LNCS 13269

Giuseppe Ateniese
Daniele Venturi (Eds.)

Applied Cryptography and Network Security

20th International Conference, ACNS 2022
Rome, Italy, June 20–23, 2022
Proceedings

Springer

Lecture Notes in Computer Science 13269

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

Giuseppe Ateniese · Daniele Venturi (Eds.)

Applied Cryptography and Network Security

20th International Conference, ACNS 2022
Rome, Italy, June 20–23, 2022
Proceedings

Springer

Editors

Giuseppe Ateniese
Stevens Institute of Technology
Hoboken, NJ, USA

Daniele Venturi
Sapienza University of Rome
Rome, Italy

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-09233-6 ISBN 978-3-031-09234-3 (eBook)
https://doi.org/10.1007/978-3-031-09234-3

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

Preface

We are pleased to present the proceedings of the 20th International Conference on Applied Cryptography and Network Security (ACNS 2022). ACNS 2022 was held in Rome, Italy. Due to the ongoing COVID-19 crisis, we decided to have a hybrid conference to face any health risks or travel restrictions for attending the conference. The organization was in the capable hands of Mauro Conti (University of Padua, Italy) and Angelo Spognardi (Sapienza University of Rome, Italy) as general co-chairs, and Massimo Bernaschi (National Research Council, IAC-CNR, Italy) and Fabio De Gaspari (Sapienza University of Rome, Italy) as local organizing chairs. We are deeply indebted to them for their tireless work to ensure the success of the conference even in such complex conditions.

For the third time, ACNS had two rounds of submission cycles, with deadlines in September 2021 and January 2022, respectively. We received a total of 185 submissions from authors in 37 countries. This year's Program Committee (PC) consisted of around 150 members with diverse backgrounds and broad research interests. The review process was double-blind and rigorous, and papers were evaluated on the basis of research significance, novelty, and technical quality. In total, 691 reviews were submitted, with four reviews for most papers. Some papers submitted in the first round received a decision of major revision. The revised versions of those papers were further evaluated in the second round and some of them were accepted. After the review process concluded, a total of 44 papers were accepted to be presented at the conference and included in the proceedings, representing an acceptance rate of around 24%.

Among those papers, we awarded the Best Student Paper Award to Narmeen Shafqat (Northeastern University, Boston, MA, USA) for the paper "ZLeaks: Passive Inference Attacks on Zigbee based Smart Homes" (co-authored with Daniel J. Dubois, David Choffnes, Aaron Schulman, Dinesh Bharadia, and Aanjhan Ranganathan). The monetary prize of 1,000 euro was generously sponsored by Springer.

We had a rich program including eight satellite workshops in parallel with the main event, providing a forum to address specific topics at the forefront of cybersecurity research. The papers presented at those workshops were published in separate proceedings.

This year we had two outstanding keynote talks: "Chosen Ciphertext Security from Injective Trapdoor Functions" by Prof. Susan Hohenberger Waters (Johns Hopkins University, USA), and "Secure Computation in Practice" by Prof. Raluca Ada Popa (University of California, Berkeley, USA). To them, our heartfelt gratitude for their outstanding presentations.

The conference was made possible by the untiring efforts of many individuals and organizations. We are grateful to all the authors for their submissions. We sincerely appreciate the outstanding work of all the PC members and the external reviewers, who selected the papers after reading, commenting, and debating them. Finally, we thank all the people who volunteered their time and energy to put together the conference, the speakers and session chairs, and everyone who contributed to the success of the conference. We are also grateful to Riccardo Lazzeretti (Sapienza University of Rome, Italy) for taking care of these proceedings. Last, but certainly not least, we are very grateful to Frontiers for sponsoring the conference, Easychair for the management of the submissions, and Springer for their help in assembling these proceedings.

June 2022

Daniele Venturi
Giuseppe Ateniese

Organization

General Chairs

Mauro Conti	University of Padua, Italy
Angelo Spognardi	Sapienza University of Rome, Italy

Program Chairs

Giuseppe Ateniese	Stevens Institute of Technology, USA
Daniele Venturi	Sapienza University of Rome, Italy

Workshop Chair

Jianying Zhou	Singapore University of Technology and Design, Singapore

Poster Chair

Emiliano Casalicchio	Sapienza University of Rome, Italy

Local Organization Chairs

Massimo Bernaschi	National Council of Research, Italy
Fabio De Gaspari	Sapienza University of Rome, Italy

Publicity Chair

Alessandro Brighente	University of Padua, Italy

Publication Chair

Riccardo Lazzeretti	Sapienza University of Rome, Italy

Web Chair

Alicia K. Bidi	Sapienza University of Rome, Italy

Program Committee

Masayuki Abe	NTT, Japan
Mitsuaki Akiyama	NTT, Japan
Cristina Alcaraz	University of Malaga, Spain
Giuseppe Ateniese	George Mason University, USA
Xiaolong Bai	Alibaba Group, China
Lejla Batina	Radboud University, The Netherlands
Carsten Baum	Aarhus University, Denmark
Estuardo Bock	Aalto University, Finland
Matteo Campanelli	Protocol Labs, Denmark
Ignacio Cascudo	IMDEA Software Institute, Spain
Sang Kil Cha	Korea Advanced Institute of Science and Technology, South Korea
Sudipta Chattopadhyay	Singapore University of Technology and Design, Singapore
Sherman S. M. Chow	Chinese University of Hong Kong, Hong Kong
Michele Ciampi	University of Edinburgh, UK
Mauro Conti	University of Padua, Italy
Sandro Coretti	IOHK, Switzerland
Marc Dacier	Qatar Computing Research Institute, Qatar
Roberto Di Pietro	Hamad Bin Khalifa University, Qatar
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Nico Döttling	Aarhus University, Denmark
Antonio Faonio	EURECOM, France
Prastudy Fauzi	Simula UiB, Norway
Tommaso Gagliardoni	Kudelski Security, Switzerland
Chaya Ganesh	Aarhus University, Denmark
Debin Gao	Singapore Management University, Singapore
Paolo Gasti	New York Institute of Technology, USA
Esha Ghosh	Microsoft, USA
Yong Guan	Iowa State University, USA
Susan Hohenberger	Johns Hopkins University, USA
Hsu-Chun Hsiao	National Taiwan University, China
Hongxin Hu	University at Buffalo, SUNY, USA
Xinyi Huang	Fujian Normal University, China
Sotiris Ioannidis	Technical University of Crete, Greece
Hai Jin	Huazhong University of Science and Technology, China
Stefan Katzenbeisser	University of Passau, Germany
Kwok Yan Lam	Nanyang Technological University, Singapore
Peeter Laud	Cybernetica AS, Estonia
Xiapu Luo	Hong Kong Polytechnic University, Hong Kong

Bernardo Magri	Aarhus University, Denmark
Mark Manulis	Universität der Bundeswehr München, Germany
Giorgia Azzurra Marson	NEC Labs Europe, Germany
Daniel Masny	Meta, USA
Christian Matt	Concordium, Switzerland
Vashek Matyas	Masaryk University, Czech Republic
Veelasha Moonsamy	Ruhr University Bochum, Germany
Pratyay Mukherjee	Hedera Hashgraph/Swirlds, USA
David Naccache	ENS, France
Ariel Nof	Technion, Israel
Sabine Oechsner	University of Edinburgh, UK
Cristina Onete	Université de Limoges, France
Gerardo Pelosi	Politecnico di Milano, Italy
Giuseppe Persiano	Università degli Studi di Salerno, Italy
Thomas Peters	Université catholique de Louvain, Belgium
Josef Pieprzyk	CSIRO/Data61, Australia
Bertram Poettering	IBM Research - Zurich, Switzerland
Divya Ravi	Aarhus University, Denmark
Reihaneh Safavi-Naini	University of Calgary, Canada
Nitesh Saxena	Texas A&M University, USA
Janno Siim	University of Tartu, Finland
Mark Simkin	Ethereum Foundation
Angelo Spognardi	Sapienza Università di Roma, Italy
Purui Su	Institute of Software, CAS, China
Qiang Tang	University of Sydney, Australia
Mehdi Tibouchi	NTT, Japan
Daniel Tschudi	Concordium, Switzerland
Yiannis Tselekounis	University of Edinburgh
Daniele Venturi	Sapienza University of Rome, Italy
Ivan Visconti	University of Salerno, Italy
Cong Wang	City University of Hong Kong, Hong Kong
Zhaoyan Xu	Palo Alto Networks, USA
Chao Zhang	Tsinghua University, China
Fan Zhang	Zhejiang University, China
Kehuan Zhang	Chinese University of Hong Kong, Hong Kong
Yinqian Zhang	Southern University of Science and Technology, China
Hong-Sheng Zhou	Virginia Commonwealth University, USA
Jianying Zhou	Singapore University of Technology and Design, Singapore
Yajin Zhou	Zhejiang University, China

Contents

Encryption

Attacks

Cryptographic Protocols

System Security

Cryptographic Primitives

MPC

Blockchain

Block-Cyphers

Post-quantum Cryptography