

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

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

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Ed Dawson Duncan S. Wong (Eds.)

Information Security Practice and Experience

Third International Conference, ISPEC 2007
Hong Kong, China, May 7-9, 2007
Proceedings

Volume Editors

Ed Dawson
Queensland University of Technology
Information Security Institute
GPO Box 2434, Brisbane Qld 4001, Australia
E-mail: e.dawson@qut.edu.au

Duncan S. Wong
City University of Hong Kong
Department of Computer Science
83 Tat Chee Ave, Hong Kong, China
E-mail: duncan@cityu.edu.hk

Library of Congress Control Number: 2007924822

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-540-72159-2 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-72159-8 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 is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12055104 06/3180 5 4 3 2 1 0

Preface

The third international conference on Information Security Practice and Experience (ISPEC 2007) was held in Hong Kong, China, May 7 – 9, 2007. The conference was organized and sponsored by City University of Hong Kong.

As applications of information security technologies become pervasive, issues pertaining to their deployment and operation are becoming increasingly important. ISPEC is an annual conference that brings together researchers and practitioners to provide a confluence of new information security technologies, their applications and their integration with IT systems in various vertical sectors. In 2005 and 2006, the first and second conferences were held successfully in Singapore and Hangzhou, China, respectively. The conference proceedings were published by Springer in the *Lecture Notes in Computer Science* series.

The Program Committee received 135 submissions, and accepted 24 papers for presentation. The final versions of the accepted papers, which the authors finalized on the basis of comments from the reviewers, are included in the proceedings. The entire reviewing process took nine weeks, each paper was carefully evaluated by at least three members from the Program Committee. The individual reviewing phase was followed by a Web-based discussion. Papers over which the reviewers significantly disagreed were further reviewed by external experts. Based on the comments and scores given by reviewers, the final decisions on acceptance were made. We appreciate the hard work of the members of the Program Committee and external referees, who gave many hours of their valuable time.

In addition to the contributed papers, there were four invited talks: Bill Caelli spoke on “Application Security—Myth or Reality?”, Robert H. Deng on “Towards Efficient and Novel Security Solutions—A Marriage of Crypto and Trusted Computing Platform,” Lucas Hui on “Computer Forensics Tools and Technology: Research and Development in Hong Kong” and Victor K. Wei on “E-voting by Zero-Knowledge.”

We would like to thank all the people involved in organizing this conference. In particular, we would like to thank colleagues from the Department of Computer Science, City University of Hong Kong, for their time and efforts, as well as Dennis Liu, Chung Ki Li and Qiong Huang for their excellent work on maintaining the submission/reviewing software and taking care of all the technical aspects of the review process. Finally, we would like to thank all the authors who submitted papers to the conference.

May 2007

Ed Dawson
Duncan Wong

Organization

ISPEC 2007 was organized by the Department of Computer Science, City University of Hong Kong, China.

General Chair

Xiaotie Deng	City University of Hong Kong, China
C. H. Lee	City University of Hong Kong, China

Program Committee Co-chairs

Ed Dawson	QUT, Australia
Duncan Wong	City University of Hong Kong, China

Steering Committee

Feng Bao	I2R, Singapore
Robert H. Deng	Singapore Management U, Singapore

Organizing Committee

Xiaotie Deng	City University of Hong Kong, China
L. F. Kwok	City University of Hong Kong, China
C. H. Lee	City University of Hong Kong, China
Duncan Wong	City University of Hong Kong, China
Giovanna Yau	

Program Committee

Joonsang Baek	I2R, Singapore
Feng Bao	I2R, Singapore
Kefei Chen	SJTU, China
Liqun Chen	HP Bristol Labs, UK
Mathieu Ciet	Gemplus, France
Ed Dawson	QUT, Australia (Co-chair)
Cunsheng Ding	HKUST, China
Dengguo Feng	Chinese Academy of Sciences, China
Dieter Gollmann	TU Hamburg, Germany

Javier Herranz	CWI, The Netherlands
Lucas Hui	Hong Kong University, China
Min-Shiang Hwang	National Chung Hsing University, Taiwan
Tetsu Iwata	Nagoya University, Japan
Kazukuni Kobara	AIST, Japan
Kaoru Kurosawa	Ibaraki University, Japan
Kwangjo Kim	ICU, Korea
L. F. Kwok	City University of Hong Kong, China
Xuejia Lai	SJTU, China
Dong Hoon Lee	Korea University, Korea
Benoit Libert	UCL, Belgium
Joseph K. Liu	University of Bristol, UK
Javier Lopez	University of Malaga, Spain
Stefan Lucks	University of Mannheim, Germany
Richard Lui	City University of Hong Kong, China
Wenbo Mao	HP Lab, China
SangJae Moon	Kyungpook National University, Korea
Yi Mu	University of Wollongong, Australia
David Naccache	ENS and Paris II, France
Raphael C.-W. Phan	Swinburne University of Technology, Malaysia
Josef Pieprzyk	Macquarie University, Australia
Jean-Jacques Quisquater	UCL, Belgium
C. Pandu Rangan	Indian Institute of Technology, India
Reihaneh Safavi-Naini	University of Wollongong, Australia
Hovav Shacham	Weizmann Institute of Science, Israel
Ron Steinfeld	Macquarie University, Australia
Willy Susilo	University of Wollongong, Australia
Tsuyoshi Takagi	Future University - Hakodate, Japan
Xiaojian Tian	City University of Hong Kong, China
Guilin Wang	I2R, Singapore
Huaxiong Wang	Macquarie University, Australia
Stephen Wolthusen	University of London, UK
Duncan Wong	City University of Hong Kong, China (Co-chair)
Joe Yau	Hong Kong Baptist University, China
Sung-Ming Yen	National Central University, Taiwan
Yiqun Lisa Yin	Independent Consultant, USA
Siu-Ming Yiu	Hong Kong University, China
Fangguo Zhang	Sun Yat-sen University, China
Zhenfeng Zhang	Chinese Academy of Sciences, China
Yunlei Zhao	Fudan University, China
Yuliang Zheng	UNC Charlotte, USA
Jianyong Zhou	I2R, Singapore
Huafei Zhu	I2R, Singapore

External Reviewers

Manfred Aigner	Tanmoy Kanti Das	Weijun Shen
Man Ho Au	Stefan Katzenbeisser	Nicholas Sheppard
Philippe Bulens	Eike Kiltz	Mi Na Shim
Xuefei Cao	Jongsung Kim	SeongHan Shin
Julien Cathalo	Hirotsugu Kinoshita	Masaaki Shirase
Zhenchuan Chai	Divyan M. Konidala	Nigel Smart
Chris Charnes	Ulrich Kühn	Dirk Stegemann
Chien-Ning Chen	Byoungcheon Lee	Purui Su
Haibo Chen	HoonJae Lee	Willy Susilo
Jing Chen	Sang Gon Lee	Tsuyoshi Takagi
Lily Chen	Lan Li	Keisuke Tanaka
Xiaofeng Chen	Vo Duc Liem	Hitoshi Tanuma
Yongxi Cheng	Hsi-Chung Lin	Emin Islam Tatli
Benoit Chevallier-Mames	Jenny Liu	Feng Tu
Yvonne Cliff	Yu Long	Jheng-Hong Tu
Scott Contini	Miao Ma	Damien Vergnaud
Kim-Kwang Raymond Choo	Adrian McCullagh	Lionel Victor
Andrew Clark	Pablo Najera	Jose L. Vivas
Hanane Fathi	Dang Ngyuen Duc	Eric Wang
Benoit Feix	Lan Nguyen	Shuhong Wang
Evan Fleischmann	Juan Gonzalez Nieto	Zhenghong Wang
David Galindo	Peng Ning	Brent Waters
Zheng Gong	Miyako Ohkubo	Baodian Wei
Qianhong Huang	Yasuhiro Ohtaki	Mi Wen
Qiong Huang	Pascal Paillier	Jian Weng
Dennis Hofheinz	Kun Peng	Chi-Dian Wu
Xuan Hong	Ying Qiu	Qianhong Wu
Jeffrey Horton	Rodrigo Roman	Guomin Yang
Chao-Chih Hsu	Chun Ruan	Kee-Young Yoo
Zoe Jiang	Eun-Kyung Ryu	Jin Yuan
Haimin Jin	Hendra Saptura	Erik Zenner
Marc Joye	Werner Schindler	Rui Zhang
	Francesc Sebé	Chang'an Zhao

Sponsoring Institutions

City University of Hong Kong, China

Table of Contents

Invited Talks

Application Security – Myth Or Reality?	1
<i>William J. Caelli</i>	
Tools and Technology for Computer Forensics: Research and Development in Hong Kong	11
<i>Lucas C.K. Hui, K.P. Chow, and S.M. Yiu</i>	

Cryptanalysis

A Linear Analysis of Blowfish and Khufu	20
<i>Jorge Nakahara Jr.</i>	
Related-Key Rectangle Attack on 43-Round SHACAL-2	33
<i>Gaoli Wang</i>	
On the Ability of AES S-Boxes to Secure Against Correlation Power Analysis	43
<i>Zheng-lin Liu, Xu Guo, Yi-cheng Chen, Yu Han, and Xue-cheng Zou</i>	

Signatures

A Sanitizable Signature Scheme with Aggregation	51
<i>Tetsuya Izu, Noboru Kunihiro, Kazuo Ohta, Masahiko Takenaka, and Takashi Yoshioka</i>	
A Novel Verifiably Encrypted Signature Scheme Without Random Oracle	65
<i>Jianhong Zhang and Jian Mao</i>	
Certificate Based (Linkable) Ring Signature	79
<i>Man Ho Au, Joseph K. Liu, Willy Susilo, and Tsz Hon Yuen</i>	
An Efficient ID-Based Verifiably Encrypted Signature Scheme Based on Hess's Scheme	93
<i>Saeran Kwon and Sang-Ho Lee</i>	
On the Sequentiality of Three Optimal Structured Multisignature Schemes	105
<i>Zuhua Shao</i>	

Network Security and Security Management

Secure Feedback Service in Wireless Sensor Networks	116
<i>Di Ma</i>	
An Economical Model for the Risk Evaluation of DoS Vulnerabilities in Cryptography Protocols	129
<i>Zhen Cao, Zhi Guan, Zhong Chen, Jianbin Hu, and Liyong Tang</i>	
Practical Uses of Virtual Machines for Protection of Sensitive User Data	145
<i>Peter C.S. Kwan and Glenn Durfee</i>	
Formalization of RBAC Policy with Object Class Hierarchy	162
<i>Jung Hwa Chae and Nematollah Shiri</i>	

Privacy and Applications

Privacy-Preserving Credentials Upon Trusted Computing Augmented Servers	177
<i>Yanjiang Yang, Robert H. Deng, and Feng Bao</i>	
Two-Party Privacy-Preserving Agglomerative Document Clustering	193
<i>Chunhua Su, Jianying Zhou, Feng Bao, Tsuyoshi Takagi, and Kouichi Sakurai</i>	
Efficient Bid Validity Check in ElGamal-Based Sealed-Bid E-Auction . . .	209
<i>Kun Peng and Ed Dawson</i>	

Cryptographic Algorithms and Implementations

How to Prevent DPA and Fault Attack in a Unified Way for ECC Scalar Multiplication – Ring Extension Method	225
<i>Yoo-Jin Baek and Ihor Vasylytsov</i>	
Secure Signed Radix- r Recoding Methods for Constrained-Embedded Devices	238
<i>Dong-Guk Han, Sung-Kyoung Kim, Ho Won Kim, Kyo IL Chung, and Jongin Lim</i>	
Some Efficient Algorithms for the Final Exponentiation of η_T Pairing . . .	254
<i>Masaaki Shirase, Tsuyoshi Takagi, and Eiji Okamoto</i>	
Towards Minimizing Memory Requirement for Implementation of Hyperelliptic Curve Cryptosystems	269
<i>Pradeep Kumar Mishra, Pinakpani Pal, and Palash Sarkar</i>	

Authentication and Key Management

Achieving End-to-End Authentication in Intermediary-Enabled Multimedia Delivery Systems	284
<i>Robert H. Deng and Yanjiang Yang</i>	
Scalable Group Key Management Protocol Based on Key Material Transmitting Tree	301
<i>Minghui Zheng, Guohua Cui, Muxiang Yang, and Jun Li</i>	
A Time-Based Key Management Protocol for Wireless Sensor Networks	314
<i>Jiyong Jang, Taekyoung Kwon, and Jooseok Song</i>	

Cryptosystems

Identity-Based Threshold Decryption Revisited	329
<i>Shengli Liu, Kefei Chen, and Weidong Qiu</i>	
Visual Cryptography Schemes with Dihedral Group Access Structure for Many Images	344
<i>Miyuki Uno and M. Kano</i>	
Author Index	361