Lecture Notes in Computer Science 5037

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

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

Springer

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

Springer is a part of Springer Science+Business Media

springer.com

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

Table of Contents