

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

New York University, NY, 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

John Ioannidis Angelos Keromytis
Moti Yung (Eds.)

Applied Cryptography and Network Security

Third International Conference, ACNS 2005
New York, NY, USA, June 7-10, 2005
Proceedings

Volume Editors

John Ioannidis
Columbia University
Center for Computational Learning Systems
NY, USA
E-mail: ji@cs.columbia.edu

Angelos Keromytis
Moti Yung
Columbia University
Department of Computer Science
NY, USA
E-mail: {angelos,moti}@cs.columbia.edu

Library of Congress Control Number: 2005926829

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

ISSN	0302-9743
ISBN-10	3-540-26223-7 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-26223-7 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

springeronline.com

© Springer-Verlag Berlin Heidelberg 2005
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 11496137 06/3142 5 4 3 2 1 0

Preface

The 3rd International Conference on Applied Cryptography and Network Security (ACNS 2005) was sponsored and organized by ICISA (the International Communications and Information Security Association). It was held at Columbia University in New York, USA, June 7–10, 2005. This conference proceedings volume contains papers presented in the academic/research track.

ACNS covers a large number of research areas that have been gaining importance in recent years due to the development of the Internet, wireless communication and the increased global exposure of computing resources. The papers in this volume are representative of the state of the art in security and cryptography research, worldwide.

The Program Committee of the conference received a total of 158 submissions from all over the world, of which 35 submissions were selected for presentation at the academic track. In addition to this track, the conference also hosted a technical/ industrial/ short papers track whose presentations were also carefully selected from among the submissions. All submissions were reviewed by experts in the relevant areas.

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 Michael E. Locasto for his help in all technical and technological aspects of running the conference and Sophie Majewski for the administrative support in organizing the conference. We wish to thank the graduate students at Columbia University's Computer Science Department who helped us as well.

We wish to acknowledge the financial support of our sponsors, and their employees who were instrumental in the sponsorship process: Morgan Stanley (Ben Fried), Gemplus (David Naccache), and Google (Niels Provos).

Finally, we would like to thank all the authors who submitted papers to the conference; the continued support of the security and cryptography research community worldwide is what really enabled us to have this conference.

May 2005

John Ioannidis
Angelos Keromytis
Moti Yung

ACNS 2005

3rd International Conference on Applied Cryptography and Network Security

New York, USA
June 7–10, 2005

Sponsored and organized by the
International Communications and Information Security Association (ICISA)

In coöperation with
Columbia University, USA

General Chair

John Ioannidis Columbia University

Program Chairs

Moti Yung Columbia University and RSA Labs
Angelos Keromytis Columbia University

Program Committee

Scott Alexander Telcordia, USA
Tuomas Aura Microsoft Research, UK
David Brumley CMU, USA
Ran Canetti IBM Research, USA
Marc Dacier Eurecom, France
Ed Dawson Queensland University of Technology, Australia
Glenn Durfee PARC, USA
Virgil Gligor University of Maryland, USA
Peter Gutman University of Auckland, New Zealand
Goichiro Hanaoka National Institute of Advanced Industrial Science
and Technology (AIST), Japan
Amir Herzberg Bar Ilan University, Israel
Russ Housley Vigilsec, USA
John Ioannidis Columbia University, USA
Sotiris Ioannidis University of Pennsylvania, USA

Stas Jarecki	UC Irvine, USA
Ari Juels	RSA Laboratories, USA
Angelos Keromytis	Columbia University, USA
Aggelos Kiayias	University of Connecticut, USA
Tanja Lange	Ruhr-Universität Bochum, Germany
Dong Hoon Lee	Korea University, South Korea
Fabio Massacci	University Trento, Italy
Atsuko Miyaji	JAIST, Japan
Frederic Muller	DCSSI Crypto Lab, France
Kaisa Nyberg	Nokia, Finland
Bart Preneel	K.U.Leuven, Belgium
Vassilis Prevelakis	Drexel University, USA
Niels Provos	Google, USA
Pierangela Samarati	University of Milan, Italy
Tomas Sander	HP, USA
Dan Simon	Microsoft Research, USA
Tsuyoshi Takagi	T.U. Darmstadt, Germany
Wen-Guey Tzeng	NCTU, Taiwan
Dan Wallach	Rice University, USA
Susanne Wetzel	Stevens Institute, USA
Moti Yung	Columbia University, USA
Jianying Zhou	I2R, Singapore
Lidong Zhou	Microsoft Research, USA

External Reviewers

Kouichiro Akiyama, Kostas Anagnostakis, Farooq Anjum, N. Asokan, Nuttapong Attrapadung, Roberto Avanzi, Dirk Balfanz, Lejla Batina, Steven Bellovin, Josh Benaloh, Enrico Blanzieri, Christophe de Canniere, Alvaro Cardenas, Roberto Cascella, Jae-Gwi Choi, Stelvio Cimato, Jared Cordasco, Giovanni di Crescenzo, Eric Cronin, Stefano Crosta, Yang Cui, Ernesto Damiani, Seiji Doi, Wenliang Du, Detlef Duehnlein, Patrick Felke, Pierre-Alain Fouque, Eiichiro Fujisaki, Abhrajit Ghosh, Philippe Golle, Michael Greenwald, Shai Halevi, Nick Howgrave-Graham, Seokhie Hong, Omer Horvitz, Tetsu Iwata, Eliane Jaulmes, Markus Kaiser, Tetsutaro Kobayashi, Sébastien Kunz-Jacques, Kaoru Kurosawa, Klaus Kursawe, Joseph Liu, Dahlia Malkhi, Gwenaëlle Martinet, Mitsuru Matsui, Breno de Medeiros, Nele Mentens, Bernd Meyer, Ulrike Meyer, Ilya Mironov, Anderson Nascimento, Francesco De Natale, Svetla Nikova, Akihito Niwa, Takeshi Okamoto, Tatsuaki Okamoto, Renaud Pacalet, Young-Ho Park, Kirthika Parmeswaran, Guillaume Poupard, Vincent Rijmen, Michael Roe, Tomas Sander, Hisayoshi Sato, Nitesh Saxena, Katja Schmidt-Samoa, Micah Sherr, Diana Smetters, Masakazu Soshi, Jessica Staddon, Martijn Stam, Maria Striki, Gelareh Taban, Rajesh Talpade, Yuuko Tamura, Simon Tsang, Guillaume Urvoy-Keller, Frederik Vercauteren, Sabrina de Capitani di Vimercati, Camille Vuillaume, Zhiguo Wan, Guilin Wang, Kai Wirt, Hongjun Wu, Bennet Yee, Rui Zhang, Sheng Zhong, Huafei Zhu

Table of Contents

Two-Server Password-Only Authenticated Key Exchange	1
<i>Jonathan Katz, Philip MacKenzie, Gelareh Taban, and Virgil Gligor</i>	
Strengthening Password-Based Authentication Protocols	
Against Online Dictionary Attacks	17
<i>Peng Wang, Yongdae Kim, Vishal Kher, and Taekyoung Kwon</i>	
Cryptanalysis of an Improved Client-to-Client Password-Authenticated	
Key Exchange (C2C-PAKE) Scheme	33
<i>Raphael C.-W. Phan and Bok-Min Goi</i>	
Efficient Security Mechanisms	
for Overlay Multicast-Based Content Distribution	40
<i>Sencun Zhu, Chao Yao, Donggang Liu, Sanjeev Setia, and Sushil Jajodia</i>	
A Traitor Tracing Scheme Based on RSA for Fast Decryption	56
<i>John Patrick McGregor, Yiqun Lisa Yin, and Ruby B. Lee</i>	
N-Party Encrypted Diffie-Hellman Key Exchange Using Different Passwords	75
<i>Jin Wook Byun and Dong Hoon Lee</i>	
Messin' with Texas Deriving Mother's Maiden Names Using Public Records	91
<i>Virgil Griffith and Markus Jakobsson</i>	
Mitigating Network Denial-of-Service	
Through Diversity-Based Traffic Management	104
<i>Ashraf Matrawy, Paul C. van Oorschot, and Anil Somayaji</i>	
Searching for High-Value Rare Events with Uncheatable Grid Computing	122
<i>Wenliang Du and Michael T. Goodrich</i>	
Digital Signatures Do Not Guarantee Exclusive Ownership	138
<i>Thomas Pornin and Julien P. Stern</i>	
Thompson's Group and Public Key Cryptography	151
<i>Vladimir Shpilrain and Alexander Ushakov</i>	
Rainbow, a New Multivariable Polynomial Signature Scheme	164
<i>Jintai Ding and Dieter Schmidt</i>	
Badger – A Fast and Provably Secure MAC	176
<i>Martin Boesgaard, Thomas Christensen, and Erik Zenner</i>	
IDS False Alarm Reduction Using Continuous and Discontinuous Patterns	192
<i>Abdulrahman Alharby and Hideki Imai</i>	

Indexing Information for Data Forensics	206
<i>Michael T. Goodrich, Mikhail J. Atallah, and Roberto Tamassia</i>	
Model Generalization and Its Implications on Intrusion Detection	222
<i>Zhuowei Li, Amitabha Das, and Jianying Zhou</i>	
Intrusion-Resilient Secure Channels	238
<i>Gene Itkis, Robert McNeerney Jr., and Scott Russell</i>	
Optimal Asymmetric Encryption and Signature Paddings	254
<i>Benoît Chevallier-Mames, Duong Hieu Phan, and David Pointcheval</i>	
Efficient and Leakage-Resilient Authenticated Key Transport Protocol Based on RSA	269
<i>SeongHan Shin, Kazukuni Kobara, and Hideki Imai</i>	
Identity Based Encryption Without Redundancy	285
<i>Benoît Libert and Jean-Jacques Quisquater</i>	
OACerts: Oblivious Attribute Certificates	301
<i>Jiangtao Li and Ninghui Li</i>	
Dynamic k -Times Anonymous Authentication	318
<i>Lan Nguyen and Rei Safavi-Naini</i>	
Efficient Anonymous Roaming and Its Security Analysis	334
<i>Guomin Yang, Duncan S. Wong, and Xiaotie Deng</i>	
Quantifying Security in Hybrid Cellular Networks	350
<i>Markus Jakobsson and Liu Yang</i>	
Off-Line Karma: A Decentralized Currency for Peer-to-peer and Grid Applications	364
<i>Flavio D. Garcia and Jaap-Henk Hoepman</i>	
Building Reliable Mix Networks with Fair Exchange	378
<i>Michael K. Reiter, XiaoFeng Wang, and Matthew Wright</i>	
SCARE of the DES (Side Channel Analysis for Reverse Engineering of the Data Encryption Standard)	393
<i>Rémy Daudigny, Hervé Ledig, Frédéric Muller, and Frédéric Valette</i>	
Robust Key Extraction from Physical Uncloneable Functions	407
<i>B. Škorić, P. Tuyls, and W. Ophey</i>	
Efficient Constructions for One-Way Hash Chains	423
<i>Yih-Chun Hu, Markus Jakobsson, and Adrian Perrig</i>	
Privacy Preserving Keyword Searches on Remote Encrypted Data	442
<i>Yan-Cheng Chang and Michael Mitzenmacher</i>	

An Efficient Solution to the Millionaires' Problem Based on Homomorphic Encryption	456
<i>Hsiao-Ying Lin and Wen-Guey Tzeng</i>	
Non-interactive Zero-Knowledge Arguments for Voting	467
<i>Jens Groth</i>	
Short Signature and Universal Designated Verifier Signature Without Random Oracles	483
<i>Rui Zhang, Jun Furukawa, and Hideki Imai</i>	
Efficient Identity Based Ring Signature	499
<i>Sherman S.M. Chow, Siu-Ming Yiu, and Lucas C.K. Hui</i>	
New Signature Schemes with Coupons and Tight Reduction	513
<i>Benoît Chevallier-Mames</i>	
Author Index	529