Lecture Notes in Computer Science 2576
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

Stelvio Cimato
Clemente Galdi
Giuseppe Persiano (Eds.)

Security in Communication Networks

Third International Conference, SCN 2002
Amalfi, Italy, September 11-13, 2002
Revised Papers

Springer

Volume Editors

Stelvio Cimato
Giuseppe Persiano
Università di Salerno
Dipartimento di Informatica ed Applicazioni
Via S. Allende, 84081 Baronissi (SA), Italy
E-mail: {cimato/giuper}@dia.unisa.it

Clemente Galdi
Computer Technology Institute and
University of Patras
Dept. of Computer Engineering and Informatics
26500 Rio, Greece
E-mail: clegal@ceid.upatras.gr

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

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 3-540-00420-3 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 10872336 06/3142 5 4 3 2 1 0

Preface

The Third International Conference on Security in Communication Networks 2002 (SCN 2002) was held in the Salone Morelli of the Civic Museum of Amalfi, Italy, September 11–13, 2002. The conference takes place every three years (previous ones were held in 1996 and 1999 in Amalfi too) and aims to bring together researchers in the field of security in communication networks to foster cooperation and the exchange of ideas.

The main topics included all technical aspects of data security including: anonymity implementation, authentication, key distribution, block ciphers, operating systems security, complexity-based cryptography, privacy, cryptanalysis, protocols, digital signatures, public key encryption, electronic money, public key infrastructure, hash functions, secret sharing, identification, surveys, and the state of the art.

The program committee received 90 submissions in electronic format from 5 continents of which 24 were selected for presentation in 8 sessions. We had two invited talks, one by Eyal Kushilevitz from the Technion, Israel on "Some Applications of Polynomials for the Design of Cryptographic Protocols," and the other by Ueli Maurer from ETH, Zurich, on "Secure Multi-Party Computation Made Simple."

Due to the high number of submissions, the reviewing phase was a very challenging process, and many good submissions had to be rejected. We are very grateful to all the program committee members, assisted by their colleagues, who devoted much effort and valuable time to read and select the papers.

We want to thank the Municipality of Amalfi that agreed to host the conference in one of the most beautiful halls in Amalfi. Finally, we would like to thank all the authors who submitted their papers, the Program Committee members, and all the conference participants.

September 2002

S. Cimato
C. Galdi
G. Persiano

Organization

SCN 2002 was organized with the financial support of the Dipartimento di Informatica ed Applicazioni "R.M. Capocelli" and the Facoltà di Scienze Matematiche, Fisiche e Naturali of the Università di Salerno under the auspices of the Amalfi Municipality.

Program Chair

Giuseppe Persiano	Università di Salerno, Italy

General Chair

Carlo Blundo	Università di Salerno, Italy

Program Committee

Giuseppe Ateniese	(Johns Hopkins University, USA)
Carlo Blundo	(Università di Salerno, Italy)
Christian Cachin	(IBM Research, Switzerland)
Giovanni Di Crescenzo	(Telcordia Technologies, USA)
Alfredo De Santis	(Università di Salerno, Italy)
Rafail Ostrovsky	(Telcordia Technologies, USA)
Giuseppe Persiano	(Università di Salerno, Italy)
Jacques Stern	(École Normale Supérieure, France)
Doug Stinson	(University of Waterloo, Canada)
Gene Tsudik	(University of California at Irvine, USA)
Moti Yung	(Columbia University, USA)

Organizing Committee

Stelvio Cimato	Università di Salerno, Italy
Paolo D'Arco	Università di Salerno, Italy
Clemente Galdi	Università di Salerno, Italy
Barbara Masucci	Università di Salerno, Italy

Publicity Chairs

Vincenzo Auletta	Università di Salerno, Italy
Domenico Parente	Università di Salerno, Italy

Table of Contents

Invited Talks

Forward Security

Foundations of Cryptography

Key Management

Cryptanalysis

System Security

Signature Schemes

Zero Knowledge

Information Theory and Secret Sharing