Lecture Notes in Computer Science 11035

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

Editorial Board

More information about this series at http://www.springer.com/series/7410

Dario Catalano · Roberto De Prisco (Eds.)

Security and Cryptography for Networks

11th International Conference, SCN 2018 Amalfi, Italy, September 5–7, 2018 Proceedings

Springer

Editors
Dario Catalano
University of Catania
Catania
Italy

Roberto De Prisco
University of Salerno
Fisciano
Italy

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-98112-3 ISBN 978-3-319-98113-0 (eBook)
https://doi.org/10.1007/978-3-319-98113-0

Library of Congress Control Number: 2018950389

LNCS Sublibrary: SL4 – Security and Cryptology

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 11th Conference on Security and Cryptography for Networks (SCN 2018) was held in Amalfi, Italy, during September 5–7, 2018. The conference has traditionally been held in Amalfi, with the exception of the fifth edition, held in the nearby Maiori. After the editions of 1996, 1999 and 2002, it has been organized biannually thereafter.

In the digital era, communications crucially rely on computer networks. These allow both easy and fast access to information. At the same time, guaranteeing the security of modern communications is a delicate and challenging task. The SCN conference is an international meeting whose focus is on the cryptographic and information security methodologies needed to address such challenges. SCN allows researchers, practitioners, developers, and users interested in the security of communication networks to meet and exchange ideas in the wonderful scenario of the Amalfi Coast.

These proceedings contain the 30 papers that were selected by the Program Committee (PC). The conference received 66 submissions. Each submission was assigned to at least three reviewers, while submissions co-authored by PC members received, at least, four reviews. After an initial individual review phase, the submissions were discussed for a period of three additional weeks. During the discussion phase the PC used rather intensively a, recently introduced, feature of the review system, which allows PC members to anonymously ask questions directly to authors. The reviewing and selection procedure was a challenging and difficult task. We are deeply grateful to the PC members and external reviewers for the hard and careful work they did. Special thanks to Tancrède Lepoint, Giuseppe Persiano, and Antigoni Polychroniadou for their extra work as shepherds. Many thanks also to Michel Abdalla for his constant availability and for sharing with us his experience as former SCN Program Chair.

The conference program also included invited talks by Huijia Lin (University of California Santa Barbara, USA) and Eike Kiltz (Ruhr-University Bochum, Germany). We would like to thank both of them as well as all the other speakers for their contribution to the conference.

SCN 2018 was organized in cooperation with the International Association for Cryptologic Research (IACR). The paper submission, review, and discussion processes were effectively and efficiently made possible by the IACR Web-Submission-and-Review software, written by Shai Halevi. Many thanks to Shai for setting up the system for us and for his assistance and constant availability.

We thank all the authors who submitted papers to this conference, the Organizing Committee members, colleagues, and student helpers for their valuable time and effort, and all the conference attendees who made this event truly intellectually stimulating through their active participation.

September 2018

Dario Catalano
Roberto De Prisco

SCN 2018

The 11th Conference on Security and Cryptography for Networks

Amalfi, Italy
September 5–7, 2018

Program Chair

Dario Catalano	Università di Catania, Italy

General Chair

Roberto De Prisco	Università di Salerno, Italy

Organizing Committee

Carlo Blundo	Università di Salerno, Italy
Aniello Castiglione	Università di Salerno, Italy
Luigi Catuogno	Università di Salerno, Italy
Paolo D'Arco	Università di Salerno, Italy

Steering Committee

Alfredo De Santis	Università di Salerno, Italy
Ueli Maurer	ETH Zürich, Switzerland
Rafail Ostrovsky	University of California, Los Angeles, USA
Giuseppe Persiano	Università di Salerno, Italy
Jacques Stern	ENS, France
Douglas Stinson	University of Waterloo, Canada
Gene Tsudik	University of California, Irvine, USA
Moti Yung	Snapchat and Columbia University, USA

Program Committee

Elena Andreeva	KU Leuven, Belgium
Manuel Barbosa	INESC TEC and FC Univers. do Porto, Portugal
Carlo Blundo	Università di Salerno, Italy
Jean-Sébastien Coron	University of Luxembourg
Mario Di Raimondo	Università di Catania, Italy
Léo Ducas	CWI, Amsterdam, The Netherlands
Marc Fischlin	Darmstadt University of Technology, Germany
Pierre-Alain Fouque	University of Rennes, France

Georg Fuchsbauer	Inria and ENS, Paris, France
Romain Gay	ENS Paris, France
Carmit Hazay	Bar-Ilan University, Israel
Tancrède Lepoint	SRI International, USA
Gaëtan Leurent	Inria, France
Benoît Libert	CNRS and ENS de Lyon, France
Daniel Masny	UC Berkeley, USA
Svetla Nikova	KU Leuven, Belgium
Ryo Nishimaki	NTT, Japan
Luca Nizzardo	IMDEA Software Institute, Madrid, Spain
Emmanuela Orsini	University of Bristol, UK
Giuseppe Persiano	Università di Salerno, Italy
Thomas Peyrin	Nanyang Technological University, Singapore
Krzysztof Pietrzak	IST, Austria
Antigoni Polychroniadou	Cornell University, USA
Dominique Schröder	Friedrich-Alexander-Universität, Erlangen, Germany
Alessandra Scafuro	North Carolina State University, USA
Martijn Stam	University of Bristol, UK
Damien Stehlé	ENS de Lyon, France
Mehdi Tibouchi	NTT, Japan
Daniele Venturi	Università di Roma, La Sapienza, Italy
Damien Vergnaud	Sorbonne University and Institut Universitaire de France, Paris, France
Vanessa Vitse	Institut Fourier, University of Grenoble Alpes, France
Bogdan Warinschi	University of Bristol, UK

Additional Reviewers

Aysajan Abidin
Hamza Abusalah
José Bacelar Almeida
Miguel Ambrona
Nuttapong Attrapadung
Balthazar Bauer
Carsten Baum
Pauline Bert
Carl Bootland
Olivier Bronchain
Jie Chen
Ilaria Chillotti
Michele Ciampi
Aisling Connolly
Jan Czajkowski
Nico Doettling
Thomas Espitau
Antonio Faonio
David Galindo-Chacón
Ran Gelles
Irene Giacomelli
Junqing Gong
Alonso Gonzalez
Antoine Joux
Karen Klein
Ilan Komargodski
Russell W. F. Lai
Kwangsu Lee
Eleftheria Makri
Giulio Malavolta
Chanathip Namprempre
Maria Naya-Plasencia

Khoa Nguyen
Ariel Nof
Cristina Onete
Alain Passelègue
Alice Pellet–Mary
Olivier Pereira
Rafael Del Pino
Bernardo Portela
Chen Qian
Razvan Rosie
Edouard Dufour Sans
John Schank
Thomas Shrimpton
Luisa Siniscalchi
Christoph Striecks
Junichi Tomida
Ni Trieu
Ida Tucker
Furkan Turan
Yohei Watanabe
Tim Wood
Takashi Yamakawa
Avishay Yanai
Ren Zhang

IACR

This event was organized in cooperation with the International Association for Cryptologic Research (IACR).

Sponsors

InfoCert, GRUPPO TECNOINVESTIMENTI, Rome, Italy

Contents

Multiparty Computation

Anonymity and Zero Knowledge

Secret Sharing and Oblivious Transfer

Lattices and Post Quantum Cryptography