Lecture Notes in Computer Science 7485

Ivan Visconti Roberto De Prisco (Eds.)

Security and Cryptography for Networks

8th International Conference, SCN 2012
Amalfi, Italy, September 5-7, 2012
Proceedings

Springer

Volume Editors

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

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-32927-2 e-ISBN 978-3-642-32928-9
DOI 10.1007/978-3-642-32928-9
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012945012

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2.0, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The 8th Conference on Security and Cryptography for Networks (SCN 2012) was held in Amalfi, Italy, during September 5–7, 2012. This biennial conference has traditionally been held in Amalfi, with the exception of the fifth edition which was held in nearby Maiori.

The world-wide use of computer networks, and in particular of the Internet, opens new challenges for the security of electronic and distributed transactions. Cryptography and information security must face both the theoretical and practical aspects of the above challenges, by providing concepts, techniques, applications, and practical experiences. The principal aim of SCN as a conference is to bring together researchers, practitioners, developers, and users interested in the above fields, to foster cooperation and to exchange techniques, tools, experiences, and ideas in the stunning Amalfi Coast setting.

The conference received 72 submissions in a broad range of cryptography and security areas. The selection of papers was a difficult task. This year we received many high-quality submissions and 31 of them were accepted for publication in these proceedings on the basis of quality, originality, and relevance to the conference's scope.

At least three Program Committee (PC) members—out of 28 world-renowned experts in the conference's various areas of interest—reviewed each submitted paper, while submissions co-authored by a PC member were subjected to the more stringent evaluation of five PC members.

In addition to the PC members, many external reviewers joined the review process in their particular areas of expertise. We were fortunate to have this knowledgeable and energetic team of experts, and are deeply grateful to all of them for their hard and thorough work, which included a very active discussion phase—almost as long as the initial individual reviewing period. The paper submission, review, and discussion processes were effectively and efficiently made possible by the Web-Submission-and-Review software, written by Shai Halevi, and hosted by the International Association for Cryptologic Research (IACR). Many thanks to Shai for his assistance with the system's various features and for his constant availability.

Given the perceived quality of the submissions, the PC decided also this year to give a Best-Paper Award, both to promote outstanding work in the fields of cryptography and information security and to keep encouraging high-quality submissions to SCN. "Deterministic Public Key Encryption and Identity-Based Encryption from Lattices in the Auxiliary-Input Setting" by Xiang Xie, Rue Xue, and Rui Zhang was conferred such distinction.

The program was further enriched by the invited talks of Yuval Ishai (Technion, Israel) and Giuseppe Persiano (Università di Salerno, Italy), top experts on the subjects of the conference.

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 a truly intellectually stimulating one through their active participation.

We finally thank the *Dipartimento di Informatica* of the University of Salerno, Italy, for the financial support.

September 2012

Ivan Visconti
Roberto De Prisco

SCN 2012
The 8th Conference on Security and Cryptography for Networks

September 5–7, 2012, Amalfi, Italy

Program Chair

Ivan Visconti	Università di Salerno, Italy

Program Committee

Masayuki Abe	NTT, Japan
Amos Beimel	Ben-Gurion University, Israel
Carlo Blundo	Università di Salerno, Italy
Alexandra Boldyreva	Georgia Institute of Technology, USA
Xavier Boyen	PARC, USA
Dario Catalano	University of Catania, Italy
Melissa Chase	Microsoft Research Redmond, USA
Dana Dachman-Soled	Microsoft Research New England, USA
Stefan Dziembowski	University of Warsaw, Poland and Sapienza University of Rome, Italy
Pierre-Alain Fouque	ENS, France
Juan Garay	AT&T Labs-Research, USA
Vipul Goyal	Microsoft Research, India
Brett Hemenway	University of Michigan, USA
Martin Hirt	ETH Zurich, Switzerland
Dennis Hofheinz	Karlsruhe Institute of Technology, Germany
Stanislaw Jarecki	UCI, USA
Gregory Neven	IBM Research, Switzerland
Carles Padro	Nanyang Technological University, Singapore
Benny Pinkas	Bar Ilan University, Israel, and Google, USA
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Matt Robshaw	Orange Labs, France
Alon Rosen	IDC Herzliya, Israel
abhi shelat	University of Virginia, USA
Francois-Xavier Standaert	UCL, Belgium
Dominique Unruh	University of Tartu, Estonia
Bogdan Warinschi	University of Bristol, UK
Daniel Wichs	IBM T.J. Watson Research Center, USA
Moti Yung	Google, USA and Columbia University, USA

General Chair

Roberto De Prisco	Università di Salerno, Italy

Organizing Committee

Aniello Castiglione	Università di Salerno, Italy
Paolo D'Arco	Università di Salerno, Italy

Steering Committee

Carlo Blundo	Università di Salerno, Italy
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 Paris, France
Douglas Stinson	University of Waterloo, Canada
Gene Tsudik	University of California - Irvine, USA
Moti Yung	Google, USA and Columbia University, USA

External Reviewers

Shweta Agrawal
Giulia Alberini
Joël Alwen
Gilad Asharov
Abhishek Banerjee
Steven Bellovin
Charles Bouillaguet
David Cash
Iwen Coisel
Sandro Coretti
Reza Curtmola
Gregory Demay
Patrick Derbez
Mario Di Raimondo
Laila El Aimani
Oriol Farràs
Dario Fiore
Atsushi Fujioka
Clemente Galdi
Chaya Ganesh
Peter Gaži
Clint Givens
Dov Gordon
Divya Gupta
Tibor Jager
Jeremy Jean
Tomasz Kazana
François Koeune
Stephan Krenn
Huijia Lin
Steve Lu
Christoph Lucas
Benjamin Martin
Christian Matt
Irippuge Milinda Perera
Miyako Ohkubo
Ilan Orlov
Chris Peikert
Vanishree Rao
Mariana Raykova
Elizabeth Quaglia
Alessandra Scafuro
Hakan Seyalioglu
Adam Smith
Adam Stubblefield
Björn Tackmann
Yevgeniy Vahlis
Jorge L. Villar
Keita Xagawa
Vassilis Zikas
Yunlei Zhao
Hong-Sheng Zhou

Table of Contents

Cryptography from Lattices

Signature Schemes

Encryption Schemes I

Efficient Two-Party and Multi-Party Computation

Security in the UC Framework

Cryptanalysis

Encryption Schemes II

Efficient Constructions

Protocols and Combiners