Lecture Notes in Computer Science 9603

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

Jens Grossklags · Bart Preneel (Eds.)

Financial Cryptography and Data Security

20th International Conference, FC 2016
Christ Church, Barbados, February 22–26, 2016
Revised Selected Papers

Springer

Editors
Jens Grossklags
Department of Informatics
Technical University Munich
Garching
Germany

Bart Preneel
Department of Electrical Engineering-ESAT
KU Leuven
Leuven
Belgium

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-662-54969-8 ISBN 978-3-662-54970-4 (eBook)
DOI 10.1007/978-3-662-54970-4

Library of Congress Control Number: 2017940629

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer-Verlag GmbH Germany
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

Preface

FC 2016, the 20th International Conference on Financial Cryptography and Data Security, was held during February 22–26, 2016, at the Accra Beach Hotel and Spa Barbados. This edition was a special 20th anniversary edition featuring some extra items in the program.

We received 137 paper submissions, out of which 36 were accepted, nine as short papers and 27 as full papers, resulting in an acceptance rate of 26%. These proceedings contain revised versions of all the papers. The 20th anniversary keynotes were delivered by privacy pioneer David Chaum, who spoke on "Privategrity" and Turing award winner Adi Shamir who shared with the audience his perspective on "The Past, Present and Future of Financial Cryptography." The program was complemented by a special anniversary panel entitled "The Promises and Pitfalls of Distributed Consensus Systems: From Contract Signing to Cryptocurrencies."

The Program Committee consisted of 49 members with diverse backgrounds and broad research interests. The review process was double-blind. Each paper received at least three reviews; for submissions by Program Committee members this was increased to four. During the discussion phase, additional reviews were solicited when necessary. An intensive discussion was held to clarify issues and to converge towards decisions. The selection of the program was challenging; in the end some high-quality papers had to be rejected due to lack of space.

We would like to sincerely thank the authors of all submissions for contributing high-quality submissions and giving us the opportunity to compile a strong and diverse program.

Special thanks go to the Program Committee members; we value their hard work and dedication to write careful and detailed reviews and to engage in interesting discussions. A few Program Committee members, whom we asked to serve as shepherds, spent additional time in order to help the authors improve their works. More than 60 external reviewers contributed to the review process; we would like to thank them for their efforts.

We are greatly indebted to Rafael Hirschfeld, the conference general chair, for his tireless efforts to make the conference a success. We also would like to thank the anniversary chairs, Sven Dietrich and Ahmad Sadeghi. Special thanks go the board of directors of the International Financial Cryptography Association for their support and advice.

Finally, we would like to thank the Office of Naval Research Global (ONR Global), bitt, the CROSSING project at TU Darmstadt, Rohde & Schwartz, AtenCoin, Gemini, Google, the *Journal of Cybersecurity*, KOBIL, SAP, KPMG, Worldpay, and the NSF for their generous support of the conference.

We hope that the papers in this volume prove valuable for your research and professional activities and that Financial Cryptography and Data Security will continue to play its unique role in bringing together researchers and practitioners in the area of secure digital commerce.

February 2017

Jens Grossklags
Bart Preneel

FC 2016

Financial Cryptography and Data Security 2016
Accra Beach Hotel and Spa, Barbados
February 22–26, 2016

Organized by the
International Financial Cryptography Association

In cooperation with the
International Association for Cryptologic Research

General Chair

Rafael Hirschfeld	Unipay, The Netherlands

Anniversary Chairs

Sven Dietrich	City University of New York, USA
Ahmad Sadeghi	TU Darmstadt, Germany

Program Chairs

Jens Grossklags	TU Munich, Germany
Bart Preneel	KU Leuven, Belgium

Program Committee

Masayuki Abe	NTT Laboratories, Japan
Alessandro Acquisti	Carnegie Mellon University, USA
Ross Anderson	Cambridge University, UK
Elli Androulaki	IBM Research Zurich, Switzerland
N. Asokan	Aalto University, Finland
Paulo Barreto	University of Sao Paulo, Brazil
Steven Bellovin	Columbia University, USA
Daniel Bernstein	University of Illinois at Chicago, USA
Rainer Böhme	University of Innsbruck, Austria
Alvaro Cardenas	University of Texas at Dallas, USA
Jeremy Clark	Concordia University, USA
Nicolas Courtois	University College London, UK
George Danezis	University College London, UK
Serge Egelman	UC Berkeley, USA

Seda Gürses	NYU, USA
Feng Hao	Newcastle University, UK
Thorsten Holz	Ruhr University Bochum, Germany
Trent Jaeger	The Pennsylvania State University, USA
Markus Jakobsson	Qualcomm, USA
Benjamin Johnson	Carnegie Mellon University, USA
Aniket Kate	Purdue University, USA
Florian Kerschbaum	SAP, Germany
Aggelos Kiayias	National and Kapodistrian University of Athens, Greece
Bart Knijnenburg	Clemson University, USA
Markulf Kohlweiss	Microsoft Research, UK
Aron Laszka	UC Berkeley, USA
Anja Lehmann	IBM Research Zurich, Switzerland
Arjen Lenstra	EPFL, Switzerland
Patrick Loiseau	EURECOM, France
Travis Mayberry	US Naval Academy, USA
Catherine Meadows	Naval Research Laboratory, USA
Sarah Meiklejohn	University College London, UK
Tyler Moore	University of Tulsa, USA
Steven Murdoch	University College London, UK
Tatsuaki Okamoto	NTT Laboratories, Japan
Kenneth Paterson	Royal Holloway, University of London, UK
Roberto Perdisci	University of Georgia, USA
Avi Rubin	Johns Hopkins University, USA
Ahmad Sadeghi	TU Darmstadt, Germany
Rei Safavi-Naini	University of Calgary, Canada
Nigel Smart	University of Bristol, UK
Jessica Staddon	Google, USA
Carmela Troncoso	Gradiant, Spain
Damien Vergnaud	École Normale Supérieure, France
Nicholas Weaver	International Computer Science Institute, USA
Xinyu Xing	The Pennsylvania State University, USA
Moti Yung	Google and Columbia University, USA

Additional Reviewers

Svetlana Abramova	Zekeriya Erkin	Vijay Kamble
Enrique Argones	Sadegh Farhang	Gabe Kaptchuk
Ero Balsa	Ben Fisch	Carmen Kempka
Erik-Oliver Blass	Oana Goga	Sheharbano Khattak
Matthias Carnein	Steven Goldfeder	Ryo Kikuchi
Joseph Carrigan	Marian Harbach	Markus Krause
Alex Davidson	Heqing Huang	Junichiro Kume
Angelo De Caro	Brittany Johnson	Stefan Laube

Sebastian Luhn
Caitlin Lustig
Samuel Marchal
Paul Martin
Patrick Mccorry
Maryam Mehrnezhad
Aastha Mehta
Tarik Moataz
Malte Möser
Thomas Nyman
Miyako Ohkubo
Olga Ohrimenko
Melek Önen
Cristina Onete
Simon Oya
Giorgos Panagiotakos
Goutam Paul
Andrew Paverd
Yu Pu
Elizabeth Anne Quaglia
Markus Riek
Michael Rushanan
Katerina Samari
Daniel Sanchez
Luiza Sayfullina
Pascal Schoettle
Siamak F. Shahandashti
Kumar Sharad
Karthik Sheshadri
Brian Sniffen
Koutarou Suzuki
Syed Taha
Sandeep Tamrakar
Qiang Tang
Yiannis Tselekounis
Marie Vasek
David Wagner
Brecht Wyseur
Yi Xu
Thomas Zacharias
Greg Zaverucna
Bingsheng Zhang
Dionysis Zindros

Contents