Lecture Notes in Computer Science **10052**

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

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

Sara Foresti · Giuseppe Persiano (Eds.)

Cryptology and Network Security

15th International Conference, CANS 2016 Milan, Italy, November 14–16, 2016 Proceedings

Springer

Editors
Sara Foresti
Università degli Studi di Milano
Crema
Italy

Giuseppe Persiano
Università degli Studi di Salerno
Fisciano
Italy

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-48964-3 ISBN 978-3-319-48965-0 (eBook)
DOI 10.1007/978-3-319-48965-0

Library of Congress Control Number: 2016955512

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

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

Preface

These proceedings contain the papers selected for presentation at the 15th International Conference on Cryptology and Network Security (CANS 2016), held in Milan, Italy, on November 14–16, 2016. The conference was held in cooperation with the International Association of Cryptologic Research and focuses on technical aspects of cryptology and of data, network, and computer security. These proceedings contain 30 full papers (with an acceptance rate of 25.86 %) and 18 short papers selected by the Program Committee from 116 submissions. The proceedings also contain an extended abstract for the 8 posters presented at the conference.

The many high-quality submissions made it easy to build a strong program but also required rejecting good papers. Each submission was judged by at least three reviewers and the whole selection process included about six weeks of reading and discussion in the Program Committee.

The credit for the success of an event like CANS 2016 belongs to a number of people, who devoted their time and energy to put together the conference and who deserve acknowledgment. There is a long list of people who volunteered their time and energy to organize the conference, and who deserve special thanks. We would like to thank all the members of the Program Committee and all the external reviewers, for all their hard work in evaluating all the papers during the summer. We are grateful to CANS Steering Committee for their support. Thanks to Giovanni Livraga, for taking care of publicity and chairing local organization. We are very grateful to the local organizers for their support in the conference organization and logistics. We would like to thank the keynote speakers for accepting our invitation to deliver a talk at the conference.

Special thanks are due to the Università degli Studi di Milano for its support and for hosting the event, and to the Italian Association for Information Processing (AICA) for support in the secretarial and registration process.

Last but certainly not least, our thanks go to all the authors who submitted papers and posters and to all the conference's attendees. We hope you find the program of CANS 2016 interesting, stimulating, and inspiring for your future research.

November 2016

Sara Foresti
Pino Persiano
Pierangela Samarati

Organization

General Chair

Pierangela Samarati	Università degli Studi di Milano, Italy

Program Chairs

Sara Foresti	Università degli Studi di Milano, Italy
Giuseppe Persiano	Università degli Studi di Salerno, Italy

Poster Chairs

Sara Foresti	Università degli Studi di Milano, Italy
Giuseppe Persiano	Università degli Studi di Salerno, Italy
Pierangela Samarati	Università degli Studi di Milano, Italy

Publicity Chair

Giovanni Livraga	Università degli Studi di Milano, Italy

Local Arrangements Chair

Giovanni Livraga	Università degli Studi di Milano, Italy

Steering Committee

Yvo Desmedt (Chair)	The University of Texas at Dallas, USA
Juan A. Garay	Yahoo! Labs, USA
Amir Herzberg	Bar Ilan University, Israel
Yi Mu	University of Wollongong, Australia
David Pointcheval	CNRS and ENS Paris, France
Huaxiong Wang	Nanyang Technological University, Singapore

Program Committee

Lejla Batina	Radboud University, The Netherlands
Carlo Blundo	Università degli Studi di Salerno, Italy
Henry Carter	Villanova University, USA
Nishanth Chandran	Microsoft Research, India
Yingying Chen	Stevens Institute of Technology, USA

Sherman S.M. Chow	Chinese University of Hong Kong, Hong Kong
Ricardo Dahab	IC-UNICAMP, Brazil
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Angelo De Caro	IBM Research, Zurich, Switzerland
Yvo Desmedt	The University of Texas at Dallas, USA
Nelly Fazio	City University of New York, USA
Georg Fuchsbauer	Ecole Normale Supérieure, France
Rosario Gennaro	City University of New York, USA
Amir Herzberg	Bar Ilan University, Israel
Vincenzo Iovino	University of Luxembourg, Luxembourg
Rob Johnson	Stony Brook University, USA
Florian Kerschbaum	SAP, Germany
Aggelos Kiayias	University of Athens, Greece
Albert Levi	Sabanci University, Turkey
Ming Li	University of Arizona, USA
Dongdai Lin	Chinese Academy of Sciences, China
Peng Liu	The Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
Steve Lu	Stealth Software Technologies Inc., USA
Atsuko Miyaji	Osaka University/JAIST, Japan
Evagelos Markatos	University of Crete, Greece
Refik Molva	Eurecom, France
Yi Mu	University of Wollongong, Australia
Gregory Neven	IBM Research, Zurich, Switzerland
Antonio Nicolosi	Stevens Institute of Technology, USA
Svetla Nikova	KU Leuven, Belgium
Emmanuela Orsini	University of Bristol, UK
Panos Papadimitratos	KTH, Stockholm, Sweden
Stefano Paraboschi	Università di Bergamo, Italy
Gerardo Pelosi	Politecnico di Milano, Italy
Benny Pinkas	Bar Ilan University, Israel
Pierangela Samarati	Università degli Studi di Milano, Italy
Nitesh Saxena	University of Alabama at Birmingham, USA
Andreas Schaad	Huawei Research, Germany
Dominique Schroeder	Saarland University, Germany
Peter Schwabe	Radboud University, The Netherlands
Willy Susilo	University of Wollongong, Australia
Katsuyuki Takashima	Mitsubishi Electric, Japan
Qiang Tang	University of Luxembourg, Luxembourg
Meng Yu	University of Texas at San Antonio, USA
Huaxiong Wang	Nanyang Technological University, Singapore

External Reviewers

Hamza Abusalah
Zakir Akram
Duygu Karaoğlan Altop
S. Abhishek Anand
Diego Aranha
Tomer Ashur
Seiko Arita
Arash Atashpendar
Pol Van Aubel
Monir Azraoui
Saikrishna Badrinarayanan
Amos Beimel
Daniel Bernau
Jonas Boehler
Carl Bootland
Raphael Bost
Christina Boura
Florian Bourse
Alexandre Braga
Luigi Catuogno
Rongmao Chen
Michele Ciampi
Guo Chun
Mario Cornejo
Joan Daemen
Christophe Doche
Kaoutar Elkhiyaoui
Keita Emura
Martianus Frederic Ezerman
Nils Fleischhacker
Atsushi Fujioka
Yuichi Futa
Marios Georgiou
Esha Ghosh
Rishab Goyal
Le Guan
Xue Haiyang
Jin Han
Wenhui Hu
Yupeng Jiang
Süleyman Kardaş
Aniket Kate
Akinori Kawachi
Anselme Kemgne Tueno
Mathias Kohler
Anna Krasnova
Ashutosh Kumar
Jianchang Lai
Russell W.F. Lai
Obbattu Sai Lakshmi Bhavana
Hyung Tae Lee
Iraklis Leontiadis
Hemi Leibowitz
Bin Liu
Meicheng Liu
Naiwei Liu
Yunwen Liu
Zhen Liu
Jose M. Lopez
Isis Lovecruft
Atul Luykx
Chang Lv
Jack P.K. Ma
Mohammad Mamun
Pedro Maat Massolino
Peihan Miao
Christoph Michel
Shigeo Mitsunari
Eduardo Morais
Toru Nakanishi
Luiz Navarro
Ajaya Neupane
Khoa Nguyen
Hod Bin Noon
Maciej Obremski
Kazumasa Omote
Adam O'Neill
Melek Önen
Stjepan Picek
Fabio Piva
Elizabeth Quaglia
Srinivasan Raghuraman
Manuel Reinert
Oscar Reparaz
Vincent Rijmen
Ruben Rios
Adeline Roux-Langlois
Vipin Singh Sehrawat
Sruthi Sekar
Babins Shrestha
Maliheh Shirvanian
Roee Shlomo
Prakash Shrestha
Luisa Siniscalchi
William Skeith
Maciej Skórski
Akshayaram Srinivasan
Raymond K.H. Tai
Sri Aravinda Krishnan Thyagarajan
Chenyang Tu
Miguel Urquidi
Cédric Van Rompay
Dimitrios Vasilopoulos
Gabriele Viglianisi
Xiao Wang
Xiuhua Wang
Yongge Wang
Harry W.H. Wong
Brecht Wyseur
Tran Phuong Viet Xuan
Bohan Yang
Eunjung Yoon
Libo Zhang
Miaomiao Zhang
Shiwei Zhang
Tao Zhang
Yongjun Zhao
Jingyuan Zhao
Jincheng Zhuang

Contents

Virtual Private Network

Signatures and Hash

MultiParty Computation

Symmetric Cryptography and Authentication

Malware and Attacks

MultiParty Computation and Functional Encryption

Network Security, Privacy, and Authentication

Posters