Lecture Notes in Computer Science 4521

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

Editorial Board

Jonathan Katz Moti Yung (Eds.)

Applied Cryptography and Network Security

5th International Conference, ACNS 2007
Zhuhai, China, June 5-8, 2007
Proceedings

Springer

Volume Editors

Jonathan Katz
University of Maryland
Dept. of Computer Science
A.V. Williams Building, College Park, MD 20742, USA
E-mail: jkatz@cs.umd.edu

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

Library of Congress Control Number: 2007927501

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-72737-X Springer Berlin Heidelberg New York
ISBN-13 978-3-540-72737-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12067848 06/3180 5 4 3 2 1 0

Preface

The Fifth International Conference on Applied Cryptography and Network Security (ACNS 2007) was held in Zhuhai, China, June 5–8, 2007. This volume contains papers that were accepted to the academic track of the conference.

The conference received an astounding number of submissions this year, which made the review process a challenging and demanding task. We are indebted to the members of the Program Committee and the external reviewers for all their hard work. The committee accepted 31 papers from roughly 260 submissions. These proceedings contain revised versions of the accepted papers. While revisions are expected to take the referees' comments into account, this was not enforced and the authors bear full responsibility for the content of their papers.

In addition to the academic track, the conference hosted a non-archival industrial track whose papers were also carefully selected from among the submissions.

Shai Halevi deserves the community's gratitude for writing his Web submission and review software, which we used for this conference. On a more personal level, we would like to extend our own deepest thanks to Shai for not only writing his software, but for installing and maintaining the submission server for this conference. Thanks go also to the International Association for Cryptologic Research (IACR) for agreeing to host the server.

It is our pleasure to thank the General Chair Yongfei Han, the Publicity Chair Jianying Zhou, and the Chair of the Organizing Committee Li Nan for their help and support in putting this conference together. Without their help, this conference would not have been possible. Finally, we are grateful to ONETS and Zhuhai College, Jilin University, for sponsoring the conference.

March 2007

Jonathan Katz
Moti Yung

ACNS 2007

Fifth International Conference on Applied Cryptography and Network Security

Zhuhai, China
June 5-8, 2007

Organized and Sponsored by

ONETS, China
and
Zhuhai College, Jilin University, China

General Chair

Yongfei Han ..... ONETS, China

Program Chairs

Jonathan Katz ..... University of Maryland, USA
Moti Yung ..... Columbia University, USA

Program Committee

Giuseppe Ateniese ..... Johns Hopkins University, USA
Michael Backes ..... Saarland University, Germany
Feng Bao ..... Institute for Infocomm Research, Singapore
Steven M. Bellovin ..... Columbia University, USA
John Black ..... University of Colorado at Boulder, USA
Levente Buttyán .Budapest University of Technology and Economics, Hungary
Claude Castellucia ..... INRIA, France
Jean-Sébastien Coron ..... University of Luxembourg, Luxembourg
Nicolas Courtois ..... University College of London, UK and Gemalto, France
Kevin Fu ..... University of Massachusetts Amherst, USA
Philippe Golle ..... PARC, USA
Michael Goodrich ..... University of California at Irvine, USA
Alejandro Hevia ..... University of Chile, Chile
Susan Hohenberger ..... IBM Research, Switzerland
Nick Hopper ..... University of Minnesota, USA
Charanjit Jutla ..... IBM Research, USA

Kaoru Kurosawa ..... Ibaraki University, Japan
Xuejia Lai ..... Shanghai Jiaotong University, China
Dong Hoon Lee ..... CIST, South Korea
Phil MacKenzie ..... Google, USA
Ilya Mironov ..... Microsoft Research, USA
Pascal Paillier ..... Gemalto, France
Kenny Paterson ..... Royal Holloway, University of London, UK
Raphael Phan ..... EPFL, Switzerland
Benny Pinkas ..... University of Haifa, Israel
David Pointcheval ..... CNRS and ENS, France
Zulfikar Ramzan ..... Symantec, Inc., USA
Phil Rogaway ..... UC Davis, USA and Chiang Mai University, Thailand
Kazue Sako ..... NEC, Japan
Palash Sarkar ..... Indian Statistical Institute, India
Vitaly Shmatikov ..... University of Texas at Austin, USA
Thomas Shrimpton ..... Portland State University, USA
Nigel Smart ..... University of Bristol, UK
Ron Steinfeld ..... Macquarie University, Australia
Adam Stubblefield ..... Johns Hopkins University, USA
Mike Szydlo ..... Akamai, USA
Brent Waters ..... SRI International, USA
Avishai Wool ..... Tel Aviv University, Israel
Sung-Ming Yen ..... National Central University, Taiwan
Jianying Zhou ..... Institute for Infocomm Research, Singapore

Publicity Chair

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

Organizing Committee

Li Nan ..... ONETS, China

Steering Committee

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

External Reviewers

Gergely Acs
Ben Adida
Toshinori Araki
Joonsang Baek
Dan Bailey
Lucas Ballard
Gregory V. Bard
Elad Barkan
Constantinos Bartzis
Ohad Ben-Cohen
Boldizsar Bencsath
Bobby Bhattacharjee

Marina Blanton
Jin Wook Byun
Srdjan Capkun
Aldar Chan
Melissa Chase
Sanjit Chatterjee
Chien-Ning Chen
Pau-Chen Cheng
Benoit Chevallier-Mames
Han-Fei Chiang
Kuo-Zhe Chiou
Eun Young Choi
Kyu Young Choi
Seung Geol Choi
JM Combes
Scott Contini
Debbie Cook
Laszlo Csik
Yang Cui
Reza Curtmola
Dimitri DeFigueiredo
Blandine Debraize
Benessa Defend
Alex Dent
Laszlo Dora
Ehud Doron
Markus Duermuth
Wu-chang Feng
Pierre-Alain Fouque
Aurelien Francillon
Eiichiro Fujisaki
Jun Furukawa
Steven Galbraith
Craig Gentry
Vipul Goyal
Matt Green
David Gross-Amblard
Fanglu Guo
Goichiro Hanaoka
Carmit Hazay
Swee-Huay Heng
T. Heydt-Benjamin
Shoichi Hirose
James Hoagland
Chao-Chih Hsu
Toshiyuki Isshiki
Ik Rae Jeong
Antoine Joux
Marcelo Kaihara
Edward Kaiser
Yael Tauman Kalai
Seny Kamara
Aggelos Kiayias
Eike Kiltz
Bum Han Kim
Hugo Krawczyk
Jeong Ok Kwon
Amit Lakhani
Loukas Lazos
Hwa Sung Lee
Hyun Sook Lee
Tieyan Li
Xiangxue Li
Wei-Chih Lien
Hsi-Chung Lin
Lang Lin
Yehuda Lindell
Nathan Linger
Matteo Maffei
Wenbo Mao
Josh Mason
Breno de Medeiros
Kazuhiko Minematsu
Atsuko Miyaji
Nagendra Modadugu
Kengo Mori
Yoichiro Morita
Masayuki Nakae
Toru Nakanishi
Juanma Nieto
Satoshi Obana
Jong Whan Park
Maura Paterson
Michael Ø. Pedersen
Chris Peikert
Duong Hieu Phan
Le Trieu Phong
Josef Pieprzyk
Axel Poschman
Julio Quinteros
Moheeb Abu Rajab
David Safford
Peter Schaffer
Jacob Schuldt
Hovav Shacham
Radu Sion
William Skeith
Sam Small
Angelo Spognardi
Martijn Stam
Keisuke Tanaka
Isamu Teranishi
Dominique Unruh
Matthew Vail
Istvan Vajda
Yongdong Wu
Guilin Wang
Huaxiong Wang
Enav Weinreb
Stephen A. Weis
Chi-Dian Wu
Kazuo Yanoo
Po-Wah Yau
Lidong Zhou
Huafei Zhu

Table of Contents

Signature Schemes I

Generic Transformation to Strongly Unforgeable Signatures 1
Qiong Huang, Duncan S. Wong, and Yiming Zhao

Efficient Generic On-Line/Off-Line Signatures Without Key Exposure 18
Xiaofeng Chen, Fangguo Zhang, Willy Susilo, and Yi Mu

Merkle Signatures with Virtually Unlimited Signature Capacity 31
Johannes Buchmann, Erik Dahmen, Elena Klintsevich, Katsuyuki Okeya, and Camille Vuillaume

Computer and Network Security

Midpoints Versus Endpoints: From Protocols to Firewalls 46
Diana von Bidder-Senn, David Basin, and Germano Caronni

An Adversary Aware and Intrusion Detection Aware Attack Model Ranking Scheme 65
Liang Lu, Rei Safavi-Naini, Jeffrey Horton, and Willy Susilo

Analyzing an Electronic Cash Protocol Using Applied Pi Calculus 87
Zhengqin Luo, Xiaojuan Cai, Jun Pang, and Yuxin Deng

Cryptanalysis

Cryptanalysis of the TRMC-4 Public Key Cryptosystem 104
Xuyun Nie, Lei Hu, Jintai Ding, Jianyu Li, and John Wagner

Estimating the Prime-Factors of an RSA Modulus and an Extension of the Wiener Attack 116
Hung-Min Sun, Mu-En Wu, and Yao-Hsin Chen

A Timing Attack on Blakley's Modular Multiplication Algorithm, and Applications to DSA 129
Bahador Bakhshi and Babak Sadeghiyan

Protecting AES Software Implementations on 32-Bit Processors Against Power Analysis 141
Stefan Tillich, Christoph Herbst, and Stefan Mangard

Group-Oriented Security

Constant-Round Authenticated Group Key Exchange with Logarithmic Computation Complexity 158
Junghyun Nam, Juryon Paik, Ung Mo Kim, and Dongho Won

Preventing Collusion Attacks on the One-Way Function Tree (OFT) Scheme 177
Xuxin Xu, Lingyu Wang, Amr Youssef, and Bo Zhu

Bayesian Methods for Practical Traitor Tracing 194
Philip Zigoris and Hongxia Jin

Cryptographic Protocols

A New Protocol for Conditional Disclosure of Secrets and Its Applications 207
Sven Laur and Helger Lipmaa

An Unconditionally Secure Protocol for Multi-Party Set Intersection ... 226
Ronghua Li and Chuankun Wu

Privacy-Preserving Set Union 237
Keith Frikken

Anonymous Authentication

Universal Accumulators with Efficient Nonmembership Proofs 253
Jiangtao Li, Ninghui Li, and Rui Xue

Unlinkable Secret Handshakes and Key-Private Group Key Management Schemes 270
Stanisław Jarecki and Xiaomin Liu

Identity-Based Cryptography

Identity-Based Proxy Re-encryption 288
Matthew Green and Giuseppe Ateniese

A More Natural Way to Construct Identity-Based Identification Schemes 307
Guomin Yang, Jing Chen, Duncan S. Wong, Xiaotie Deng, and Dongsheng Wang

Tweaking TBE/IBE to PKE Transforms with Chameleon Hash Functions 323
Rui Zhang

Certified E-Mail Protocol in the ID-Based Setting 340
Chunxiang Gu, Yuefei Zhu, and Yonghui Zheng

Security in Wireless, Ad-Hoc, and Peer-to-Peer Networks

Efficient Content Authentication in Peer-to-Peer Networks 354
Roberto Tamassia and Nikos Triandopoulos

An Identity-Based Signcryption Scheme for Multi-domain Ad Hoc Networks 373
Fagen Li, Yupu Hu, and Chuanrong Zhang

Efficient Self-healing Key Distribution with Revocation for Wireless Sensor Networks Using One Way Key Chains 385
Ratna Dutta, Ee-Chien Chang, and Sourav Mukhopadhyay

BAP: Broadcast Authentication Using Cryptographic Puzzles 401
Patrick Schaller, Srdjan Čapkun, and David Basin

Efficient Implementation

Compressed XTR 420
Masaaki Shirase, Dong-Guk Han, Yasushi Hibino, Ho Won Kim, and Tsuyoshi Takagi

Sliding Window Method for NTRU 432
Mun-Kyu Lee, Jung Woo Kim, Jeong Eun Song, and Kunsoo Park

Signature Schemes II

Efficient Certificateless Signature Schemes 443
Kyu Young Choi, Jong Hwan Park, Jung Yeon Hwang, and Dong Hoon Lee

Security Mediated Certificateless Signatures 459
Wun-She Yap, Sherman S.M. Chow, Swee-Huay Heng, and Bok-Min Goi

Gradually Convertible Undeniable Signatures 478
Laila El Aimani and Damien Vergnaud

Author Index 497