Network Security

Security Applications