

*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*

Alfred Kobsa

*University of California, Irvine, CA, 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*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Steven M. Bellovin   Rosario Gennaro  
Angelos Keromytis   Moti Yung (Eds.)

# Applied Cryptography and Network Security

6th International Conference, ACNS 2008  
New York, NY, USA, June 3-6, 2008  
Proceedings

## Volume Editors

Steven M. Bellovin  
Angelos Keromytis  
Columbia University  
1214 Amsterdam Avenue, New York, NY 10027, USA  
E-mail: {smb,angelos}@cs.columbia.edu

Rosario Gennaro  
IBM T.J.Watson Research Center  
19 Skyline Dr., Hawthorne, NY 10532, USA  
E-mail: rosario@us.ibm.com

Moti Yung  
Google Inc.  
and  
Columbia University, Department of Computer Science  
1214 Amsterdam Avenue, New York, NY 10027, USA  
E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2008927608

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 3-540-68913-3 Springer Berlin Heidelberg New York  
ISBN-13 978-3-540-68913-3 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 2008  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper SPIN: 12278923 06/3180 5 4 3 2 1 0

# Preface

ACNS 2008, the 6th International Conference on Applied Cryptography and Network Security, was held in New York, New York, June 3–6, 2008, at Columbia University. ACNS 2008 was organized in cooperation with the International Association for Cryptologic Research (IACR) and the Department of Computer Science at Columbia University. The General Chairs of the conference were Angelos Keromytis and Moti Yung.

The conference received 131 submissions, of which the Program Committee, chaired by Steven Bellovin and Rosario Gennaro, selected 30 for presentation at the conference. The Best Student Paper Award was given to Liang Xie and Hui Song for their paper “On the Effectiveness of Internal Patch Dissemination Against File-Sharing Worms” (co-authored with Sencun Zhu).

These proceedings consist of revised versions of the presented papers. The revisions were not reviewed. The authors bear full responsibility for the contents of their papers.

There were many submissions of good quality, and consequently the selection process was challenging and very competitive. Indeed, a number of good papers were not accepted due to lack of space in the program. The main considerations in selecting the program were conceptual and technical innovation and quality of presentation. As reflected in the Call for Papers, an attempt was made to solicit and publish papers suggesting novel paradigms, original directions, or non-traditional perspectives.

We would like to extend our heartfelt thanks to the Program Committee members, who dedicated so much time and effort to provide a thorough and in-depth review of the submissions, with high standards of professional integrity. We also thank the many external reviewers who assisted the Program Committee in its work. Most importantly, we thank the authors of submitted papers for their contributions; without these papers, after all, there would be no ACNS conference.

A special thanks is due to Shai Halevi for writing the software that greatly facilitated the committee work, and for his responsiveness in answering all our questions.

We are grateful to Jianying Zhou who, as Publicity Chair, relentlessly advertised the conference, to Angelika Zavou for her timely maintenance of the conference website and to Sophie Majewski for helping with the local arrangements.

Finally, we appreciate the assistance provided by the Springer LNCS editorial staff in assembling these proceedings.

June 2008

Steven Bellovin  
Rosario Gennaro  
Angelos Keromytis  
Moti Yung

# ACNS 2008

## 6th Annual Conference on Applied Cryptography and Network Security

Columbia University, New York, NY, USA  
June 3–6, 2008

### General Chairs

Angelos Keromytis, Columbia University  
Moti Yung, Google Inc.

### Program Chairs

Steven M. Bellovin, Columbia University  
Rosario Gennaro, IBM Research

### Program Committee

Masayuki Abe	NTT, Japan
Ben Adida	Harvard University, USA
Feng Bao	Institute for Infocomm Research, Singapore
Lujo Bauer	CMU, USA
Giampaolo Bella	University of Catania, Italy
Steven Bellovin	Columbia University, USA
John Black	University of Colorado, USA
Nikita Borisov	University of Illinois Urbana-Champaign, USA
Colin Boyd	Queensland University of Technology, Australia
Dario Catalano	University of Catania, Italy
Debra Cook	Alcatel-Lucent Bell Labs, USA
Alexander W. Dent	Royal Holloway, University of London, UK
Nelly Fazio	IBM Research, USA
Marc Fischlin	Darmstadt University of Technology, Germany
Debin Gao	Singapore Management University, Singapore
Rosario Gennaro	IBM Research, USA
Peter Gutmann	University of Auckland, New Zealand
John Ioannidis	Packet General Networks, USA
Stanislaw Jarecki	University of California Irvine, USA
Ari Juels	RSA Laboratories, USA
Kaoru Kurosawa	Ibaraki University, Japan
Yehuda Lindell	Bar-Ilan University, Israel

Moses Liskov	The College of William and Mary, USA
Javier Lopez	University of Malaga, Spain
Jelena Mirkovic	USC/ISI, USA
David Naccache	Ecole Normale Supérieure, France
Alina Oprea	RSA Laboratories, USA
Tom Shrimpton	Portland State University, USA
Jonathan Smith	University of Pennsylvania, USA
Angelos Stavrou	George Mason University, USA
Xiaoyun Wang	Shandong University, China
Nicholas Weaver	ICSI Berkeley, USA
Steve Weis	Google, USA
Tara Whalen	Dalhousie University, Canada
Michael Wiener	Cryptographic Clarity, Canada
Avishai Wool	Tel-Aviv University, Israel
Diego Zamboni	IBM Research, Switzerland
Jianying Zhou	Institute for Infocomm Research, Singapore

## External Reviewers

Cristina Alcaraz	Swee-Huay Heng	Chris Peikert
Joonsang Baek	Shoichi Hirose	Thomas Peyrin
Daniel Bailey	Huseyin Hisil	Bart Preneel
Mira Belenkyi	Christian Hoertnagl	Mario Di Raimondo
Vicente Benjumea	Susan Hohenberger	Vincent Rijmen
Kevin Bowers	Stefan Katzenbeisser	Rodrigo Roman
Christian Cachin	Gunes Kayacik	Alex Ross
Carlos Cid	Takeshi Koshihara	Jason Rouse
Mauro Conti	Anja Lehmann	Yu Sasaki
Nicolas Courtois	Andrew Lewis	Dominique Schroeder
Erik Dahmen	Francesco Librizzi	Matthias Schunter
Ehud Doron	Jennifer Lindsay	Elizabeth C. Schwartz
Maria Fernandez-Gago	Norka Lucena	Amir Shenhav
Dario Fiore	Ling Cheung	Nigel Smart
Keith Frikken	Jean Martina	Alessandro Sorniotti
Jun Furukawa	David Molnar	Natasa Terzija
David Galindo	Steven Murdoch	Yuuki Tokunaga
Deepak Garg	Pablo Najera	Eran Tromer
Scott Garriss	Aleksandra Nenadic	Duong Quang Viet
Carrie Gates	Antonio Nicolosi	Zhaohui Wang
Chris Giblin	Wakaha Ogata	Andreas Westfeld
David Goldenberg	Katsuyuki Okeya	Juerg Wullschlegler
Juan González	Dan Page	Yanjiang Yang
Choudary Gorantla	Pascal Paillier	Lei Zhang
Robbert de Haan	Kenneth G. Paterson	
Shai Halevi	Maura Paterson	

# Table of Contents

On the Effectiveness of Internal Patching Against File-Sharing Worms .....	1
<i>Liang Xie, Hui Song, and Suncun Zhu</i>	
Peeking Through the Cloud: DNS-Based Estimation and Its Applications.....	21
<i>Moheeb Abu Rajab, Fabian Monrose, Andreas Terzis, and Niels Provos</i>	
Pushback for Overlay Networks: Protecting Against Malicious Insiders .....	39
<i>Angelos Stavrou, Michael E. Locasto, and Angelos D. Keromytis</i>	
PPAA: Peer-to-Peer Anonymous Authentication .....	55
<i>Patrick P. Tsang and Sean W. Smith</i>	
Generic Constructions of Stateful Public Key Encryption and Their Applications.....	75
<i>Joonsang Baek, Jianying Zhou, and Feng Bao</i>	
Traceable and Retrievable Identity-Based Encryption .....	94
<i>Man Ho Au, Qiong Huang, Joseph K. Liu, Willy Susilo, Duncan S. Wong, and Guomin Yang</i>	
Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures .....	111
<i>Takashi Nishide, Kazuki Yoneyama, and Kazuo Ohta</i>	
Attacking Reduced Round SHA-256 .....	130
<i>Somitra Kumar Sanadhya and Palash Sarkar</i>	
DAKOTA – Hashing from a Combination of Modular Arithmetic and Symmetric Cryptography .....	144
<i>Ivan B. Damgård, Lars R. Knudsen, and Søren S. Thomsen</i>	
Getting the Best Out of Existing Hash Functions; or What if We Are Stuck with SHA? .....	156
<i>Yevgeniy Dodis and Prashant Puniya</i>	
Replay Attack in a Fair Exchange Protocol.....	174
<i>Macià Mut-Puigserver, Magdalena Payeras-Capellà, Josep Lluís Ferrer-Gomila, and Llorenç Huguet-Rotger</i>	
Improved Conditional E-Payments .....	188
<i>Marina Blanton</i>	

Anonymity in Transferable E-cash .....	207
<i>Sébastien Canard and Aline Gouget</i>	
Generic Security-Amplifying Methods of Ordinary Digital Signatures ...	224
<i>Jin Li, Kwangjo Kim, Fangguo Zhang, and Duncan S. Wong</i>	
New Differential-Algebraic Attacks and Reparametrization of Rainbow .....	242
<i>Jintai Ding, Bo-Yin Yang, Chia-Hsin Owen Chen, Ming-Shing Chen, and Chen-Mou Cheng</i>	
Trapdoor Sanitizable Signatures and Their Application to Content Protection .....	258
<i>Sébastien Canard, Fabien Laguillaumie, and Michel Milhau</i>	
Multi-factor Authenticated Key Exchange .....	277
<i>David Pointcheval and Sébastien Zimmer</i>	
Repelling Detour Attack Against Onions with Re-encryption .....	296
<i>Marek Klonowski, Mirosław Kutylowski, and Anna Lauks</i>	
Analysis of EAP-GPSK Authentication Protocol .....	309
<i>John C. Mitchell, Arnab Roy, Paul Rowe, and Andre Scedrov</i>	
Efficient Device Pairing Using “Human-Comparable” Synchronized Audiovisual Patterns .....	328
<i>Ramnath Prasad and Nitesh Saxena</i>	
PUF-HB: A Tamper-Resilient HB Based Authentication Protocol .....	346
<i>Ghaith Hammouri and Berk Sunar</i>	
An Authentication Scheme Based on the Twisted Conjugacy Problem .....	366
<i>Vladimir Shpilrain and Alexander Ushakov</i>	
Restricted Queries over an Encrypted Index with Applications to Regulatory Compliance .....	373
<i>Nikita Borisov and Soumyadeb Mitra</i>	
A Practical and Efficient Tree-List Structure for Public-Key Certificate Validation .....	392
<i>Tong-Lee Lim, A. Lakshminarayanan, and Vira Saksen</i>	
On the Security of the CCM Encryption Mode and of a Slight Variant .....	411
<i>Pierre-Alain Fouque, Gwenaëlle Martinet, Frédéric Valette, and Sébastien Zimmer</i>	
$wNAF^*$ , an Efficient Left-to-Right Signed Digit Recoding Algorithm ...	429
<i>Brian King</i>	



A Very Compact “Perfectly Masked” S-Box for AES .....	446
<i>D. Canright and Lejla Batina</i>	
Steel, Cast Iron and Concrete: Security Engineering for Real World Wireless Sensor Networks .....	460
<i>Frank Stajano, Dan Cvrcek, and Matt Lewis</i>	
Traceable Privacy of Recent Provably-Secure RFID Protocols.....	479
<i>Khaled Ouafi and Raphael C.-W. Phan</i>	
The Security of EPC Gen2 Compliant RFID Protocols.....	490
<i>Mike Burmester and Breno de Medeiros</i>	
<b>Author Index</b> .....	507