

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

New York University, NY, 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

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

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

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
springeronline.com

© Springer-Verlag Berlin Heidelberg 2005
Printed in Germany

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 Suciú	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

Risk Assessment of Production Networks Using Honeynets – Some Practical Experience

Stephan Riebach, Erwin P. Rathgeb, Birger Toedtman 1

POSSET – Policy-Driven Secure Session Transfer

Philip Robinson, Christian Schaefer, Thomas Walter 13

Modeling and Evaluation of Security Architecture for Wireless Local Area Networks by Indexing Method: A Novel Approach

Debabrata Nayak, D.B. Phatak, V.P. Gulati 25

Robust Routing in Malicious Environment for Ad Hoc Networks

Zhongchao Yu, Chuk-Yang Seng, Tao Jiang, Xue Wu, William A. Arbaugh 36

Cryptographic Techniques I

Short Linkable Ring Signatures for E-Voting, E-Cash and Attestation

Patrick P. Tsang, Victor K. Wei 48

Tracing Traitors by Guessing Secrets .The q -Ary Case

Marcel Fernandez, Miguel Soriano, Josep Cotrina 61

Probabilistic Analyses on Finding Optimal Combinations of Primality Tests in Real Applications

Heejin Park, Sang Kil Park, Ki-Ryong Kwon, Dong Kyue Kim 74

Countermeasures for Preventing Comb Method Against SCA Attacks

Mustapha Hedabou, Pierre Pinel, Lucien Bénéteau 85

Secure Architecture I

An Email Worm Vaccine Architecture
Stelios Sidiroglou, John Ioannidis, Angelos D. Keromytis, Salvatore J. Stolfo 97

Enforcing the Principle of Least Privilege with a State-Based Privilege Control Model
Bin Liang, Heng Liu, Wenchang Shi, Yanjun Wu 109

Security On-demand Architecture with Multiple Modules Support
Yanjun Wu, Wenchang Shi, Hongliang Liang, Qinghua Shang, Chunyang Yuan, Bin Liang 121

Measuring Resistance to Social Engineering
Hågen Hasle, Yngve Kristiansen, Ketil Kintel, Einar Snekkenes 132

Access Control

Conformance Checking of RBAC Policy and Its Implementation
Frode Hansen, Vladimir Oleshchuk 144

A Practical Aspect Framework for Enforcing Fine-Grained Access Control in Web Applications
Kung Chen, Chih-Mao Huang 156

A Task-Oriented Access Control Model for WfMS
Xu Liao, Li Zhang, Stephen C.F. Chan 168

Intrusion Detection

A Brief Observation-Centric Analysis on Anomaly-Based Intrusion Detection
Zonghua Zhang, Hong Shen 178

Detection of Distributed Denial of Service Attacks Using Statistical Pre-processor and Unsupervised Neural Networks <i>Rasool Jalili, Fatemeh Imani-Mehr, Morteza Amini, Hamid Reza Shahriari</i>	192
Visual Spoofing of SSL Protected Web Sites and Effective Countermeasures <i>Andre Adelsbach, Sebastian Gajek, Jörg Schwenk</i>	204
Model Redundancy vs. Intrusion Detection <i>Zhuowei Li, Amitabha Das, Sabu Emmanuel</i>	217
Applications and Case Studies	
An Open Approach for Designing Secure Electronic Immobilizers <i>Kerstin Lemke, Ahmad-Reza Sadeghi, Christian Stübke</i>	230
An Empirical Study on the Usability of Logout in a Single Sign-On System <i>Mikael Linden, Inka Vilpola</i>	243
Secure Software Delivery and Installation in Embedded Systems <i>André Adelsbach, Ulrich Huber, Ahmad-Reza Sadeghi</i>	255
A Restricted Multi-show Credential System and Its Application on E-Voting <i>Joseph K. Liu, Duncan S. Wong</i>	268
Secure Architecture II	
Recard: Using Recommendation Cards Approach for Building Trust in Peer-to-Peer Networks <i>Hany A. Samuel, Yasser H. Dakroury, Hussein I. Shahein</i>	280
Using Trust for Restricted Delegation in Grid Environments <i>Wenbao Jiang, Chen Li, Shuang Hao, Yiqi Dai</i>	293
Computer Vulnerability Evaluation Using Fault Tree Analysis <i>Tao Zhang, Mingzeng Hu, Xiaochun Yun, Yongzheng Zhang</i>	302

An Identity-Based Grid Security Infrastructure Model

Xiaoqin Huang, Lin Chen, Linpeng Huang, Minglu Li 314

Data Security

Towards Multilateral-Secure DRM Platforms

Ahmad-Reza Sadeghi, Christian Stübke 326

Hiding Data in Binary Images

Chin-Chen Chang, Chun-Sen Tseng, Chia-Chen Lin 338

Performance Analysis of CDMA-Based Watermarking with Quantization Scheme

Yanmei Fang, Limin Gu, Jiwu Huang 350

Protecting Mass Data Basing on Small Trusted Agent

Fangyong Hou, Zhiying Wang, Kui Dai, Yun Liu 362

Cryptographic Techniques II

On the Security of Some Nonrepudiable Threshold Proxy Signature Schemes

Zuowen Tan, Zhuojun Liu, Mingsheng Wang 374

Token-Controlled Public Key Encryption

Joonsang Baek, Reihaneh Safavi-Naini, Willy Susilo 386

A New Class of Codes for Fingerprinting Schemes

Marcel Fernandez, Miguel Soriano, Josep Cotrina 398

t -Out-of- n String/Bit Oblivious Transfers Revisited

Qianhong Wu, Bo Qin, Changjie Wang, Xiaofeng Chen, Yuming Wang 410

Author Index 423