Lecture Notes in Computer Science 3439

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

Editorial Board

Robert H. Deng Feng Bao
HweeHwa Pang Jianying Zhou (Eds.)

Information Security Practice and Experience

First International Conference, ISPEC 2005
Singapore, April 11-14, 2005
Proceedings

Springer

Volume Editors

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

Feng Bao
HweeHwa Pang
Jianying Zhou
Institute for Infocomm Research
21 Heng Mui Keng Terrace, Singapore 119613
E-mail: {baofeng, hhpang, jyzhou}@i2r.a-star.edu.sg

Library of Congress Control Number: 2005923658

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

ISSN 0302-9743
ISBN-10 3-540-25584-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-25584-0 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11407959 06/3142 5 4 3 2 1 0

Preface

The inaugural Information Security Practice and Experience Conference (ISPEC) was held on April 11–14, 2005, in Singapore.

As applications of information security technologies become pervasive, issues pertaining to their deployment and operation are becoming increasingly important. ISPEC is intended to be 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. The Program Committee consisted of leading experts in the areas of information security, information systems, and domain experts in applications of IT in vertical business segments.

The topics of the conference covered security applications and case studies, access control, network security, data security, secure architectures, and cryptographic techniques. Emphasis was placed on the application of security research to meet practical user requirements, both in the paper selection process and in the invited speeches.

Acceptance into the conference proceedings was very competitive. The Call for Papers attracted more than 120 submissions, out of which the Program Committee selected only 35 papers for inclusion in the proceedings.

This conference was made possible only through the contributions from many individuals and organizations. We would like to thank all the authors who submitted papers. We also gratefully acknowledge the members of the Program Committee and the external reviewers, for the time and effort they put into reviewing the submissions.

Special thanks are due to Ying Qiu for managing the website for paper submission, review and notification. Patricia Loh was kind enough to arrange for the conference venue, and took care of the administration in running the conference.

Last but not least, we are grateful to the Institute for Infocomm Research, and also the School of Information Systems, Singapore Management University for sponsoring the conference.

February 2005

Robert H. Deng,
Feng Bao, HweeHwa Pang,
Jianying Zhou

ISPEC 2005

First Information Security Practice and Experience Conference

Singapore
April 11–14, 2005

Organized by

Institute for Infocomm Research, Singapore

Sponsored by

Institute for Infocomm Research, Singapore
and
Singapore Management University, Singapore

General Chair

Robert H. Deng ..... Singapore Management University, Singapore

Program Chairs

Feng Bao ..... Institute for Infocomm Research, Singapore
HweeHwa Pang ..... Institute for Infocomm Research, Singapore

Publication Chair

Jianying Zhou ..... Institute for Infocomm Research, Singapore

Program Committee

Tuomas Aura ..... Microsoft Research, UK
Elisa Bertino ..... Purdue Univ., USA
Colin Boyd ..... QUT, Australia
Chin-Chen Chang ..... CCU, Taiwan
Kefei Chen ..... Shanghai Jiaotong Univ., China
Liqun Chen ..... HP Bristol Labs, UK
Xiaotie Deng ..... City Univ. of Hong Kong, China
Dengguo Feng ..... Chinese Academy of Sciences, China
Dieter Gollmann ..... TU Hamburg-Harburg, Germany
Hideki Imai ..... Univ. of Tokyo, Japan
Sushil Jajodia ..... GMU, USA
Pradeep K. Khosla ..... CMU, USA
Dong Hoon Lee ..... Korea Univ., Korea
Javier Lopez ..... Univ. of Malaga, Spain

David Naccache ..... Gemplus, France
Masahiro Mambo ..... Univ. of Tsukuba, Japan
Chris Mitchell ..... Univ. of London, UK
SangJae Moon ..... Kyungpook National Univ., Korea
Reihaneh Safavi-Naini ..... Univ. of Wollongong, Australia
Kouichi Sakurai ..... Kyushu Univ., Japan
Ravi Sandhu ..... GMU, USA
Shiuhpyng Shieh ..... NCTU, Taiwan
Dawn Song ..... CMU, USA
Dan Suciu ..... Univ. of Washington, USA
Rahul Telang ..... CMU, USA
Vijay Varadharajan ..... Macquarie Univ., Australia
Victor Wei ..... Chinese Univ. of Hong Kong, China
Moti Yung ..... Columbia Univ., USA
Jianying Zhou ..... I2R, Singapore

External Reviewers

Issac Agudo, Joonsang Baek, Lujo Bauer, Eric Brier, Julien Brouchier, Kisik Chang, C.I. Chen, Shiping Chen, Xi Chen, Benoit Chevallier-Mames, Eun Young Choi, Jean-Sebastien Coron, Guerric Meurice de Dormale, Y.J. Fu, Juan Gonzalez, Huiping Guo, Helena Handschuh, Yvonne Hitchcock, Yoshiaki Hori, Shih-I Huang, Changho Jung, Lea Kissner, Caroline Kudla, Anantharaman Lakshminarayanan, Fu-Yuan Lee, Kwangsoo Lee, Zhou-Yu Lee, Feiyu Lei, Shiqun Li, Tieyan Li, Xiangxue Li, Ya-Jeng Lin, Becky Liu, Changshe Ma, Jose A. Montenegro, James Newsome, Jose A. Onieva, Alina Opera, Pascal Paillier, Joseph Pamula, Young-Ho Park, Kun Peng, Angela Piper, Kyung-Hyune Rhee, Rodrigo Roman, W. Shin, Yuji Suga, Toshihiro Tabata, Yoshifumi Ueshige, Lionel Victor, Guilin Wang, Lingyu Wang, Shuhong Wang, Claire Whelan, Hongjun Wu, Hsiao-Chan Wu, Yongdong Wu, Yi Xu, G.M. Yang, Tzu-I Yang, Jungjae Yoo, Kee-Young Yoo, T.H. Yuen, Ruishan Zhang, Xuan Zhou, Bo Zhu, Huafei Zhu

Table of Contents

Network Security

Cryptographic Techniques I

Secure Architecture I

Access Control

Intrusion Detection

Applications and Case Studies

Secure Architecture II

Data Security

Cryptographic Techniques II