

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Alfred Kobsa

*University of California, Irvine, CA, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*University of Dortmund, Germany*

Madhu Sudan

*Massachusetts Institute of Technology, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

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

## Volume Editors

Feng Bao

Institute for Infocomm Research (I<sup>2</sup>R)  
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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

[springer.com](http://springer.com)

© Springer-Verlag Berlin Heidelberg 2009  
Printed in Germany

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  
Jianfeng Ma

Singapore Management University, Singapore  
Xidian University, China

## Program Chairs

Feng Bao  
Hui Li

I<sup>2</sup>R, Singapore  
Xidian University, China

## Publication Chair

Guilin Wang

University of Birmingham, UK

## Organizing Committee Chairs

Qingqi Pei  
Xiaoyan Zhu  
Yuanyuan Zuo

Xidian University, China  
Xidian University, China  
Xidian University, China

**Program Committee**

Kefei Chen	Shanghai Jiaotong University, China
Lily Chen	NIST, USA
Liqun Chen	HP Labs, UK
Doocho 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
Mirosław Kutylowski	Wrocław 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 Politècnica de Catalunya, Spain
Guilin Wang	University of Birmingham, UK
Duncan Wong	City University of Hong Kong, China
Yongdong Wu	I <sup>2</sup> R, 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 <sup>2</sup> R, 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

Efficient and Provable Secure Ciphertext-Policy Attribute-Based Encryption Schemes . . . . .	1
<i>Luan Ibraimi, Qiang Tang, Pieter Hartel, and Willem Jonker</i>	
A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length . . . . .	13
<i>Keita Emura, Atsuko Miyaji, Akito Nomura, Kazumasa Omote, and Masakazu Soshi</i>	
RSA-Based Certificateless Public Key Encryption . . . . .	24
<i>Junzuo Lai, Robert H. Deng, Shengli Liu, and Weidong Kou</i>	

## Digital Signatures

Strongly Unforgeable ID-Based Signatures without Random Oracles . . . .	35
<i>Chifumi Sato, Takeshi Okamoto, and Eiji Okamoto</i>	
On the Security of a Certificate-Based Signature Scheme and Its Improvement with Pairings . . . . .	47
<i>Jianhong Zhang</i>	

## System Security

An Empirical Investigation into the Security of Phone Features in SIP-Based VoIP Systems . . . . .	59
<i>Ruishan Zhang, Xinyuan Wang, Xiaohui Yang, Ryan Farley, and Xuxian Jiang</i>	
Reconstructing a Packed DLL Binary for Static Analysis . . . . .	71
<i>Xianggen Wang, Dengguo Feng, and Purui Su</i>	
Static Analysis of a Class of Memory Leaks in TrustedBSD MAC Framework . . . . .	83
<i>Xinsong Wu, Zhouyi Zhou, Yeping He, and Hongliang Liang</i>	

## Applied Cryptography

Efficient Concurrent $n^{\text{poly}(\log n)}$ -Simulatable Argument of Knowledge . . .	93
<i>Guifang Huang, Dongdai Lin, and Yanshuo Zhang</i>	



New Constructions for Reusable, Non-erasure and Universally Composable Commitments . . . . .	102
<i>Huafei Zhu</i>	
Certificateless Hybrid Signcryption . . . . .	112
<i>Fagen Li, Masaaki Shirase, and Tsuyoshi Takagi</i>	
On Non-representable Secret Sharing Matroids . . . . .	124
<i>Qi Cheng, Yong Yin, Kun Xiao, and Ching-Fang Hsu</i>	

## Multimedia Security and DRM

A Novel Adaptive Watermarking Scheme Based on Human Visual System and Particle Swarm Optimization . . . . .	136
<i>Shaomin Zhu and Jianming Liu</i>	
Defending against the Pirate Evolution Attack . . . . .	147
<i>Hongxia Jin and Jeffrey Lotspiech</i>	
Security Specification for Conversion Technologies of Heterogeneous DRM Systems . . . . .	159
<i>Heasuk Jo, Woongryul Jeon, Yunho Lee, Seungjoo Kim, and Dongho Won</i>	

## Security Protocols

Analysing Protocol Implementations . . . . .	171
<i>Anders Moen Hagalisletto, Lars Strand, Wolfgang Leister, and Arne-Kristian Groven</i>	
Measuring Anonymity . . . . .	183
<i>Xiaojuan Cai and Yonggen Gu</i>	
A Hybrid E-Voting Scheme . . . . .	195
<i>Kun Peng</i>	

## Key Exchange and Management

A Framework for Authenticated Key Exchange in the Standard Model . . . . .	207
<i>Shuhua Wu and Yuefei Zhu</i>	
Secret Handshake: Strong Anonymity Definition and Construction . . . . .	219
<i>Yutaka Kawai, Kazuki Yoneyama, and Kazuo Ohta</i>	
An Extended Authentication and Key Agreement Protocol of UMTS . . . . .	230
<i>Farshid Farhat, Somayeh Salimi, and Ahmad Salah</i>	

Hash-Based Key Management Schemes for MPEG4-FGS . . . . .	245
<i>Mohamed Karroumi and Ayoub Massoudi</i>	

## Hash Functions and MACs

TWISTER – A Framework for Secure and Fast Hash Functions . . . . .	257
<i>Ewan Fleischmann, Christian Forler, Michael Gorski, and Stefan Lucks</i>	
Preimage Attack on Hash Function RIPEMD . . . . .	274
<i>Gaoli Wang and Shaohui Wang</i>	
Full Key-Recovery Attack on the HMAC/NMAC Based on 3 and 4-Pass HAVAL . . . . .	285
<i>Hongbo Yu and Xiaoyun Wang</i>	

## Cryptanalysis

Memoryless Related-Key Boomerang Attack on the Full Tiger Block Cipher . . . . .	298
<i>Ewan Fleischmann, Michael Gorski, and Stefan Lucks</i>	
Memoryless Related-Key Boomerang Attack on 39-Round SHACAL-2 . . . . .	310
<i>Ewan Fleischmann, Michael Gorski, and Stefan Lucks</i>	
Some New Observations on the SMS4 Block Cipher in the Chinese WAPI Standard . . . . .	324
<i>Wentao Zhang, Wenling Wu, Dengguo Feng, and Bozhan Su</i>	
On the Correctness of an Approach against Side-Channel Attacks . . . . .	336
<i>Peng Wang, Dengguo Feng, Wenling Wu, and Liting Zhang</i>	

## Network Security

Ranking Attack Graphs with Graph Neural Networks . . . . .	345
<i>Liang Lu, Rei Safavi-Naini, Markus Hagenbuchner, Willy Susilo, Jeffrey Horton, Sweah Liang Yong, and Ah Chung Tsoi</i>	
Implementing IDS Management on Lock-Keeper . . . . .	360
<i>Feng Cheng, Sebastian Roschke, and Christoph Meinel</i>	

## Security Applications

Ensuring Dual Security Modes in RFID-Enabled Supply Chain Systems . . . . .	372
<i>Shaoying Cai, Tieyan Li, Yingjiu Li, and Robert H. Deng</i>	

Achieving Better Privacy Protection in Wireless Sensor Networks Using Trusted Computing .....	384
<i>Yanjiang Yang, Robert H. Deng, Jianying Zhou, and Ying Qiu</i>	
Trusted Privacy Domains – Challenges for Trusted Computing in Privacy-Protecting Information Sharing .....	396
<i>Hans Löhr, Ahmad-Reza Sadeghi, Claire Vishik, and Marcel Winandy</i>	
<b>Author Index</b> .....	409