# Lecture Notes in Computer Science 3989

Jianying Zhou Moti Yung Feng Bao (Eds.)

# Applied Cryptography and Network Security

4th International Conference, ACNS 2006
Singapore, June 6-9, 2006
Proceedings

Springer

Volume Editors

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

Moti Yung
Columbia University, RSA Laboratories
1214 Amsterdam Avenue, New York, NY 10027, USA
E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2006926666

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-34703-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-34703-3 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11767480 06/3142 5 4 3 2 1 0

# Preface

The 4th International Conference on Applied Cryptography and Network Security (ACNS 2006) was held in Singapore, during June 6-9, 2006. ACNS 2006 brought together individuals from academia and industry involved in multiple research disciplines of cryptography and security to foster exchange of ideas. This volume (LNCS 3989) contains papers presented in the academic track.

ACNS was set a high standard when it was initiated in 2003. There has been a steady improvement in the quality of its program in the past 4 years: ACNS 2003 (Kunming, China), ACNS 2004 (Yellow Mountain, China), ACNS 2005 (New York, USA), ACNS 2006 (Singapore). The average acceptance rate is kept at around 16%. We wish to receive the continued support from the community of cryptography and security worldwide to further improve its quality and make ACNS one of the leading conferences.

The Program Committee of ACNS 2006 received a total of 218 submissions from all over the world, of which 33 were selected for presentation at the academic track. In addition to this track, the conference also hosted an industrial track of presentations that were carefully selected as well. All submissions were reviewed by experts in the relevant areas. We are indebted to our Program Committee members and the external reviewers for the great job they have performed. The proceedings contain revised versions of the accepted papers. However, revisions were not checked and the authors bear full responsibility for the content of their papers.

More people deserve thanks for their contribution to the success of the conference. We sincerely thank General Chair Feng Bao for his support and encouragement. Our special thanks are due to Ying Qiu for managing the website for paper submission, review and notification. Shen-Tat Goh and Patricia Loh were kind enough to arrange for the conference venue and took care of the administration in running the conference. Without the hard work of the local organizing team, this conference would not have been possible. We would also like to thank all the authors who submitted papers and the participants from all over the world who chose to honor us with their attendance.

Last but not the least, we are grateful to the Institute for Infocomm Research for organizing and sponsoring the conference.

April 2006

Jianying Zhou
Moti Yung

# ACNS 2006

## 4th International Conference on Applied Cryptography and Network Security

## Singapore
## June 6-9, 2006

*Organized and Sponsored by*

Institute for Infocomm Research, Singapore

## General Chair

| | |
|---|---|
| Feng Bao | Institute for Infocomm Research, Singapore |

## Program Chairs

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

## Program Committee

| | |
|---|---|
| Carlisle Adams | Univ. of Ottawa, Canada |
| Tuomas Aura | Microsoft Research, UK |
| Roberto Avanzi | Ruhr Univ., Germany |
| Giampaolo Bella | Univ. of Catania, Italy |
| Kefei Chen | Shanghai Jiaotong Univ., China |
| Ed Dawson | QUT, Australia |
| Robert Deng | SMU, Singapore |
| Xiaotie Deng | City Univ., Hong Kong |
| Yvo Desmedt | UCL, UK |
| Marc Girault | France Telecom, France |
| Dieter Gollmann | TU Harburg, Germany |
| Stefanos Gritzalis | Univ. of the Aegean, Greece |
| Jens Groth | UCLA, USA |
| Peter Gutmann | Univ. of Auckland, New Zealand |
| Yongfei Han | ONETS, China |
| Amir Herzberg | Bar-Ilan Univ., Israel |
| John Ioannidis | Columbia Univ., USA |
| Jonathan Katz | Univ. of Maryland, USA |
| Angelos D. Keromytis | Columbia Univ., USA |
| Taekyoung Kwon | Sejong Univ., Korea |
| Wenke Lee | Georgia Institute of Tech., USA |
| Ninghui Li | Purdue Univ., USA |

| | |
|---|---|
| Javier Lopez | Univ. of Malaga, Spain |
| Stefan Lucks | Univ. of Mannheim, Germany |
| Subhamoy Maitra | ISI, India |
| Patrick McDaniel | PSU, USA |
| Chris Mitchell | RHUL, UK |
| Refik Molva | Eurecom, France |
| Sang-Jae Moon | KNU, Korea |
| David Naccache | ENS, France |
| Rolf Oppliger | eSECURITY Technologies, Switzerland |
| Elisabeth Oswald | Graz Univ. of Tech., Austria |
| Guenther Pernul | Univ. of Regensburg, Germany |
| Raphael Phan | Swinburne UT, Malaysia |
| Michael Roe | Microsoft Research, UK |
| Rei Safavi-Naini | Univ. of Wollongong, Australia |
| Kouichi Sakurai | Kyushu Univ., Japan |
| Pierangela Samarati | Univ. of Milan, Italy |
| Vitaly Shmatikov | UT Austin, USA |
| Masakazu Soshi | JAIST, Japan |
| Francois-Xavier Standaert | UCL, Belgium |
| Ravi Sundaram | Northeastern Univ., USA |
| Tsuyoshi Takagi | Future Univ., Japan |
| Pim Tuyls | Philips Research, The Netherlands |
| Wen-Guey Tzeng | NCTU, Taiwan |
| Guilin Wang | I2R, Singapore |
| Xiaofeng Wang | Indiana Univ., USA |
| Brent Waters | Stanford Univ., USA |
| Yuliang Zheng | UNCC, USA |

## Publicity Chair

| | |
|---|---|
| Yongfei Han | ONETS, China |

## Organizing Committee

| | |
|---|---|
| Shen-Tat Goh | Institute for Infocomm Research, Singapore |
| Patricia Loh | Institute for Infocomm Research, Singapore |
| Ying Qiu | Institute for Infocomm Research, Singapore |

## Steering Committee

| | |
|---|---|
| Yongfei Han | ONETS, China |
| Moti Yung | Columbia University, USA |
| Jianying Zhou | Institute for Infocomm Research, Singapore |

## External Reviewers

Abhinav Kamra
Ajay Mahimkar
Angelos Stavrou
Avishek Adhikari
Benoit Libert
Bessie Hu
Boniface Hicks
Chae Hoon Lim
Chen-Kang Chu
Christian Schlager
Christoph Herbst
Christopher Wolf
Colin Boyd
Costas Karafasoulis
DaeHun Nyang
Dibyendu Chakrabarti
Dieter Schmidt
Duncan S. Wong
Duong Hieu Phan
Eike Kiltz
Elisavet Constantinou
Eric Dahmen
Eric Peeters
Ewan Fleischmann
Fabien Pouget
Frederik Armknecht
Gaurav Kc
Gene Beck Hahn
George Kambourakis
Greg Rose
Gregory Neven
Guerric Meurice
Guomin Yang
Herve Denar
Herve Sibert
Hidenori Kuwakado
Hovav Shacham
Hui Li
Jacques Traore
Jan Kolter
Jason Gower
Jeong Ok Kwon
Jian Wen
Jiangtao Li
Jie Guo
Ji-Won Byun
Joerg Gilberg
Johann Groszschaedl
John Canny
Juan Gonzalez Nieto
Julien Cathalo
Katja Schmidt-Samoa
Ke Wang
Keisuke Hakuta
Kenji Imamoto
Kenny Paterson
Kevin Butler
Khoongming Khoo
Kris Gaj
Kun Peng
Kurt Dietrich
Lan Nguyen
Larry Washington
Laurent Butti
Lifeng Guo
Lihua Wang
Ling Dong
Liqun Chen
Ahmad-Reza Sadeghi
Lisa Johanson
Liu Yang
Lizhen Yang
Ludwig Fuchs
Manfred Aigner
Marc Fischlin
Maria Karyda
Martin Feldhofer
Masahiro Mambo
Masayuki Terada
Mathieu Ciet
Benoit Feix
Matthew Burnside
Melek Onen
Mi Wen
Michael Jacobson
Michael Locasto
Nasir Memon
Olivier Lepetit

Olivier Pereira
Palash Sarkar
Patrick Traynor
Petros Belsis
Pierre Creut
Qi Qi
Qiang Tang
Qianhong Wu
Qihua Wang
Raylin Tso
Rodrigo Roman
Rolf Schillinger
Routo Terada
Rui Xue
Sabrina De Capitani di Vimercati
Sandra Dominikus
Shengli Liu
Shiao-Ying Lin
Shinsaku Kiyomoto
Shiqun Li
Shlomo Hershkop
Shuhong Wang
Siamak Fayyaz
Soonhak Kwon
Stanislas Francfort
Stelios Sidiroglou
Stehane Socie
Seastien Canard
Tae Hyun Kim
Tanja Lange
Tanmoy Kanti Das
Theodoros Balopoulos
Toru Nakanishi
Vanessa Gratzer
Wei Gao
Wei-Jen Li
Wolfgang Dobmeier
Xavier Boyen
Xinming Ou
Xinyi Huang
Yong-Sork Her
Yoshifumi Ueshige
Young Ho Park
Yu Long
Yunlei Zhao
Yvonne Hitchcock
Zhuowei Li

# Table of Contents

## Intrusion Avoidance and Detection

## Cryptographic Applications

## DoS: Attacks and Countermeasures

## Key Management

## Cryptanalysis

## Security of Limited Devices

## Cryptography

## Authentication and Web Security

## Ad Hoc and Sensor Network Security

## Cryptographic Constructions

## Security and Privacy