Alastair R. Beresford
Arpita Patra
Emanuele Bellini (Eds.)

LNCS 13641

Cryptology and Network Security

21st International Conference, CANS 2022
Dubai, United Arab Emirates, November 13–16, 2022
Proceedings

Springer

Lecture Notes in Computer Science 13641

More information about this series at https://link.springer.com/bookseries/558

Alastair R. Beresford · Arpita Patra ·
Emanuele Bellini (Eds.)

Cryptology and Network Security

21st International Conference, CANS 2022
Dubai, United Arab Emirates, November 13–16, 2022
Proceedings

Springer

Editors
Alastair R. Beresford
University of Cambridge
Cambridge, UK

Emanuele Bellini
Cryptography Research Center
Technology Innovation Institute
Abu Dhabi, United Arab Emirates

Arpita Patra
Indian Institute of Science
Bangalore, India

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-20973-4 ISBN 978-3-031-20974-1 (eBook)
https://doi.org/10.1007/978-3-031-20974-1

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 21st International Conference on Cryptology and Network Security (CANS 2022) was held in Abu Dhabi during November 13–16, 2022.

CANS is an established annual conference presenting novel research work on cryptology, computer and network security, data security and privacy. Previous editions of CANS were held in Taipei (2001), San Francisco (2002), Miami (2003), Xiamen (2005), Suzhou (2006), Singapore (2007), Hong Kong (2008), Kanazawa (2009), Kuala Lumpur (2010), Sanya (2011), Darmstadt (2012), Parary (2013), Crete (2014), Marrakesh (2015), Milan (2016), Hong Kong (2017), Naples (2018), Fuzhou (2019) and virtually due to COVID-19 (2020, 2021).

In 2022 we received 54 submissions, out of which 18 full papers and two short papers were accepted for publication. We used a double-blind review process with three reviews per submission. The Program Committee chairs handled conflicts and used written reviews as well as online discussion with the reviewers to select the papers included in these proceedings. All authors were given the opportunity to revise their papers in response to reviewer feedback; a few papers were assigned a member of the Program Committee as a shepherd to support this process.

We would like to thank the Technology Innovation Institute (TII) for their support during the planning and running of the conference as well as Springer for their assistance in the production of the proceedings. We are extremely grateful to all the authors of the submitted papers as well as the 45 Program Committee members and 23 external reviewers for their care and dedication. Finally, we would like to thank the steering committee and organizing committee for their support and encouragement.

September 2022

Alastair R. Beresford
Arpita Patra
Emanuele Bellini

Organization

General Chair

Emanuele Bellini	Technology Innovation Institute, UAE

Program Committee Chairs

Alastair R. Beresford	University of Cambridge, UK
Arpita Patra	Indian Institute of Science Bangalore, India

Steering Committee

Yvo G. Desmedt (Chair)	University of Texas at Dallas, USA
Juan A. Garay	Texas A&M University, USA
Yi Mu	Fujian Normal University, China
Panos Papadimitratos	KTH Royal Institute of Technology, Sweden
David Pointcheval	CNRS and ENS Paris, France
Huaxiong Wang	Nanyang Technological University, Singapore

Organizing Committee

Emanuele Bellini	Technology Innovation Institute, UAE
Ana Castillo	Technology Innovation Institute, UAE

Program Committee

Cristina Alcaraz	University of Malaga, Spain
Subhadeep Banik	École Polytechnique Fédérale de Lausanne (EPFL), Switzerland
Emanuele Bellini	Technology Innovation Institute, UAE
Arka Rai Choudhury	University of California, Berkeley, USA
Sherman Chow	Chinese University of Hong Kong, Hong Kong
Sandro Coretti-Drayton	Input Output Hong Kong (IOHK), Switzerland
Bernardo David	IT University of Copenhagen (ITU), Denmark
F. Betül Durak	Microsoft Research, USA
Pooya Farshim	Durham University, UK
Chaya Ganesh	Indian Institute of Science Bangalore, India
Satrajit Ghosh	IIT Kharagpur, India

Ariel Hamlin	MIT Lincoln Laboratory, USA
Panagiotis Ilia	University of Illinois, USA
Tetsu Iwata	Nagoya University, Japan
Ashwin Jha	CISPA Helmholtz Center for Information Security, Germany
Martin Kleppmann	University of Cambridge, UK
Ivan Martionvic	University of Oxford, UK
René Mayrhofer	Johannes Kepler University Linz, Austria
Veelasha Moonsamy	Ruhr University Bochum, Germany
Mridul Nandi	Indian Statistical Institute, India
Guevara Noubir	Northeastern University, USA
Emmanuela Orsini	Katholieke Universiteit (KU) Leuven, Belgium
Sergio Pastrana	Universidad Carlos III de Madrid, Spain
Sikhar Patranabis	IBM Research India, India
Constantinos Patsakis	University of Piraeus, Greece
Somitra Sanadhya	IIT Jodhpur, India
Dominique Schroder	University of Erlangen-Nuremberg, Germany
Mridula Singh	CISPA Helmholtz Center for Information Security, Germany
Alberto Sonnino	Mysten Labs, UK
Angelo Spognardi	Sapienza Università di Roma, Italy
Christoph Striecks	AIT Austrian Institute of Technology, Austria
Ajith Suresh	Technische Universität Darmstadt, Germany
Willy Susilo	University of Wollongong, Australia
Daniel Tschudi	Concordium, Switzerland
Giorgos Vasiliadis	FORTH and Hellenic Mediterranean University, Greece
Damien Vergnaud	LIP6, Sorbonne Université, France
João Vilela	University of Porto, Portugal
Corrado Aaron Visaggio	University of Sannio, Italy
Isabel Wagner	De Montfort University, UK
Huaxiong Wang	Nanyang Technological University, Singapore
Edgar Weippl	University of Vienna, Austria
Xingliang Yuan	Monash University, Australia
Zhenfei Zhang	Ethereum Foundation, USA

Additional Reviewers

Navid Alamati
Khashayar Barooti
Suvradip Chakraborty
Gwangbae Choi
Daniel Collins
Mariana Cunha
Avijit Dutta
Loïs Huguenin-Dumittan
Amit Jana
Matthias J. Kannwischer

Shangqi Lai
Benjamin Lipp
Omid Mir
Munkenyi Mukhandi
Rahul Rachuri
Gerald Schoiber
Karl Southern

Erkan Tairi
Serge Vaudenay
Dabao Wang
Harry W. H. Wong
Bang Wu
Huangting Wu

Contents

Zero-Knowledge and MPC

Public-Key Infrastructure

Attacks and Countermeasures

Cryptanalysis and Provable Security

Cryptographic Protocols

Blockchain and Payment Systems

Codes and Post-quantum Cryptography