Lecture Notes in Computer Science 4107

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

Giovanni Di Crescenzo Avi Rubin (Eds.)

Financial Cryptography and Data Security

10th International Conference, FC 2006
Anguilla, British West Indies, February 27-March 2, 2006
Revised Selected Papers

Springer

Volume Editors

Giovanni Di Crescenzo
Telcordia Technologies
One Telcordia Drive 1K325, Piscataway, NJ, USA
E-mail: giovanni@research.telcordia.com

Avi Rubin
Johns Hopkins University (JHUISI)
3100 Wyman Park Drive, Baltimore, MD 21211 USA
E-mail: rubin@jhu.edu

Library of Congress Control Number: 2006933057

CR Subject Classification (1998): E.3, D.4.6, K.6.5, K.4.4, C.2, J.1, F.2.1-2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-46255-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-46255-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11889663 06/3142 5 4 3 2 1 0

Preface

The 10th International Conference on Financial Cryptography and Data Security (FC 2006) was held in Anguilla, British West Indies, from February 27 to March 2, 2006. This conference continues to be the premier international forum for research, advanced development, education, exploration, and debate regarding security in the context of finance and commerce.

As we were honoured to put together the program in this conference's 10th edition, we attempted to combine the naturally festive mood with its interdisciplinary nature. Kicking off the 10th-year festivities were a welcome speech by Victor Banks, the Minister of Finance of Anguilla, and our Keynote Address by the renowned cryptographer Ron Rivest. One of the most influential figures in cryptography, Ron reviewed some of his past predictions and lessons learned over the last 10 years, and prognosticated directions for the next decade. The conference also featured an invited talk by Michael Froomkin about the current legal landscape of financial cryptography, and two interesting panel sessions: one on identity management and a second one providing further reflections on the past 10 years of financial cryptography, featuring talks by Jacques Stern, and Nicko van Someren, representing reflections from the academic and industrial world, respectively. The technical program featured 19 regular papers and 6 short papers, selected out of 64 submissions, and as always, other conference attendees were invited to make short presentations during the rump session, which maintained its lively and colorful reputation.

Putting together such a strong program would not be possible without the hard work of the Program Committee and of a large number of external reviewers, whose names are listed on separate pages. Each submission was refereed by at least three experts, and often detailed technical discussions were necessary before decisions could be made. These were often challenging due to the high quality of the submitted papers, many of which could not be included in the program. Additional thanks go to all researchers who submitted papers, hoping that enough feedback was given to them for further developments of their work.

We also would like to thank this year's General Chair, Patrick McDaniel, for valuable assistance on several aspects of the conference organization, and the Local Arrangements Chair, Rafael Hirschfeld, for handling several logistics in Anguilla. Special thanks also go to Ted Lu for helping with setting up the Web-based submission and reviewing system, which was essential for handling such a large number of submissions and reviewers, and to William Enck for onsite logistic help. We hope to have fulfilled our goal of a successful conference. Like all its participants, we look forward to (at least) 10 more years of Financial Cryptography and Data Security!

June 2006

Giovanni Di Crescenzo
Avi Rubin

Organization

The Financial Cryptography and Data Security 2006 conference was organized by the International Financial Cryptography Association (IFCA).

Program Chairs

Giovanni Di Crescenzo	Telcordia Technologies
Avi Rubin	Johns Hopkins University

General Chair

Patrick Mc Daniel	Penn State University

Local Arrangements Chair

Rafael Hirschfeld	Unipay Technologies

Program Committee

Matt Blaze	University of Pennsylvania
Alfredo De Santis	Universitá di Salerno
Sven Dietrich	Carnegie Mellon University
Juan Garay	Bell Labs
Dan Geer	Verdasys
Ari Juels	RSA
Yoshi Kohno	University of California San Diego
Arjen Lenstra	Bell Labs and Technische Universiteit Eindhoven
Helger Lipmaa	Cybernetica AS and University of Tartu
Steve Myers	Indiana University
Andrew Odlyzko	University of Minnesota
Tatsuaki Okamoto	NTT
Carles Padro	Universitat Politecnica de Catalunya
Andrew Patrick	NRC Canada
Ahmad-Reza Sadeghi	Ruhr-University Bochum
Kazue Sako	NEC
Dawn Song	Carnegie Mellon University

Stuart Stubblebine	Univ. of California Davis and Stubblebine Labs
Adam Stubblefield	Independent Security Evaluators
Paul Syverson	Naval Research Lab
Mike Szydlo	RSA
Gene Tsudik	University of California Irvine
Doug Tygar	Berkeley University
Alma Whitten	Google
Yacov Yacobi	Microsoft Research
Yuliang Zheng	University of North Carolina
Moti Yung	RSA and Columbia University

Additional Referees

Michel Abdalla
Madhukar Anand
Asokan
Giuseppe Ateniese
Lujo Bauer
Don Beaver
John Bethencort
Ziad Bizri
Daniel Bleichenbacher
David Brumley
Dario Catalano
Liqun Chen
Yuqun Chen
Monica Chew
Paolo D'Arco
Breno de Medeiros
Yevgeniy Dodis
Edith Elkind
Umberto Ferraro
Jun Furukawa
Sabastian Gajek
Ulrich Huber
Markus Jakobsson
Mariusz Jakubowski
Mike Just
Manoj Kasichainula
Aggelos Kiayias
Larry Korba
Howard Lipson
Philip MacKenzie
Peter Montgomery
Kengo Mori
Jihye Kim
Lea Kissner
Vladimir Kolesnikov
Howard Lipson
Ferran Marques
Stephen Marsh
James Newsome
Lluis Padro
Bryan Parno
Nitesh Saxena
Kai Schramm
Micah Sherr
Ronggong Song
Isamu Teranishi
Ersin Uzun
Jason Waddle
Shouhuai Xu

Sponsors

EverBank (Silver sponsor)
Navio (Silver sponsor)
Offshore Information Services (Silver sponsor)
Google (Bronze sponsor)
NCipher (Bronze sponsor)
Bibit (Sponsor in kind)

Table of Contents

Authentication and Fraud Detection

Privacy

Reputation and Mix-Nets

Short Papers

Conditional Financial Cryptography

Payment Systems

Efficient Protocols