Lecture Notes in Computer Science 7397

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

Angelos D. Keromytis (Ed.)

Financial Cryptography and Data Security

16th International Conference, FC 2012
Kralendijk, Bonaire, February 27-March 2, 2012
Revised Selected Papers

Springer

Volume Editor

Angelos D. Keromytis
Columbia University
Department of Computer Science
1214 Amsterdam Avenue
New York, NY 10027-7003, USA
E-mail: angelos@cs.columbia.edu

ISSN 0302-9743
ISBN 978-3-642-32945-6
DOI 10.1007/978-3-642-32946-3

e-ISSN 1611-3349
e-ISBN 978-3-642-32946-3

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012945011

CR Subject Classification (1998): E.3, K.6.5, K.4.4, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the proceedings of the 16th International Conference on Financial Cryptography and Data Security (FC), held at the Divi Flamingo Beach Resort, Bonaire, February 27-March 1, 2012.

FC is a well-established international forum for research, advanced development, education, exploration, and debate regarding information assurance in the context of finance and commerce. The conference covers all aspects of securing transactions and systems.

This year we assembled a diverse program featuring 29 paper and a panel on "Laws Against Adopting PETs (Privacy Enhancing Technologies)." The conference was opened by Scott M. Zoldi, Vice President for Analytic Science at FICO, with a keynote address on "Analytic Techniques for Combating Financial Fraud."

The program was put together through a standard peer-review process by a technical Program Committee selected by the Program Chair. This year we received 88 submissions from authors and institutions representing 26 countries. All submissions received at least three reviews from the 32 members of the Program Committee or from the 31 outside experts. A further online discussion phase that lasted more than 2 weeks led to the selection of 29 papers (representing an overall acceptance rate of 33%).

This conference was made possible through the dedicated work of our General Chair, Rafael Hirschfeld, from Unipay Technologies, The Netherlands. Ray also acted as our (tireless) Local Arrangements Chair. The Program Chair would like to thank especially the Program Committee members and external reviewers for contributing their time and expertise to the selection of papers for the program and for providing feedback to improve all submissions. Finally, the members of the International Financial Cryptography Association (IFCA) board should be acknowledged for keeping the FC conference going through the years. This year's conference was made more affordable thanks to the generosity of our sponsors.

March 2012 Angelos D. Keromytis

Organization

Program Committee

Mikhail Atallah	Purdue University, USA
Konstantin Beznosov	UBC, Canada
Mike Bond	
Jan Camenisch	IBM Research, Zurich Research Laboratory, Switzerland
Sonia Chiasson	Carleton University, Canada
Nicolas Christin	Carnegie Mellon University, USA
David Mandell Freeman	Stanford University, USA
Virgil Gligor	CMU, USA
Dieter Gollmann	Hamburg University of Technology, Germany
J. Alex Halderman	University of Michigan, USA
John Ioannidis	
Sotiris Ioannidis	FORTH-ICS, Greece
Stanislaw Jarecki	University of California, Irvine, USA
Somesh Jha	University of Wisconsin, USA
Jonathan Katz	University of Maryland, USA
Angelos Keromytis	Columbia University, USA
Engin Kirda	Institut Eurecom, France
Tadayoshi Kohno	University of Washington, USA
Wenke Lee	Georgia Institute of Technology, USA
Corrado Leita	Symantec Research
Arjen Lenstra	
Ninghui Li	Purdue University, USA
Helger Lipmaa	Cybernetica AS and Tallinn University, Estonia
Tal Malkin	Columbia University, USA
Patrick Mcdaniel	Pennsylvania State University, USA
Catherine Meadows	NRL
David Molnar	Microsoft Research
Fabian Monrose	The University of North Carolina at Chapel Hill, USA
Anil Somayaji	Carleton University, Canada
Jessica Staddon	Google
Angelos Stavrou	George Mason University, USA
Carmela Troncoso	IBBT-K.U.Leuven, ESAT/COSIC, Belgium
Lenore Zuck	University of Illinois in Chicago, USA

Additional Reviewers

Balasch, Josep
Barrera, David
Bos, Joppe
Boshmaf, Yazan
Brakerski, Zvika
Camp, Jean
Fan, Junfeng
Fredrikson, Matt
Henginer, Nadia
Hinrichs, Tim
Hiremagalore, Sharath
Jeske, Tobias
Jia, Quan
Koshy, Diana
Krell, Fernando
Lee, Adam J.
Meiklejohn, Sarah
Muslukhov, Ildar
Naehrig, Michael
Osvik, Dag Arne
Qardaji, Wahbeh
Raghunathan, Ananth
Raykova, Mariana
Rial, Alfredo
Seymer, Paul
Sun, San-Tsai
Uhsadel, Leif
Venkatakrishnan, Venkat
Wang, Zhaohui
Wei, Lei

Table of Contents