Lecture Notes in Computer Science 4464

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

Ed Dawson Duncan S. Wong (Eds.)

Information Security Practice and Experience

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

Springer

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

Springer is a part of Springer Science+Business Media

springer.com

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
Jianying Zhou	I2R, Singapore
Huafei Zhu	I2R, Singapore

External Reviewers

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

Sponsoring Institutions

City University of Hong Kong, China

Table of Contents

Invited Talks

Cryptanalysis

Signatures

Network Security and Security Management

Privacy and Applications

Cryptographic Algorithms and Implementations

Authentication and Key Management

Cryptosystems