

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Jianying Zhou Moti Yung Feng Bao (Eds.)

Applied Cryptography and Network Security

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

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

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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2006

Printed in Germany

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 BaoInstitute for Infocomm Research, Singapore

Program Chairs

Jianying ZhouInstitute for Infocomm Research, Singapore
Moti YungColumbia 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 Groszschädl
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
Liquan 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 Gratzner
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

Adaptive Detection of Local Scanners <i>Ahren Studer, Chenxi Wang</i>	1
Probabilistic Proof of an Algorithm to Compute TCP Packet Round-Trip Time for Intrusion Detection <i>Jianhua Yang, Yongzhong Zhang</i>	18
DSO: Dependable Signing Overlay <i>Guofei Gu, Prahlad Fogla, Wenke Lee, Douglas Blough</i>	33

Cryptographic Applications

Do Broken Hash Functions Affect the Security of Time-Stamping Schemes? <i>Ahto Buldas, Sven Laur</i>	50
A Handy Multi-coupon System <i>Sébastien Canard, Aline Gouget, Emeline Hufschmitt</i>	66
An Efficient Single-Key Pirates Tracing Scheme Using Cover-Free Families <i>Dongvu Tonien, Reihaneh Safavi-Naini</i>	82

DoS: Attacks and Countermeasures

Efficient Memory Bound Puzzles Using Pattern Databases <i>Sujata Doshi, Fabian Monrose, Aviel D. Rubin</i>	98
Effect of Malicious Synchronization <i>Mun Choon Chan, Ee-Chien Chang, Liming Lu, Peng Song Ngiam</i>	114
Misusing Unstructured P2P Systems to Perform DoS Attacks: The Network That Never Forgets <i>Elias Athanasopoulos, Kostas G. Anagnostakis, Evangelos P. Markatos</i>	130

Key Management

Password Based Server Aided Key Exchange <i>Yvonne Cliff, Yiu Shing Terry Tin, Colin Boyd</i>	146
Secure Password-Based Authenticated Group Key Agreement for Data-Sharing Peer-to-Peer Networks <i>Qiang Tang, Kim-Kwang Raymond Choo</i>	162
Stateful Subset Cover <i>Mattias Johansson, Gunnar Kreitz, Fredrik Lindholm</i>	178

Cryptanalysis

The Rainbow Attack on Stream Ciphers Based on Maiorana-McFarland Functions <i>Khoongming Khoo, Guang Gong, Hian-Kiat Lee</i>	194
Breaking a New Instance of TTM Cryptosystems <i>Xuyun Nie, Lei Hu, Jianyu Li, Crystal Updegrove, Jintai Ding</i>	210
Cryptanalysis of the N-Party Encrypted Diffie-Hellman Key Exchange Using Different Passwords <i>Raphael C.-W. Phan, Bok-Min Goi</i>	226

Security of Limited Devices

An AES Smart Card Implementation Resistant to Power Analysis Attacks <i>Christoph Herbst, Elisabeth Oswald, Stefan Mangard</i>	239
Physical Security Bounds Against Tampering <i>Kerstin Lemke, Christof Paar, Ahmad-Reza Sadeghi</i>	253
Flexible Exponentiation with Resistance to Side Channel Attacks <i>Camille Vuillaume, Katsuyuki Okeya</i>	268

Cryptography

An Improved Poly1305 MAC <i>Dayin Wang, Dongdai Lin, Wenling Wu</i>	284
--	-----

Certificateless Public-Key Signature: Security Model and Efficient Construction	
<i>Zhenfeng Zhang, Duncan S. Wong, Jing Xu, Dengguo Feng</i>	293

High Diffusion Cipher: Encryption and Error Correction in a Single Cryptographic Primitive	
<i>Chetan Nanjunda Mathur, Karthik Narayan, K.P. Subbalakshmi</i>	309

Authentication and Web Security

Authentication for Paranoids: Multi-party Secret Handshakes	
<i>Stanisław Jarecki, Jihye Kim, Gene Tsudik</i>	325

On the Security of the Authentication Module of Chinese WLAN Standard Implementation Plan	
<i>Xinghua Li, SangJae Moon, Jianfeng Ma</i>	340

W3Bcrypt: Encryption as a Stylesheet	
<i>Angelos Stavrou, Michael E. Locasto, Angelos D. Keromytis</i>	349

Ad Hoc and Sensor Network Security

Combinatorial Structures for Design of Wireless Sensor Networks	
<i>Dibyendu Chakrabarti, Jennifer Seberry</i>	365

Public Key Cryptography Sans Certificates in Ad Hoc Networks	
<i>Nitesh Saxena</i>	375

Location-Aware Key Management Using Multi-layer Grids for Wireless Sensor Networks	
<i>JongHyup Lee, Taekyoung Kwon, Jooseok Song</i>	390

Cryptographic Constructions

A General Methodology for Pipelining the Point Multiplication Operation in Curve Based Cryptography	
<i>Kishan Chand Gupta, Pradeep Kumar Mishra, Pinakpani Pal</i>	405

Results on Almost Resilient Functions	
<i>Pinhui Ke, Jie Zhang, Qiaoyan Wen</i>	421

Real Perfect Contrast Visual Secret Sharing Schemes with Reversing	
<i>Ching-Nung Yang, Chung-Chun Wang, Tse-Shih Chen</i>	433

Security and Privacy

On Optimizing the Security-Throughput Trade-Off in Wireless
Networks with Adversaries

*Mohamed A. Haleem, Chetan Nanjunda Mathur, R. Chandramouli,
K.P. Subbalakshmi* 448

Improving the Randomized Initial Point Countermeasure Against DPA

Kowichi Itoh, Tetsuya Izu, Masahiko Takenaka 459

Syntax-Driven Private Evaluation of Quantified Membership Queries

Aggelos Kiayias, Antonina Mitrofanova 470

Author Index 487