Lecture Notes in Computer Science 1334
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Yongfei Han Tatsuaki Okamoto
Sihan Qing (Eds.)

Information and Communications Security

First International Conference, ICIS '97
Beijing, China, November 11-14, 1997
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Yongfei Han, Program Co-Chair
Gemplus Technologies Asia PTE LTD
89, Science Park Drive #04-01/05
The Rutherford, Singapore Science Park, Singapore 118261
E-mail: YongFei.HAN@ccmail.edt.fr

Tatsuaki Okamoto, Program Co-Chair
NTT Labs, Room 609A
1-1 Hikarinooka, Yokosuka-shi, 239 Japan
E-mail: okamoto@sucaba.isl.ntt.co.jp

Sihan Qing, Director
Engineering Research Center for Information Security Technology
Chinese Academy of Sciences
Beijing 100080, P.R. China
E-mail: qsh@sun.ihep.ac.cn

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information and communications security : first international conference ; proceedings / ICICS '97, Beijing, China, November 11 - 13, 1997. Yongfei Han ... (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1997
(Lecture notes in computer science ; Vol. 1334)
ISBN 3-540-63696-X

CR Subject Classification (1991): E.3-4, G.2.1, D.4.6,F.2.1-2, C.2, J.1, K.6.5

ISSN 0302-9743
ISBN 3-540-63696-X Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10647862 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

The International Conference on Information and Communications Security (ICICS) represents international research and development in the area of information and communications security. The conference is held every two years (during years when Asiacrypt is not held) in different Asian countries, and it attracts an audience from the academic, commercial, and industrial communities. ICICS '97 is held in the Chinese Academy of Sciences in Beijing, P. R. China, November 11-14 1997.

ICICS '97 was sponsored by the Chinese Academy of Sciences, 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 in the Chinese Academy of Sciences in co-operation with the International Association for Cryptologic Research (IACR), IEICE, and the Asiacrypt Steering Committee.

There were 87 papers submitted for inclusion, from an international authorship, 37 papers among them have been accepted as regular papers, and 11 as short papers. We would like to thank the authors of all papers submitted, both those whose work is included in these proceedings, and those whose work could not be accommodated. Without their research and writing up there would be no conference.

The number of submitted papers put an additional strain on the program committee members. We are grateful to them all for their work in reviewing the papers in a short time and for freely giving us the benefit of their experience and support in a variety of ways. We also would like to thank all the other reviewers for their reviewing the papers.

We wish to thank all the participants, organizers, and contributors of the ICICS '97 conference.

August, 1997

Yongfei Han
Tatsuaki Okamoto
Sihan Qing

ICICS Steering Committee and ICICS '97 Program Committee

1 STEERING COMMITTEE

Chin-Chen Chang
James W. Gray, III
Yongfei Han
Kwangjo Kim
Tatsuaki Okamoto
Sihan Qing
Vijay Varadharajan

2 PROGRAM COMMITTEE

Co-Chairs
Yongfei Han (GemPlus)
Tatsuaki Okamoto (NTT, Japan)
Sihan Qing (ERCIST, China)
Member
Elisa Bertino (University of Milano, Italy)
Chin-Chen Chang (NCCU, Taiwan)
Robert Deng (NUS, Singapore)
Dieter Gollmann (University of London, UK)
James W. Gray, III (UST, Hong Kong)
Erland Jonsson (Chalmers University of Technology, Sweden)
Kwangjo Kim (ETRI, S. Korea)
Wenbo Mao (HP, UK)
Tsutomu Matsumoto (Yokohama National University, Japan)
Mitsuru Matsui (Mitsubishi, Japan)
Ueli Maurer (ETH, Switzerland)
Catherline Meadows (Naval Research Lab. USA)
Kazuo Ohta (NTT, Japan)
Eiji Okamoto (JAIST, Japan)
Jean-Jacques Quisquater (UCL, Belgium)
Phil Rogaway (UC Davis, USA)
Ravi Sandhu (George Mason University, USA)
Yiqun Lisa Yin (RSA, USA)
Moti Yung (CertCo, USA)
Vijay Varadharajan (Western Sydney University, Australia)

General Chair and Organizing Chair
General Chair: Sihan Qing
Organizing Chair: Xizhen Ni

CONTENTS