Lecture Notes in Computer Science 11598

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

Ian Goldberg · Tyler Moore (Eds.)

Financial Cryptography and Data Security

23rd International Conference, FC 2019
Frigate Bay, St. Kitts and Nevis, February 18–22, 2019
Revised Selected Papers

Springer

Editors
Ian Goldberg
Cheriton School of Computer Science
University of Waterloo
Waterloo, ON, Canada

Tyler Moore
Tandy School of Computer Science
University of Tulsa
Tulsa, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-32100-0 ISBN 978-3-030-32101-7 (eBook)
https://doi.org/10.1007/978-3-030-32101-7

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

Preface

FC 2019, the 23rd International Conference on Financial Cryptography and Data Security, was held February 18–22, 2019, at the St. Kitts Marriott Resort in Frigate Bay, St. Kitts and Nevis.

We received 178 paper submissions. Of these, 32 full papers and seven short papers were accepted, corresponding to a 21.9% acceptance rate. Revised papers appear in these proceedings.

The surge in interest in cryptocurrencies heralded by Bitcoin has been reflected in the composition of the program at FC for several years. Since 2014, a dedicated workshop, the Workshop on Bitcoin and Blockchain Research (BITCOIN), has been held in conjunction with FC. Given the quality and quantity of research appearing in this workshop, the International Financial Cryptography Association (IFCA) Steering Committee, in consultation with current and past program chairs of FC and the BITCOIN workshop, decided to integrate the BITCOIN workshop into the main FC conference as a new blockchain track.

This decision resulted in a high-quality and balanced program, with 20 papers in the new blockchain track and 19 papers in the non-blockchain track. The two tracks were held on alternating days: The blockchain track was Monday and Wednesday, and the non-blockchain track was Tuesday and Thursday. By not holding the tracks in parallel, all FC attendees could enjoy the entirety of the program. Neha Narula, Director of the MIT Digital Currency Initiative, gave an inspiring keynote entitled “Preventing Catastrophic Cryptocurrency Attacks.” Her talk highlighted some pressing and unique challenges of responsibly managing vulnerabilities affecting cryptocurrencies.

Overall, the program successfully realized the goal of creating a unified venue for blockchain papers, while keeping room for other topics that have long been part of FC. Feedback at the conference about the change was overwhelmingly positive. Therefore, we anticipate that this arrangement will continue in future editions of the conference.

We are grateful for the contributions of the 72 members of the Program Committee. Submissions had at least three reviews, or four in the case of a submission by a Program Committee member. An extensive online discussion phase was utilized to guide decisions. The Program Committee members provided thoughtful and constructive feedback to authors, which considerably strengthened the quality of the final papers appearing in this volume. Of the 39 accepted papers, 14 were shepherded by Program Committee members. We are especially thankful to the shepherds for their additional contributions. We also appreciate the reviews contributed by 59 external reviewers.

We would like to thank Rafael Hirschfeld for his unrivaled and continued dedication to FC, including his role serving as conference general chair. We also thank the IFCA directors and Steering Committee for their service.

Finally, we would like to thank the sponsors of the conference for their generous support: Research Institute, Blockstream, Chainanalysis, Kadena, Op Return, Quadrans Foundation, the Journal of Cybersecurity, and Worldpay.

We are excited to present the papers appearing in this volume. They represent some of the leading research in secure digital commerce, and we look forward to many more years of fruitful research presented at Financial Cryptography and Data Security.

July 2019

Ian Goldberg
Tyler Moore

Organization

Financial Cryptography and Data Security 2019
St. Kitts Marriott Resort, St. Kitts and Nevis
February 18–22, 2019

Organized by the
International Financial Cryptography Association

In cooperation with the
International Association for Cryptologic Research

General Chair

Rafael Hirschfeld	Unipay, The Netherlands

Program Committee Chairs

Ian Goldberg	University of Waterloo, Canada
Tyler Moore	The University of Tulsa, USA

Program Committee

Shashank Agrawal	Visa Research, USA
Ross Anderson	Cambridge University, UK
Elli Androulaki	IBM Research - Zurich, Switzerland
Diego F. Aranha	Aarhus University, Denmark/University of Campinas, Brazil
Frederik Armknecht	University of Mannheim, Germany
Foteini Baldimtsi	George Mason University, USA
Iddo Bentov	Cornell Tech, USA
Alex Biryukov	University of Luxembourg, Luxembourg
Jeremiah Blocki	Purdue University, USA
Rainer Böhme	Universität Innsbruck, Austria
Joseph Bonneau	New York University, USA
Alvaro A. Cardenas	University of Texas at Dallas, USA
Pern Hui Chia	Google, Switzerland
Sonia Chiasson	Carleton University, Canada
Nicolas Christin	Carnegie Mellon University, USA
Jeremy Clark	Concordia University, Canada
Gaby Dagher	Boise State University, USA
George Danezis	University College London, UK

Matteo Dell'Amico	Symantec Research Labs, France
Maria Dubovitskaya	DFINITY, Switzerland
Benjamin Edwards	IBM Research, USA
Tariq Elahi	University of Edinburgh, UK
William Enck	North Carolina State University, USA
Ittay Eyal	Technion, Israel
Antonio Faonio	IMDEA Software, Spain
Simone Fischer-Hübner	Karlstad University, Sweden
Bryan Ford	EPFL, Switzerland
Stephanie Forrest	Arizona State, USA
Juan Garay	Texas A&M University, USA
Christina Garman	Purdue University, USA
Matthew D. Green	Johns Hopkins University, USA
Rachel Greenstadt	New York University, USA
Jens Grossklags	Technical University of Munich, Germany
Feng Hao	Newcastle University, UK
Ethan Heilman	Boston University, USA
Urs Hengartner	University of Waterloo, Canada
Ryan Henry	University of Calgary, Canada
Nicholas Hopper	University of Minnesota, USA
Philipp Jovanovic	EPFL, Switzerland
Ghassan Karame	NEC Laboratories Europe, Germany
Aniket Kate	Purdue University, USA
Stefan Katzenbeisser	Technische Universität Darmstadt, Germany
Florian Kerschbaum	University of Waterloo, Canada
Markulf Kohlweiss	University of Edinburgh, UK
Aron Laszka	University of Houston, USA
Helger Lipmaa	University of Tartu, Estonia
Wouter Lueks	EPFL, Switzerland
Kanta Matsuura	The University of Tokyo, Japan
Travis Mayberry	USA Naval Academy, USA
Patrick McCorry	King's College London, UK
Catherine Meadows	USA Naval Research Laboratory, USA
Ian Miers	Cornell Tech, USA
Andrew Miller	University of Illinois at Urbana-Champaign, USA
Malte Maser	Princeton University, USA
Satoshi Obana	Hosei University, Japan
Olya Ohrimenko	Microsoft Research, UK
Simon Oya	University of Vigo, Spain
Elizabeth A. Quaglia	Royal Holloway, University of London, UK
Stefanie Roos	TU Delft, The Netherlands
Reihaneh Safavi-Naini	University of Calgary, Canada
Kazue Sako	NEC, Japan
Max Schuchard	University of Tennessee, USA
Abhi Shelat	Northeastern University, USA

Douglas Stebila	University of Waterloo, Canada
Luke Valenta	University of Pennsylvania, USA
Marie Vasek	University of New Mexico, USA
Marko Vukolic	IBM Research - Zurich, Switzerland
Eric Wustrow	University of Colorado Boulder, USA
Zhenfeng Zhang	Institute of Software, Chinese Academy of Sciences, China
Aviv Zohar	The Hebrew University, Israel

Additional Reviewers

Kamalesh Acharya
Sefa Akca
Miguel Ambrona
Dag Arne Osvik
Brian Arthur Shaft
Carsten Baum
Ritam Bhaumik
Chris Buckland
Matteo Campanelli
Panagiotis Chatzigiannis
Mo Chen
Gareth Davies
Angelo De Caro
Sergi Delgado Segura
Pooja Dhomse
Edward Eaton
Kasra EdalatNejad
Kaoutar Elkhiyaoui
Batnyam Enkhtaivan
Shayan Eskandari
Prastudy Fauzi
Daniel Feher
Michael Frwis
Benny Fuhry
Matthias Hamann
Ben Harsha
Haruna Higo
Toshiyuki Isshiki
Hkon Jacobsen
Benjamin Johnson
Keisuke Kajigaya
Dimitris Karakostas
Patrik Keller
Hamidreza Khoshakhlagh
Toomas Krips
Nikos Leonardos
Peiyuan Liu
Angelique Loe
Antonio Marcedone
Mohsen Minaei
Mahsa Moosavi
Pedro Geraldo Morelli Rodrigues Alves
Pratyay Mukherjee
Sanami Nakagawa
Alina Nesen
Bertram Poettering
Mastooreh Salajegheh
Sajin Sasy
Janno Siim
Claudio Soriente
Sergei Tikhomirov
Yiannis Tselekounis
Vesselin Velichkov
Dhinakaran Vinayagamurthy
Giuseppe Vitto
Tianhao Wang
Michal Zajac
Santiago Zanella
Samson Zhou

Contents

Cryptocurrency Cryptanalysis

Proofs of Stake

Measurement

Traceability and How to Stop It

Payment Protocol Security

Multiparty Protocols

Crypto Means Cryptography

Getting Formal

Off-Chain Mechanisms and More Measurement

Fraud Detection and Game Theory

IoT Security, and Crypto Still Means Cryptography