Lecture Notes in Computer Science 2846

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

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Jianying Zhou Moti Yung Yongfei Han (Eds.)

Applied Cryptography and Network Security

First International Conference, ACNS 2003
Kunming, China, October 16-19, 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

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

Moti Yung
Columbia University
S.W. Mudd Building, Computer Science Department
New York, NY 10027, USA
E-mail: moti@cs.columbia.edu

Yongfei Han
ONETS, Shangdi Zhongguancun Chuangye Dasha
Haidian District, Beijing 100085, China
E-mail: yongfei_han@onets.com.cn

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress

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, C.2, D.4.6, H.3-4, K.4.4, K.6.5

ISSN 0302-9743
ISBN 3-540-20208-0 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 10960585 06/3142 5 4 3 2 1 0

Preface

The 1st International Conference on "Applied Cryptography and Network Security" (ACNS 2003) was sponsored and organized by ICISA (International Communications and Information Security Association), in cooperation with MiAn Pte. Ltd. and the Kunming government. It was held in Kunming, China in October 2003. The conference proceedings was published as Volume 2846 of the Lecture Notes in Computer Science (LNCS) series of Springer-Verlag.

The conference received 191 submissions, from 24 countries and regions; 32 of these papers were accepted, representing 15 countries and regions (acceptance rate of 16.75%). In this volume you will find the revised versions of the accepted papers that were presented at the conference. In addition to the main track of presentations of accepted papers, an additional track was held in the conference where presentations of an industrial and technical nature were given. These presentations were also carefully selected from a large set of presentation proposals.

This new international conference series is the result of the vision of Dr. Yongfei Han. The conference concentrates on current developments that advance the areas of applied cryptography and its application to systems and network security. The goal is to represent both academic research works and developments in industrial and technical frontiers. We thank Dr. Han for initiating this conference and for serving as its General Chair.

Many people and organizations helped in making the conference a reality. We thank the conference sponsors: the Kunming government, MiAn Pte. Ltd., and ICISA. We greatly thank the organizing committee members for taking care of the registration, logistics, and local arrangements. It is due to their hard work that the conference was possible. We also wish to thank Springer and Mr. Alfred Hofmann and his staff for the advice regarding the publication of the proceedings as a volume of LNCS. Our deepest thanks go to the program committee members for their hard work in reviewing papers. We also wish to thank the external reviewers who assisted the program committee members.

Last, but not least, special thanks are due to all the authors who submitted papers and to the conference participants from all over the world. We are very grateful for their support, which was especially important in these difficult times when the SARS outbreak impacted many countries, especially China. It is in such challenging times for humanity that the strength and resolve of our community is tested: the fact that we were able to attract many papers and prepare and organize this conference is testament to the determination and dedication of the cryptography and security research community worldwide.

October 2003

Jianying Zhou
Moti Yung

ACNS 2003

1st International Conference on Applied Cryptography and Network Security

Kunming, China
October 16–19, 2003

Sponsored and organized by

International Communications and Information Security Association (ICISA)

In co-operation with

MiAn Pte. Ltd. (ONETS), China
and
Kunming Government, China

General Chair

Yongfei Han ..... ONETS, China

Program Chairs

Jianying Zhou ..... Institute for Infocomm Research, Singapore
Moti Yung ..... Columbia University, USA

Program Committee

Thomas Berson ..... Anagram, USA
Robert Deng ..... Institute for Infocomm Research, Singapore
Xiaotie Deng ..... City University, Hong Kong
Dengguo Feng ..... Chinese Academy of Sciences, China
Shai Halevi ..... IBM T.J. Watson Research Center, USA
Amir Herzberg ..... Bar-Ilan University, Israel
Sushil Jajodia ..... George Mason University, USA
Markus Jakobsson ..... RSA Lab, USA
Kwangjo Kim ..... Information and Communications University, Korea
Kwok-Yan Lam ..... Tsinghua University, China
Javier Lopez ..... University of Malaga, Spain
Keith Martin ..... Royal Holloway, University of London, UK
Catherine Meadows ..... Naval Research Lab, USA
Chris Mitchell ..... Royal Holloway, University of London, UK

Atsuko Miyaji ..... JAIST, Japan
David Naccache ..... Gemplus, France
Kaisa Nyberg ..... Nokia, Finland
Eiji Okamoto ..... University of Tsukuba, Japan
Rolf Oppliger ..... eSECURITY Technologies, Switzerland
Susan Pancho ..... University of the Philippines, Philippines
Guenther Pernul ..... University of Regensburg, Germany
Josef Pieprzyk ..... Macquarie University, Australia
Bart Preneel ..... K.U. Leuven, Belgium
Sihan Qing ..... Chinese Academy of Sciences, China
Leonid Reyzin ..... Boston University, USA
Bimal Roy ..... Indian Statistical Institute, India
Kouichi Sakurai ..... Kyushu University, Japan
Pierangela Samarati ..... University of Milan, Italy
Gene Tsudik ..... University of California, Irvine, USA
Wen-Guey Tzeng ..... National Chiao Tung University, Taiwan
Vijay Varadharajan ..... Macquarie University, Australia
Adam Young ..... Cigital, USA
Yuliang Zheng ..... University of North Carolina, Charlotte, USA

Organizing Committee

Yongfei Han ..... ONETS, China
Chuankun Wu ..... Chinese Academy of Sciences, China
Li Xu ..... ONETS, China

External Reviewers

Aditya Bagchi, Antoon Bosselaers, Christain Breu, Christophe De Cannière, Xiaofeng Chen, Benoit Chevallier-Mames, Siu-Leung Chung, Tanmoy Kanti Das, Mike David, Xuhua Ding, Ratna Dutta, Matthias Fitzi, Jacques Fournier, Youichi Futa, Hossein Ghodosi, Pierre Girard, Zhi Guo, Michael Hitchens, Kenji Imamoto, Sarath Indrakanti, Gene Itkis, Hiroaki Kikuchi, Svein Knapskog, Bao Li, Tieyan Li, Dongdai Lin, Wenqing Liu, Anna Lysyanskaya, Hengtai Ma, Subhamoy Maitra, Kostas Markantonakis, Eddy Masovic, Mitsuru Matusi, Pradeep Mishra, Sourav Mukherjee, Bjoern Muschall, Einar Mykletun, Mridul Nandy, Maithili Narasimha, Svetla Nikova, Pascal Paillier, Pinakpani Pal, Kenny Paterson, Stephanie Porte, Geraint Price, Torsten Priebe, Michael Quisquater, Pankaj Rohatgi, Ludovic Rousseau, Craig Saunders, Jasper Scholten, Yaron Sella, Hideo Shimizu, Igor Shparlinski, Masakazu Soshi, Ron Steinfeld, Hongwei Sun, Michael Szydlo, Uday Tupakula, Guilin Wang, Huaxiong Wang, Mingsheng Wang, Christopher Wolf, Hongjun Wu, Wenling Wu, Yongdong Wu, Shouhuai Xu, Masato Yamamichi, Jeong Yi, Xibin Zhao

Table of Contents

Security Modelling

Web Security

Security Protocols

Cryptanalysis

Key Management

Efficient Implementations