Lecture Notes in Computer Science 13783

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

Lejla Batina · Stjepan Picek ·
Mainack Mondal (Eds.)

Security, Privacy, and Applied Cryptography Engineering

12th International Conference, SPACE 2022
Jaipur, India, December 9–12, 2022
Proceedings

Springer

Editors
Lejla Batina
Radboud University
Nijmegen, The Netherlands

Stjepan Picek
Radboud University
Nijmegen, The Netherlands

Mainack Mondal
Indian Institute of Technology Kharagpur
Kharagpur, India

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-22828-5 ISBN 978-3-031-22829-2 (eBook)
https://doi.org/10.1007/978-3-031-22829-2

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 12th International Conference on Security, Privacy, and Applied Cryptography Engineering 2022 (SPACE 2022), was held during December 9–12, 2022. This annual event is devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering. This is a challenging field, requiring expertise from diverse domains, ranging from mathematics and computer science to circuit design. The event was hosted by the Center for Cryptography, Cyber Security and Digital Forensics (C3-SDF) at The LNM Institute of Information Technology, Jaipur, India.

This year we received 61 submissions from authors in many different countries, mainly from Asia and Europe. The submissions were evaluated based on their significance, novelty, technical quality, and relevance to the SPACE conference. The submissions were reviewed in a double-blind mode by at least two members of the Program Committee, which consisted of 47 members from all over the world. After an extensive review process, 18 papers were accepted for presentation at the conference, leading to an acceptance rate of 29.5%.

The program also included five keynotes and four tutorials on various aspects of applied cryptology, security, and privacy delivered by world-renowned researchers: Ingrid Verbauwhede, Nele Mentens, Jeyavijayan "JV" Rajendran, Chester Rebeiro, Sanjay K. Jha, Łukasz Chmielewski, Sikhar Patranabis, Nitin Singh, and Matthias Kannwischer. We sincerely thank the invited speakers for accepting our invitations in spite of their busy schedules. As in previous editions, SPACE 2022 was organized in cooperation with the International Association for Cryptologic Research (IACR). We are grateful to general chairs Jayaprakash Kar and Debdeep Mukhopadhyay for their willingness to host it physically at LMNIT Jaipur.

There is a long list of volunteers who invested their time and energy to put together the conference. We are grateful to all the members of the Program Committee and their sub-reviewers for all their hard work in the evaluation of the submitted papers. We thank our publisher Springer for agreeing to continue to publish the SPACE proceedings as a volume in the Lecture Notes in Computer Science (LNCS) series. We are grateful to the local Organizing Committee who invested a lot of time and effort in order for the conference to run smoothly.

Last, but not least, our sincere thanks go to all the authors who submitted papers to SPACE 2022 and everyone who participated (either in person or virtually).

December 2022

Lejla Batina
Stjepan Picek
Mainack Mondal

Organization

General Chairs

Jayaprakash Kar	The LNM Institute of Information Technology, India
Debdeep Mukhopadhyay	Indian Institute of Technology, Kharagpur, India

Program Committee Chairs

Lejla Batina	Radboud University, The Netherlands
Mainack Mondal	Indian Institute of Technology, Kharagpur, India
Stjepan Picek	Radboud University, The Netherlands

Program Committee

Amr Youssef	Concordia University, Canada
Anupam Chattopadhyay	Nanyang Technological University, Singapore
Bodhisatwa Mazumdar	Indian Institute of Technology, Indore, India
Bohan Yang	Tsinghua University, China
Chester Rebeiro	Indian Institute of Technology, Madras, India
Chitchanok Chuengsatiansup	University of Adelaide, Australia
Claude Carlet	University of Bergen, Norway and University of Paris 8, France
Dirmanto Jap	Nanyang Technological University, Singapore
Domenic Forte	University of Florida, USA
Eran Toch	Tel Aviv University, Israel
Fan Zhang	Zhejiang University, China
Guilherme Perin	Radboud University, The Netherlands
Ileana Buhan	Radboud University, The Netherlands
Jakub Breier	Silicon Austria Labs, Austria
Jayaprakash Kar	The LNM Institute of Information Technology, India
Jean-Luc Danger	Télécom Paris, France
Kazuo Sakiyama	University of Electro-Communications, Japan
Kerstin Lemke-Rust	Bonn-Rhein-Sieg University of Applied Sciences, Germany
Kostas Papagiannopoulos	University of Amsterdam, The Netherlands
Luca Mariot	Radboud University, The Netherlands
Lukasz Chmielewski	Radboud University, The Netherlands

Maël Gay	University of Stuttgart, Germany
Marc Stoettinger	RheinMain University of Applied Science, Germany
Marc Manzano	Sandbox@Alphabet, Spain
Marine Minier	Université de Lorraine and Loria, France
Martin Henze	Fraunhofer FKIE, Germany
Md Masoom Rabbani	KU Leuven, Belgium
Nadia El Mrabet	EMSE, France
Nalla Anandakumar Nachimuthu	University of Florida, USA
Naofumi Homma	Tohoku University, Japan
Nele Mentens	Leiden University, The Netherlands
Olga Gadyatskaya	Leiden University, The Netherlands
Peter Schwabe	MPI-SP, Germany, and Radboud University, The Netherlands
Rahul Chatterjee	University of Wisconsin-Madison, USA
Rajat Subhra Chakraborty	Indian Institute of Technology, Kharagpur, India
Rajesh Pillai	DRDO, India
Ruben Niederhagen	University of Southern Denmark, Denmark
Sébastien Canard	Orange Labs, France
Shivam Bhasin	Nanyang Technological University, Singapore
Sikhar Patranabis	IBM Research, India
Silvia Mella	Radboud University, The Netherlands
Sk Subidh Ali	Indian Institute of Technology, Bhilai, India
Somitra Sanadhya	Indian Institute of Technology, Jodhpur, India
Soumyajit Dey	Indian Institute of Technology, Kharagpur, India
Sujoy Sinha Roy	TU Graz, Germany
Urbi Chatterjee	Indian Institute of Technology, Kanpur, India
Vishal Saraswat	Bosch Engineering and Business Solutions, Bengaluru, India

Additional Reviewers

Martin Serror	Fraunhofer FKIE, Germany
Wenping Zhu	Tsinghua University, China
Soumyadyuti Ghosh	Indian Institute of Technology, Kharagpur, India
Rajat Sadhukhan	Indian Institute of Technology, Kharagpur, India
Durba Chatterjee	Indian Institute of Technology, Kharagpur, India

Contents

Symmetric Cryptography

Public-Key Cryptography, Post-quantum Cryptography, Zero Knowledge Proofs

Hardware Security and AI

Network Security, Authentication, and Privacy