

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

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

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

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-Verlag. Violations are liable for prosecution under the German Copyright Law.

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

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2003
Printed in Germany

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

VIII Organization

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 Bouchier, 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

A Fast Square Root Computation Using the Frobenius Mapping	1
<i>Wang Feng, Yasuyuki Nogami, Yoshitaka Morikawa</i>	
A Forward-Secure Blind Signature Scheme Based on the Strong RSA Assumption	11
<i>Dang Nguyen Duc, Jung Hee Cheon, Kwangjo Kim</i>	
Secure Route Structures for the Fast Dispatch of Large-Scale Mobile Agents	22
<i>Yan Wang, Chi-Hung Chi, Tieyan Li</i>	
On the RS-Code Construction of Ring Signature Schemes and a Threshold Setting of RST	34
<i>Duncan S. Wong, Karyin Fung, Joseph K. Liu, Victor K. Wei</i>	
A Policy Based Framework for Access Control	47
<i>Ricardo Nabhen, Edgard Jamhour, Carlos Maziero</i>	
Trading-Off Type-Inference Memory Complexity against Communication	60
<i>Konstantin Hyppönen, David Naccache, Elena Trichina, Alexei Tchoulkine</i>	
Security Remarks on a Group Signature Scheme with Member Deletion	72
<i>Guilin Wang, Feng Bao, Jianying Zhou, Robert H. Deng</i>	
An Efficient Known Plaintext Attack on FEA-M	84
<i>Hongjun Wu, Feng Bao, Robert H. Deng</i>	
An Efficient Public-Key Framework	88
<i>Jianying Zhou, Feng Bao, Robert Deng</i>	
ROCEM: Robust Certified E-mail System Based on Server-Supported Signature	100
<i>Jong-Phil Yang, Chul Sur, Kyung Hyune Rhee</i>	
Practical Service Charge for P2P Content Distribution	112
<i>Jose Antonio Onieva, Jianying Zhou, Javier Lopez</i>	
ICMP Traceback with Cumulative Path, an Efficient Solution for IP Traceback	124
<i>Henry C.J. Lee, Vrizlynn L.L. Thing, Yi Xu, Miao Ma</i>	

A Lattice Based General Blind Watermark Scheme	136
<i>Yongliang Liu, Wen Gao, Zhao Wang, Shaohui Liu</i>	
Role-Based Access Control and the Access Control Matrix	145
<i>Gregory Saunders, Michael Hitchens, Vijay Varadharajan</i>	
Broadcast Encryption Schemes Based on the Sectioned Key Tree	158
<i>Miodrag J. Mihaljević</i>	
Research on the Collusion Estimation	170
<i>Gang Li, Jie Yang</i>	
Multiple Description Coding for Image Data Hiding Jointly in the Spatial and DCT Domains	179
<i>Mohsen Ashourian, Yo-Sung Ho</i>	
Protocols for Malicious Host Revocation	191
<i>Oscar Esparza, Miguel Soriano, Jose L. Muñoz, Jordi Forné</i>	
A DWT-Based Digital Video Watermarking Scheme with Error Correcting Code	202
<i>Pik-Wah Chan, Michael R. Lyu</i>	
A Novel Two-Level Trust Model for Grid	214
<i>Tie-Yan Li, HuaFei Zhu, Kwok-Yan Lam</i>	
Practical t-out-n Oblivious Transfer and Its Applications	226
<i>Qian-Hong Wu, Jian-Hong Zhang, Yu-Min Wang</i>	
Adaptive Collusion Attack to a Block Oriented Watermarking Scheme	238
<i>Yongdong Wu, Robert Deng</i>	
ID-Based Distributed “Magic Ink” Signature from Pairings	249
<i>Yan Xie, Fangguo Zhang, Xiaofeng Chen, Kwangjo Kim</i>	
A Simple Anonymous Fingerprinting Scheme Based on Blind Signature	260
<i>Yan Wang, Shuwang Lü, Zhenhua Liu</i>	
Compact Conversion Schemes for the Probabilistic OW-PCA Primitives	269
<i>Yang Cui, Kazukuni Kobara, Hideki Imai</i>	
A Security Verification Method for Information Flow Security Policies Implemented in Operating Systems	280
<i>Xiao-dong Yi, Xue-jun Yang</i>	

A Novel Efficient Group Signature Scheme with Forward Security	292
<i>Jianhong Zhang, Qianhong Wu, Yumin Wang</i>	
Variations of Diffie-Hellman Problem	301
<i>Feng Bao, Robert H. Deng, HuaFei Zhu</i>	
A Study on the Covert Channel Detection of TCP/IP Header Using Support Vector Machine	313
<i>Taeshik Sohn, JungTaek Seo, Jongsub Moon</i>	
A Research on Intrusion Detection Based on Unsupervised Clustering and Support Vector Machine	325
<i>Min Luo, Lina Wang, Huanguo Zhang, Jin Chen</i>	
UC-RBAC: A Usage Constrained Role-Based Access Control Model	337
<i>Zhen Xu, Dengguo Feng, Lan Li, Hua Chen</i>	
(Virtually) Free Randomization Techniques for Elliptic Curve Cryptography	348
<i>Mathieu Ciet, Marc Joye</i>	
An Optimized Multi-bits Blind Watermarking Scheme	360
<i>Xiaoqiang Li, Xiangyang Xue, Wei Li</i>	
A Compound Intrusion Detection Model	370
<i>Jianhua Sun, Hai Jin, Hao Chen, Qian Zhang, Zongfen Han</i>	
An Efficient Convertible Authenticated Encryption Scheme and Its Variant	382
<i>Hui-Feng Huang, Chin-Chen Chang</i>	
Space-Economical Reassembly for Intrusion Detection System	393
<i>Meng Zhang, Jiu-bin Ju</i>	
A Functional Decomposition of Virus and Worm Programs	405
<i>J. Krishna Murthy</i>	
Author Index	415