Lecture Notes in Computer Science 2836

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Sihan Qing Dieter Gollmann
Jianying Zhou (Eds.)

Information and Communications Security

5th International Conference, ICICS 2003
Huhehaote, China, October 10-13, 2003
Proceedings

Springer

Volume Editors

Sihan Qing
Chinese Academy of Sciences, Institute of Software
44th Street South, ZhongGuanCun, Beijing 100080, China
E-mail: qsihan@yahoo.com

Dieter Gollmann
Microsoft Research Limited
7 J.J. Thomson Avenue, Cambridge CB3 0FB, UK
E-mail: diego@microsoft.com

Jianying Zhou
Institute for Infocomm Research
21 Heng Mui Keng Terrace, Singapore 119613
E-mail: jyzhou@i2r.a-star.edu.sg

Cataloging-in-Publication Data applied for

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1, C.2, J.1

ISSN 0302-9743
ISBN 3-540-20150-5 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by PTP-Berlin GmbH
Printed on acid-free paper SPIN: 10959817 06/3142 5 4 3 2 1 0

Preface

ICICS 2003, the Fifth International Conference on Information and Communication Security, was held in Huhehaote city, Inner Mongolia, China, 10–13 October 2003. Among the preceding conferences, ICICS'97 was held in Beijing, China, ICICS'99 in Sydney, Australia, ICICS 2001 in Xi'an, China, and ICICS 2002, in Singapore. The proceedings were released as Volumes 1334, 1726, 2229, and 2513 of the LNCS series of Springer-Verlag, respectively.

ICICS 2003 was sponsored by the Chinese Academy of Sciences (CAS), the National Natural Science Foundation of China, and the China Computer Federation. The conference was organized by the Engineering Research Center for Information Security Technology of the Chinese Academy of Sciences (ERCIST, CAS) in co-operation with the International Communications and Information Security Association (ICISA).

The aim of the ICICS conferences has been to offer the attendees the opportunity to discuss the state-of-the-art technology in theoretical and practical aspects of information and communications security. The response to the Call for Papers was surprising. When we were preparing the conference between April and May, China, including the conference venue, Huhehaote City, was fighting against SARS. Despite this 176 papers were submitted to the conference from 22 countries and regions, and after a competitive selection process, 37 papers from 14 countries and regions were accepted to appear in the proceedings and be presented at ICICS 2003. We would like to take this opportunity to thank all those who submitted papers to ICICS 2003 for their valued contribution to the conference.

We wish to thank the members of the program committee and external reviewers for their effort in reviewing the papers in a short time. We are also pleased to thank Prof. Xizhen Ni, Dr. Yeping He, and other members of the organizing committee for helping with many local details. Special thanks to Dr. Jianying Zhou who took care of most of the tough work relating to the publishing affairs and contributed to the conference in variety of ways.

It now seems that SARS is over. On behalf of the program committee and organizing committee we sincerely hope that you were able to enjoy not only the technical part of the conference, but also the historical city of Huhehaote and the beautiful grassland of Inner Mongolia in China.

October 2003

Sihan Qing
Dieter Gollmann

ICICS 2003

Fifth International Conference on Information and Communications Security

Huhehaote, China October 10–13, 2003

Sponsored by

Chinese Academy of Sciences
and
National Natural Science Foundation of China
and
China Computer Federation

Organized by

Engineering Research Center for Information Security Technology
(Chinese Academy of Sciences)
and
International Communications and Information Security Association

General Chair

Dequan He	Academician of the Chinese Academy of Engineering, China

Program Chairs

Sihan Qing	Chinese Academy of Sciences, China
Dieter Gollmann	Microsoft Research, UK

Program Committee

Feng Bao	Institute for Infocomm Research, Singapore
Thomas Berson	Anagram, USA
Chin-Chen Chang	MOE, Taiwan
Lily Chen	Motorola, USA
Welland Chu	THALES, Hong Kong, China
Edward Dawson	Queensland University of Technology, Australia
Robert Deng	Institute for Infocomm Research, Singapore
Jan Eloff	University of Pretoria, South Africa

Mariki Eloff	University of South Africa, South Africa
Dengguo Feng	Chinese Academy of Sciences, China
Yongfei Han	ONETS, China
Lein Harn	University of Missouri, USA
Yeping He	Chinese Academy of Sciences, China
Kwangjo Kim	Information and Communications University, Korea
Xuejia Lai	Swissgroup, Switzerland
Chi-Sung Laih	National Cheng Kung University, Taiwan
Javier Lopez	University of Malaga, Spain
David Naccache	Gemplus, France
Eiji Okamoto	University of Tsukuba, Japan
Susan Pancho	University of the Philippines, the Philippines
Jean-Jacques Quisquater	UCL, Belgium
Bimal Roy	Indian Statistical Institute, India
Claus Schnorr	University of Frankfurt, Germany
Vijay Varadharajan	Macquarie University, Australia
Yumin Wang	Xidian University, China
Susanne Wetzel	Stevens Institute of Technology, USA
Tara Whalen	Dalhousie University, Canada
Guozhen Xiao	Xidian University, China
Lisa Yiqun Yin	Princeton University, USA
Moti Yung	Columbia University, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

Organizing Committee

Xizhen Ni	Chinese Academy of Sciences, China
Yeping He	Chinese Academy of Sciences, China

External Reviewers

Julien Brouchier, Xiaofeng Chen, Judy Zhi Fu, Pierre Girard, Guang Gong, Helena Handschuh, Wen-Jung Hsain, Qingguang Ji, Jianchun Jiang, Wen-Chung Kuo, Bao Li, Tieyan Li, Dongdai Lin, Wenqing Liu, Hengtai Ma, Manish Mehta, Yang Meng, Pradeep Mishra, Mridul Nandi, Pascal Paillier, Pinakpani Pal, Jian Ren, Greg Rose, Hung-Min Sun, Shen-Chuan Tai, Lionel Victor, Chih-Hung Wang, Guilin Wang, Mingsheng Wang, Wenling Wu, Ching-Nung Yang, Wentao Zhang, Yongbin Zhou, Bo Zhu

Table of Contents