Lecture Notes in Computer Science 3089

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Markus Jakobsson Moti Yung
Jianying Zhou (Eds.)

Applied Cryptography and Network Security

Second International Conference, ACNS 2004
Yellow Mountain, China, June 8-11, 2004
Proceedings

Springer

Volume Editors

Markus Jakobsson
RSA Laboratories
1203 Garden Street, Hoboken, NJ 07030, USA
E-mail: mjakobsson@rsasecurity.com

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

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

Library of Congress Control Number: 2004106759

CR Subject Classification (1998): E.3, C.2, D.4.6, H.3-4, K.4.4, K.6.5

ISSN 0302-9743
ISBN 3-540-22217-0 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 11014096 06/3142 5 4 3 2 1 0

Preface

The second International Conference on Applied Cryptography and Network Security (ACNS 2004) was sponsored and organized by ICISA (the International Communications and Information Security Association). It was held in Yellow Mountain, China, June 8–11, 2004. The conference proceedings, representing papers from the academic track, are published in this volume of the Lecture Notes in Computer Science (LNCS) of Springer-Verlag.

The area of research that ACNS covers has been gaining importance in recent years due to the development of the Internet, which, in turn, implies global exposure of computing resources. Many fields of research were covered by the program of this track, presented in this proceedings volume. We feel that the papers herein indeed reflect the state of the art in security and cryptography research, worldwide.

The program committee of the conference received a total of 297 submissions from all over the world, of which 36 submissions were selected for presentation during the academic track. In addition to this track, the conference also hosted a technical/industrial track of presentations that were carefully selected as well. All submissions were reviewed by experts in the relevant areas.

Starting from the first ACNS conference last year, ACNS has given best paper awards. Last year the best student paper award went to a paper that turned out to be the only paper written by a single student for ACNS 2003. It was Kwong H. Yung who got the award for his paper entitled "Using Feedback to Improve Masquerade Detection." Continuing the "best paper tradition" this year, the committee decided to select two student papers among the many high-quality papers that were accepted for this conference, and to give them best student paper awards. These papers are: "Security Measurements of Steganographic Systems" by Weiming Zhang and Shiqu Li, and "Evaluating Security of Voting Schemes in the Universal Composability Framework" by Jens Groth. Both papers appear in this proceedings volume, and we would like to congratulate the recipients for their achievements.

Many people and organizations helped in making the conference a reality. We would like to take this opportunity to thank the program committee members and the external experts for their invaluable help in producing the conference's program. We also wish to thank Thomas Herlea of KU Leuven for his extraordinary efforts in helping us to manage the submissions and for taking care of all the technical aspects of the review process. Thomas, single-handedly, served as the technical support committee of this conference! We extend our thanks also to the general chair Jianying Zhou (who also served as publication chair and helped in many other ways), the chairs of the technical/industrial track (Yongfei Han and Peter Landrock), the local organizers, who worked hard to assure that the conference took place, and the publicity chairs. We also thank the various

sponsoring companies and government bodies. Finally, we would like to thank all the authors who submitted papers to the conference.

April 2004 Markus Jakobsson and Moti Yung

ACNS 2004

Second International Conference on Applied Cryptography and Network Security

Yellow Mountain, China
June 8–11, 2004

Sponsored and organized by the

International Communications and Information Security Association (ICISA)

In co-operation with

MiAn Pte Ltd (ONETS), China
RSA Security Inc., USA
Ministry of Science and Technology, China
Yellow Mountain City Government, China

General Chair

Jianying Zhou ..... Institute for Infocomm Research, Singapore

Program Chairs

Markus Jakobsson ..... RSA Labs, USA
Moti Yung ..... Columbia University, USA

Program Committee

Masayuki Abe ..... NTT, Japan
N. Asokan ..... Nokia, Finland
Feng Bao ..... I2R, Singapore
Kijoon Chae ..... Ewha Women's Univ., Korea
Ed Dawson ..... QUT, Australia
Xiaotie Deng ..... City Univ. of HK, China
Philippe Golle ..... PARC, USA
Dieter Gollmann ..... TU Hamburg, Germany
Goichiro Hanaoka ..... Univ. of Tokyo, Japan
Els van Herreweghen ..... IBM, Zurich
Chi-Sung Laih ..... NCKU, Taiwan
Kwok-Yan Lam ..... Tsinghua Univ., China
Heejo Lee ..... Korea Univ., Korea

Pil Joong Lee ..... Postech, Korea
Helger Lipmaa ..... Helsinki Univ. of Tech., Finland
Javier Lopez ..... Univ. of Malaga, Spain
Charanjit Jutla ..... IBM T.J. Watson, USA
Hiroaki Kikuchi ..... Univ. of Tokai, Japan
Kwangjo Kim ..... Info. & Communication Univ., Korea
Wenbo Mao ..... HP Labs, UK
David Naccache ..... Gemplus, France
Chanathip Namprempre ..... Thammasat U., Thailand
Phong Nguyen ..... ENS, France
Adrian Perrig ..... Carnegie Mellon Univ., USA
Josef Pieprzyk ..... Macquarie University, Australia
Radha Poovendran ..... Univ. of Washington, USA
Tomas Sander ..... HP Labs, USA
Dawn Song ..... Carnegie Mellon Univ., USA
Julien Stern ..... Cryptolog International, France
Sal Stolfo ..... Columbia Univ., USA
Michael Szydlo ..... RSA Labs, USA
Wen-Guey Tzeng ..... NCTU, Taiwan
Shouhuai Xu ..... Univ. of Texas at San Antonio, USA
Bennet Yee ..... Google, USA
Yuliang Zheng ..... UNC Charlotte, USA

Chairs of Technical/Industrial Track

Yongfei Han ..... ONETS, China
Peter Landrock ..... Cryptomathic, Denmark

Publicity Chairs

Michael Szydlo ..... RSA Labs, USA
Guilin Wang ..... I2R, Singapore

Technical and Administrative Support

Thomas Herlea ..... KU Leuven, Belgium
Li Xue ..... ONETS, China

External Reviewers

Michel Abdalla, Nuttapong Attrapadung, Dan Bailey, Dirk Balfanz, Endre-Felix Bangerter, Alexandra Boldyreva, Colin Boyd, Eric Brier, Julien Brouchier, Sonja Buchegger, Christian Cachin, Jan Camenisch, Cedric Cardonnel, Haowen Chan, Xiaofeng Chen, Benoît Chevallier-Mames, Hung Chim, Jung-Hui Chiu, Jae-Gwi Choi, Chen-Kang Chu, Siu-Leung Chung, Andrew Clark, Scott Contini, Jean-Sébastien Coron, Yang Cui, Matthew Dailey,

Jean-François Dhem, Xuhua Ding, Glenn Durfee, Pasi Eronen, Chun-I Fan, Serge Fehr, Atsushi Fujioka, Eiichiro Fujisaki, Debin Gao, Philip Ginzboorg, Juanma Gonzalez-Nieto, Louis Goubin, Zhi Guo, Shin Seong Han, Yumiko Hanaoka, Helena Handschuh, Matt Henricksen, Sha Huang, Yong Ho Hwang, Tetsuya Izu, Moon Su Jang, Ari Juels, Burt Kaliski, Bong Hwan Kim, Byung Joon Kim, Dong Jin Kim, Ha Won Kim, Kihyun Kim, Tae-Hyung Kim, Yuna Kim, Lea Kissner, Tetsutaro Kobayashi, Byoungcheon Lee, Dong Hoon Lee, Hui-Lung Lee, Chin-Laung Lei, Jung-Shian Li, Mingyan Li, Minming Li, Tieyan Li, Becky Jie Liu, Krystian Matusiewicz, Bill Millan, Ilya Mironov, David M'Raïhi, Yasusige Nakayama, Gregory Neven, James Newsome, Valtteri Niemi, Takashi Nishi, Kaisa Nyberg, Luke O'Connor, Kazuto Ogawa, Miyako Ohkubo, Jose A. Onieva, Pascal Paillier, Dong Jin Park, Heejae Park, Jae Hwan Park, Joonhah Park, Leonid Peshkin, Birgit Pfitzmann, James Riordan, Rodrigo Roman, Ludovic Rousseau, Markku-Juhani Saarinen, Radha Sampigethaya, Paolo Scotton, Elaine Shi, Sang Uk Shin, Diana Smetters, Miguel Soriano, Jessica Staddon, Ron Steinfeld, Reto Strobl, Hong-Wei Sun, Koutarou Suzuki, Vanessa Teague, Lawrence Teo, Ali Tosun, Johan Wallen, Guilin Wang, Huaxiong Wang, Yuji Watanabe, Yoo Jae Won, Yongdong Wu, Yeon Hyeong Yang, Tommy Guoming Yang, Sung Ho Yoo, Young Tae Youn, Dae Hyun Yum, Rui Zhang, Xinwen Zhang, Hong Zhao, Xi-Bin Zhao, Yunlei Zhao, Huafei Zhu

Table of Contents

Security Modelling

Authenticated Key Exchange

Security of Deployed Systems

Cryptosystems: Design and Analysis

Cryptographic Protocols

Side Channels and Protocol Analysis

Intrusion Detection and DoS

Cryptographic Algorithms