Lecture Notes in Computer Science 4886

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

Sven Dietrich Rachna Dhamija (Eds.)

Financial Cryptography and Data Security

11th International Conference, FC 2007, and
1st International Workshop on Usable Security, USEC 2007
Scarborough, Trinidad and Tobago, February 12-16, 2007
Revised Selected Papers

Volume Editors

Sven Dietrich
Stevens Institute of Technology, Computer Science Department
Castle Point on Hudson, Hoboken, NJ 07030, USA
E-mail: spock@cs.stevens.edu

Rachna Dhamija
Harvard University, Center for Research on Computation and Society, DEAS
Maxwell Dworkin 110, 33 Oxford Street, Cambridge, MA 02138, USA
E-mail: rachna@deas.harvard.edu

Library of Congress Control Number: 2007941592

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 3-540-77365-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-77365-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12206735 06/3180 5 4 3 2 1 0

The original version of the book was revised: The copyright line was incorrect. The Erratum to the book is available at
DOI: 10.1007/978-3-540-77366-5_37

Preface

The 11th International Conference on Financial Cryptography and Data Security (FC 2007, http://fc07.ifca.ai), organized by the International Financial Cryptography Association (IFCA, http://www.ifca.ai/), was held in Tobago, February 12–15, 2007. The conference is a well-established and premier international forum for research, advanced development, education, exploration, and debate regarding security in the context of finance and commerce. We continue to cover all aspects of securing transactions and systems, which this year included a range of technical areas such as cryptography, payment systems, anonymity, privacy, authentication, and commercial and financial transactions. For the first time, there was an adjacent workshop on Usable Security, held after FC 2007 in the same location. The papers are included in the last part of this volume. The conference goal was to bring together top cryptographers, data-security specialists, and computer scientists with economists, bankers, implementers, and policy makers.

The goal was met this year: there were 85 submissions, out of which 17 research papers and 1 system presentation paper were accepted. In addition, the conference featured two distinguished speakers, Mike Bond and Dawn Jutla, and two panel sessions, one on RFID and one on virtual economies. As always, there was the rump session on Tuesday evening, colorful as usual.

Putting together the program was a challenging task: the Program Committee fought long and hard in online discussions in late fall 2006 over which papers to accept, assisted by the many external reviewers who brought in their respective expertise. Each paper was carefully evaluated by at least three referees. The work was made more difficult by the large number of high-quality papers received and the relatively small number which could be accepted. We would like to thank all submitters for the papers and their hard work, and hope that the comments received from the reviewers will allow them to progress with their work.

I would like to thank the General Chair, Rafael Hirschfeld, and the Sponsorship Chair, Burton Rosenberg, for all their hard work in getting this conference organized and sponsored in Tobago, its southernmost location thus far, and Jon Callas for moderating the rump session. Special thanks go to Joe McManus, Rudy Maceyko, and Jason McCormick at CERT for setting up, securing, and running the Web-based submission and reviewing system in a tight environment.

I hope all of the participants found this year's program as exciting as I did, with its continued interdisciplinary views on the subject and its strong focus on the financial side, and that the conference continues to provide an opportunity to participate in fruitful discussions on the issues and trends in the financial industry and cryptography.

June 2007 Sven Dietrich

Financial Cryptography and Data Security 2007

11th International Conference
February 12–15, 2007
Lowlands, Scarborough, Trinidad and Tobago

Program Chair

Sven Dietrich, Carnegie Mellon University, USA

General Chair

Rafael Hirschfeld, Unipay Technologies, Netherlands

Program Committee

Alessandro Acquisti	Carnegie Mellon University, USA
Jon Callas	PGP Corporation, USA
Yvo Desmedt	University College London, UK
Giovanni Di Crescenzo	Telcordia, USA
Roger Dingledine	The Tor Project, USA
Bernhard Esslinger	Deutsche Bank and University of Siegen, Germany
Philippe Golle	Palo Alto Research Center, USA
Klaus Kursawe	Philips Research Eindhoven, Netherlands
Arjen Lenstra	EPFL, Switzerland
Patrick McDaniel	Penn State University, USA
Tatsuaki Okamoto	NTT, Japan
Kazue Sako	NEC, Japan
Radu Sion	Stony Brook University, USA
Stuart Stubblebine	Stubblebine Consulting/Research and UC Davis, USA
Paul Syverson	Naval Research Laboratory, USA
Mike Szydlo	RSA, USA
Jonathan Trostle	JHU/APL, USA
Moti Yung	RSA Labs. (EMC) and Columbia University, USA
Yuliang Zheng	University of North Carolina at Charlotte, USA

External Reviewers

Farid Ahmed	Lisa Johansen
Patrick Amon	Stefan Katzenbeisser
Toshinori Araki	Tim Kerrins
Kevin Butler	Aggelos Kiayias

Bogdan Carbunar
Scott Contini
David Dagon
William Enck
Allan Friedman
Jun Furukawa
Craig Gentry
Rachel Greenstadt
Stuart Haber
Boniface Hicks
Toshiyuki Isshiki
Eike Kiltz
Phil MacKenzie
Kengo Mori
Rei Safavi-Naini
Gregory Neven
Satoshi Obana
Pascal Paillier
Luke St. Clair
Isamu Teranishi
Patrick Traynor
Shoko Yonezawa

Sponsorship Chair

Burton Rosenberg, University of Miami, USA

Sponsors

Bronze Sponsors: Google, Inc.
nCipher
PGP Corporation
EverBank

In-kind Sponsor: Bibit Global Payment Services

Table of Contents

Authentication

Anonymity and Privacy

Cryptography and Commercial Transactions

Financial Transactions and Web Services

Panel

Invited Talk

System Presentation

Cryptography

Usable Security Workshop

Full Papers

Short Papers