Lecture Notes in Computer Science 3352

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

Editorial Board

Carlo Blundo Stelvio Cimato (Eds.)

Security in Communication Networks

4th International Conference, SCN 2004
Amalfi, Italy, September 8-10, 2004
Revised Selected Papers

Springer

Volume Editors

Carlo Blundo
Stelvio Cimato
Università degli Studi di Salerno, Dipartimento di Informatica ed Applicazioni
84081 Baronissi (SA), Italy
E-mail: {carblu, cimato}@dia.unisa.it

Library of Congress Control Number: 2004117660

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

ISSN 0302-9743
ISBN 3-540-24301-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11375937 06/3142 5 4 3 2 1 0

Preface

The 4th International Conference on Security in Communication Networks 2004 (SCN 2004) was held at the "Diocese Hall" of the Archdiocese of Amalfi-Cava de' Tirreni and the "Armorial Bearings Hall" of the Archbishop Palace in Amalfi, Italy, on September 8–10, 2004. Previous conferences also took place in Amalfi in 1996, 1999 and 2002.

The conference aimed at bringing together researchers in the fields of cryptography and security in communication networks to foster cooperation and the exchange of ideas.

The main topics included all technical aspects of data security, including: anonymity, authentication, block ciphers, complexity-based cryptography, cryptanalysis, digital signatures, distributed cryptography, hash functions, identification, implementations, key distribution, privacy, public key encryption, threshold cryptography, and zero knowledge.

The Program Committee, consisting of 21 members, considered 79 papers and selected 26 for presentation; one of them was withdrawn by the authors. These papers were selected on the basis of originality, quality and relevance to cryptography and security in communication networks.

Due to the high number of submissions, paper selection was a difficult and challenging task, and many good submissions had to be rejected. Each submission was refereed by at least three reviewers and some had four reports or more. We are very grateful to all the program committee members, who devoted much effort and valuable time to read and select the papers. In addition, we gratefully acknowledge the help of colleagues who reviewed submissions in their areas of expertise. They are all listed on page VII and we apologize for any inadvertent omissions.

These proceedings include the revised versions of the 26 accepted papers and the abstract of the invited talk by Bart Preneel (*ECRYPT: the Cryptographic Research Challenges for the Next Decade*).

Following the example of the previous editions of SCN, we encouraged authors to submit their contributions in electronic format. We handled the submissions with CyberChair (http://www.CyberChair.org) a free Web-based paper submission and reviewing system.

Finally, we would like to thank all the authors who submitted their papers for making this conference possible, the Program Committee members, as well as all the conference participants.

September 2004

C. Blundo
S. Cimato

SCN 2004
September 8–10 2004, Amalfi, Italy

Program Chair

Carlo Blundo	Università di Salerno, Italy

General Chair

Stelvio Cimato	Università di Salerno, Italy

Program Committee

Giuseppe Ateniese	Johns Hopkins University, USA
Carlo Blundo	Università di Salerno, Italy (Chair)
Christian Cachin	IBM Research, Switzerland
Ran Canetti	IBM Research, USA
Xiaotie Deng	City University, Hong Kong, China
Alfredo De Santis	Università di Salerno, Italy
Yvo Desmedt	University College London, UK
Giovanni Di Crescenzo	Telcordia Technology, USA
Rosario Gennaro	IBM Research, USA
Eyal Kushilevitz	Technion, Israel
Tanja Lange	University of Bochum, Germany
Ueli Maurer	ETH Zurich, Switzerland
Eiji Okamoto	Tsukuba University, Japan
Rafail Ostrovsky	UCLA, USA
Giuseppe Persiano	Università di Salerno, Italy
Leonid Reyzin	Boston University, USA
Rei Safavi-Naini	University of Wollongong, Australia
Jacques Stern	ENS, France
Doug Stinson	University of Waterloo, Canada
Gene Tsudik	UCI, USA
Moti Yung	Columbia University, USA

Local Organizing Committee

Paolo D'Arco	Università di Salerno, Italy
Barbara Masucci	Università di Salerno, Italy

Sponsoring Institutions

Dipartimento di Informatica ed Applicazioni, Università di Salerno, Italy
Lanfredi Fund, France

Referees

Michel Abdalla
Joonsang Baek
Amos Beimel
Jan Camenisch
Claude Castelluccia
Dario Catalano
Xi Chen
Qi Cheng
Hung Chim
Stelvio Cimato
Paolo D'Arco
Breno de Medeiros
Xuhua Ding
Pierre-Alain Fouque
Clemente Galdi
Louis Granboulan
Matthew Green
Daniel Hamburg
Jason Hinek
Seny Kamara
Aggelos Kiayias
Hugo Krawczyk
TieYan Li
Becky Liu
John Malone-Lee
Barbara Masucci
Lan Nguyen
Phong Nguyen
David Pointcheval
David Safford
Willy Susilo
Nicolas Tadeusz Courtois
Ivan Visconti
Duncan Wong
Shouhuai Xu
Jianhong Zhang
Huafei Zhu

Table of Contents

Authentication and Identification

Zero Knowledge

Public Key Cryptosystems

Distributed Cryptography

Cryptanalysis of Public Key Cryptosystems

Cryptanalysis

Email Security

Key Distribution and Feedback Shift Registers