Lecture Notes in Computer Science 5229

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

Rafail Ostrovsky Roberto De Prisco
Ivan Visconti (Eds.)

Security and Cryptography for Networks

6th International Conference, SCN 2008
Amalfi, Italy, September 10-12, 2008
Proceedings

Springer

Volume Editors

Rafail Ostrovsky
University of California, Los Angeles
Department of Computer Science
Box 951596, 3732D BH, Los Angeles, CA, 90095-1596, USA
E-mail: rafail@cs.ucla.edu

Roberto De Prisco
Università di Salerno
Dipartimento di Informatica ed Applicazioni
via Ponte don Melillo, 84084 Fisciano (SA), Italy
E-mail: robdep@dia.unisa.it

Ivan Visconti
Università di Salerno
Dipartimento di Informatica ed Applicazioni
via Ponte don Melillo, 84084 Fisciano (SA), Italy
E-mail: visconti@dia.unisa.it

Library of Congress Control Number: 2008933864

CR Subject Classification (1998): E.3, C.2, D.4.6, K.4.1, K.4.4, K.6.5, F.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-85854-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-85854-6 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12512393 06/3180 5 4 3 2 1 0

Preface

The 6th Conference on Security and Cryptography for Networks (SCN 2008) was held in Amalfi, Italy, on September 10–12, 2008. The first four editions of the conference where held in Amalfi, while, two years ago, the fifth edition was held in the nearby Maiori. This year we moved back to the traditional location.

Security and privacy are increasing concerns in computer networks such as the Internet. The availability of fast, reliable, and cheap electronic communication offers the opportunity to perform, electronically and in a distributed way, a wide range of transactions of a most diverse nature. The conference brought together researchers in the fields of cryptography and security in communication networks with the goal of fostering cooperation and exchange of ideas. The main topics of the conference this year included anonymity, implementations, authentication, symmetric-key cryptography, complexity-based cryptography, privacy, cryptanalysis, cryptographic protocols, digital signatures, public-key cryptography, hash functions, identification.

The international Program Committee consisted of 24 members who are top experts in the conference fields. The PC received 71 submissions and selected 26 papers for presentation at the conference. These proceedings include the 26 accepted papers and the abstract of the invited talk by Shai Halevi.

The PC selected papers on the basis of originality, quality and relevance to the conference scope. Due to the high number of submissions, paper selection was a difficult task and many good papers had to be rejected. Each paper was refereed by three or four reviewers. We thank the members of the PC for the effort invested in the selection process. We also gratefully acknowledge the help of the external reviewers who evaluated submissions in their area of expertise. The names of these reviewers are listed on page VIII, and we apologize for any inadvertent omissions or mistakes.

Finally, we would like to thank the authors of all submitted papers and the conference participants, who ultimately made this conference possible.

September 2008

R. Ostrovsky
R. De Prisco
I. Visconti

SCN 2008

September 10–12, 2008, Amalfi, Italy

Program Chair

Rafail Ostrovsky	University of California, Los Angeles, USA

General Chairs

Roberto De Prisco	Università di Salerno, Italy
Ivan Visconti	Università di Salerno, Italy

Program Committee

Carlo Blundo	Università di Salerno, Italy
Xavier Boyen	Voltage Inc, USA
Ran Canetti	IBM, USA
Dario Catalano	Università di Catania, Italy
Ronald Cramer	CWI & Leiden University, The Netherlands
Serge Fehr	CWI, The Netherlands
Juan Garay	Bell Labs - Alcatel-Lucent, USA
Rosario Gennaro	IBM, USA
Jens Groth	University College London, UK
Yuval Ishai	Technion and UCLA, Israel and USA
Jonathan Katz	University of Maryland, USA
Eyal Kushilevitz	Technion, Israel
Ueli Maurer	ETH Zurich, Switzerland
Daniele Micciancio	UCSD, USA
Phong Nguyen	ENS, France
Tatsuaki Okamoto	NTT Laboratories, Japan
Rafail Ostrovsky (chair)	UCLA, USA
Giuseppe Persiano	Università di Salerno, Italy
Benny Pinkas	University of Haifa, Israel
Tal Rabin	IBM, USA
Leonid Reyzin	Boston University, USA
Adi Rosen	CNRS and University of Paris 11, France
Adam Smith	Pennsylvania State University, USA
Ivan Visconti	Università di Salerno, Italy

Referees

Divesh Aggarwal
Zuzana Beerliova
Charles Bouillaguet
Suresh Chari
Debbie Cook
Cécile Delerablée
Mario Di Raimondo
Orr Dunkelman
Dario Fiore
Sebastian Gajek
David Galindo
Peter Gaži
Craig Gentry
Sharon Goldberg
Amir Herzberg
Alejandro Hevia
Dennis Hofheinz
Susan Hohenberger
Emeline Hufschmitt
Charanjit Jutla
Bhavana Kanukurthi
Aggelos Kiayias
Eike Kiltz
Vladimir Kolesnikov
Gaëtan Leurent
Anna Lysyanskaya
Vadim Lyubashevsky
Alexander May
Lorenz Minder
David Molnar
Christopher Portmann
Emmanuel Prouff
Dominik Raub
Mike Rosulek
Amit Sahai
Christian Schaffner
Nigel Smart
Stefano Tessaro
Carmine Ventre
Enav Weinreb
Daniel Wichs
Vassilis Zikas
Cliff Changchun Zou

Table of Contents

Session 5: Primitives

Session 6: Signatures

Session 7: Hardware and Cryptanalysis

Session 8: Protocols II

Session 9: Encryption III

Session 10: Key Exchange