Lecture Notes in Computer Science 12484

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

Joaquin Garcia-Alfaro · Guillermo Navarro-Arribas ·
Jordi Herrera-Joancomarti (Eds.)

Data Privacy Management, Cryptocurrencies and Blockchain Technology

ESORICS 2020 International Workshops, DPM 2020 and CBT 2020
Guildford, UK, September 17–18, 2020
Revised Selected Papers

Springer

Editors
Joaquin Garcia-Alfaro
Télécom SudParis
Evry Cedex, France

Jordi Herrera-Joancomarti
Escola d'Enginyeria
Universitat Autònoma de Barcelona
Cerdanyola del Vallès, Barcelona, Spain

Guillermo Navarro-Arribas
Departament d'Enginyeria de la Informació i de les Comunicacions
Universitat Autonoma de Barcelona
Bellaterra, Spain

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-66171-7 ISBN 978-3-030-66172-4 (eBook)
https://doi.org/10.1007/978-3-030-66172-4

LNCS Sublibrary: SL4 – Security and Cryptology

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

Foreword from the DPM 2020 Program Chairs

This volume contains the post-proceedings of the 15th Data Privacy Managmeent International Workshop (DPM 2020), which was organized within the 25th European Symposium on Research in Computer Security (ESORICS 2020). The DPM series started in 2005 when the first workshop took place in Tokyo, Japan. Since then, the event has been held in different venues: Atlanta, USA (2006); Istanbul, Turkey (2007); Saint-Malo, France (2009); Athens, Greece (2010); Leuven, Belgium (2011); Pisa, Italy (2012); Egham, UK (2013); Wrocław, Poland (2014); Vienna, Austria (2015); Crete, Greece (2016); Oslo, Norway (2017); Barcelona, Spain (2018); and Luxembourg (2019).

This 2020 edition was intended to be held in the University of Surrey, UK, but was finally held virtually due to the COVID-19 pandemic together with the ESORICS main conference and all its workshops.

We received 38 submissions. The Program Committee performed excellent work and all submissions went through a careful review process. Each paper was evaluated on the basis of significance, novelty, and technical quality. After reviewing the submissions, 12 full papers and 5 short papers were accepted for presentation at the event and further publication in these post-proceedings.

We would like to thank everyone who helped in organizing the event, including all the members of the Organizing Committee of both ESORICS and DPM 2020. Our gratitude goes to Mark Manulis, the workshop chair of ESORICS 2020, and to the ESORICS 2020 general chair, Steve Schneider. During the event, we had the valued assistance and help from Kent Leeding. Thanks also go to Sergi Delgado, CEO of Talaia Labs, Spain, and Marc Juarez, from the University of Southern California, USA, for accepting our invitation to conduct the invited talks. Last, but by no means least, we thank all the DPM 2020 Program Committee members, additional reviewers, all the authors who submitted papers, and all the workshop attendees.

Finally, we want to acknowledge the support received from the sponsors of the workshop: Institut Mines-Telecom and Institut Polytechnique de Paris (Télécom SudParis), France, Universitat Autònoma de Barcelona, Spain, UNESCO Chair in Data Privacy, Cybercat, and projects TIN2017-87211-R and SECURITAS RED2018-102321-T from the Spanish Government.

November 2020

Joaquin Garcia-Alfaro
Guillermo Navarro-Arribas

DPM 2020 Organization

PC Chairs

Joaquin Garcia-Alfaro	Intitut Polytechnique de Paris, France
Guillermo Navarro-Arribas	Universitat Autònoma de Barcelona, Spain

Program Committee

Jordi Casas-Roma	Universitat Oberta de Catalunya, Spain
Jordi Castellà-Roca	Universitat Rovira i Virgili, Spain
Mauro Conti	University of Padua, Italy
Jorge Cuellar	University of Passau, Germany
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Jose Maria de Fuentes	Universidad Carlos III de Madrid, Spain
Roberto Di Pietro	Hamad Bin Khalifa University, Qatar
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Sara Foresti	Università degli Studi di Milano, Italy
Sebastien Gambs	Université du Québec à Montréal, Canada
Javier Herranz	Universitat Politècnica de Catalunya, Spain
Jordi Herrera-Joancomartí	Universitat Autònoma de Barcelona, Spain
Marc Juarez	University of Southern California, USA
Christos Kalloniatis	University of the Aegean, Greece
Florian Kammueller	Middlesex University London, UK, and TU Berlin, Germany
Sokratis Katsikas	Open University of Cyprus, Cyprus
Hiroaki Kikuchi	Meiji University, Japan
Evangelos Kranakis	Carleton University, Canada
Alptekin Küpçü	Koç University, Turkey
Costas Lambrinoudakis	University of Piraeus, Greece
Maryline Laurent	Institut Mines-Télécom, France
Giovanni Livraga	University of Milan, Italy
Brad Malin	Vanderbilt University, USA
Chris Mitchell	Royal Holloway, University of London, UK
Anna Monreale	University of Pisa, Italy
Jordi Nin	ESADE, Universitat Ramon Llull, Spain
Martín Ochoa	AppGate Inc., USA
Melek Önen	EURECOM, France
Gerardo Pelosi	Politecnico di Milano, Italy
Silvio Ranise	Fondazione Bruno Kessler, Italy
Kai Rannenberg	Goethe University Frankfurt, Germany
Ruben Rios	University of Malaga, Spain

Yves Roudier	University of Nice Sophia Antipolis, France
Pierangela Samarati	Università degli Studi di Milano, Italy
David Sanchez	University Rovira i Virgili, Spain
Qiang Tang	Luxembourg Institute of Science and Technology, Luxembourg
Yasuyuki Tsukada	Kanto Gakuin University, Japan
Alexandre Viejo	Universitat Rovira i Virgili, Spain
Isabel Wagner	De Montfort University, UK
Jens Weber	University of Victoria, Canada
Nicola Zannone	Eindhoven University of Technology, The Netherlands

Steering Committee

Joaquin Garcia-Alfaro	Intitut Polytechnique de Paris, France
Guillermo Navarro-Arribas	Universitat Autònoma de Barcelona, Spain
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Vicenç Torra	Umeå University, Sweden

Additional Reviewers

Tahir Ahmad	Salimeh Dashti
Stefano Berlato	Angeliki Kitsiou
Osman Biçer	Katerina Mavroeidi
Matteo Cardaioli	Luca Pajola
Marco Casagrande	Argyri Pattakou

Foreword from the CBT 2020 Program Chairs

The 4th International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2020) was held in collaboration with the 25th European Symposium on Research in Computer Security (ESORICS 2020) and the 15th International Workshop on Data Privacy Management (DPM 2020). Due to the COVID-19 outbreak, the event was held virtually.

We wish to thank all of the authors who submitted their work. This year, CBT received 24 submissions, out of which, 8 papers were accepted for presentation as full papers, complemented by 4 short papers, 2 invited talks, and a discussion panel. The review process was conducted virtually, involving a rigorous process conducted by the Technical Program Committee (TPC) chairs, all the members of the TPC, and the help of some external reviewers.

The CBT 2020 program was organized in three sessions grouping the contributions into the following topics: Transactions, Mining, Second Layer, Signature Schemes, Formal Methods, Privacy, SNARKs, and Anonymity. The sessions were chaired by members of the TCP, and authors and attendees engaged in exciting discussions on new frontiers in the field of cryptocurrencies and blockchain technology.

We would like to thank all of the people involved in CBT 2020. We are grateful to the TPC members and the external reviewers for their help in providing detailed and timely reviews of the submissions; to Sergi Delgado, CEO of Talaia Labs, Spain, and Marc Juarez, from the University of Southern California, USA, for accepting our invitation to conduct two keynotes, and for their presence during the event and talks; to Shin'ichiro Matsuo (Georgetown University, USA), Pindar Wong (VeriFi Ltd., Hong Kong), Nat Sakimura (OpenID Foundation), Julien Bringer (Convenor of ISO TC307/WG2), Patrick McCorry (PISA Research), and Florian Kammueller (Middlesex University London, UK, and TU Berlin, Germany) for accepting our invitation to conduct a discussion panel on "How cryptocurrency and blockchain technology will become a trust foundation for the New Normal while ensuring data privacy management?" We also thank all the members of the Surrey team, especially to Steve Schneider, Mark Manulis, Kent Leeding, and Mohammed Alsadi, for all their help and support. Thanks also go to Springer for their great support throughout the entire process.

Finally, the organization was made possible through the strong help of our supporters: Institut Mines-Télécom and Institut Polytechnique de Paris, SAMOVAR, France, Universitat Autonoma de Barcelona, Spain, Cybercat, BART (Inria, IRT SYSTEMX, Télécom SudParis, and Télécom Paris, France). A special thank you to all of them. Last, but by no means least, we thank all the authors who submitted papers and talks, and all the workshop attendees.

November 2020

Joaquin Garcia-Alfaro
Jordi Herrera-Joancomartí

CBT 2020 Organization

Program Committee Chairs

Joaquin Garcia-Alfaro	Intitut Polytechnique de Paris, France
Jordi Herrera-Joancomart	Universitat Autònoma de Barcelona, Spain

Program Committee

Daniel Augot	Inria Saclay, France
Alex Biryukov	University of Luxembourg, Luxembourg
Rainer Böhme	Universität Innsbruck, Austria
Joseph Bonneau	New York University, USA
Alexander Chepurnoy	IOHK Research, Russia
Mauro Conti	University of Padua, Italy
Vanesa Daza	Universitat Pompeu Fabra, Spain
Sergi Delgado-Segura	Talaia Labs, Spain
Arthur Gervais	Imperial College London, UK
Hannes Hartenstein	Karlsruhe Institute of Technology, Germany
Ghassan Karame	NEC Research, Germany
Eleftherios Kokoris-Kogias	Novi, Switzerland
Shin'ichiro Matsuo	Georgetown University, USA
Andrew Miller	University of Illinois at Urbana-Champaign, USA
Pedro Moreno-Sanchez	IMDEA, Spain
Guillermo Navarro	Universitat Autònoma de Barcelona, Spain
Cristina Pérez-Solà	Universitat Oberta de Catalunya, Spain
Matteo Signorini	Nokia Bell Labs France, France
Khalifa Toumi	IRT SystemX, France

Steering Committee

Rainer Böhme	Universität Innsbruck, Austria
Joaquin Garcia-Alfaro	Intitut Polytechnique de Paris, France
Hannes Hartenstein	Karlsruher Institut für Technologie, Germany
Jordi Herrera-Joancomart	Universitat Autònoma de Barcelona, Spain

Additional Reviewers

Florian Jacob
Sébastien Andreina
Rahul Saha
Ankit Gangwal
Arantxa Zapico
Oliver Stengele
Federico Franzoni
Daniel Feher
Gulshan Kumar
Alexei Zamyatin
Matthias Grundmann
Abhimanyu Rawat

Contents