Lecture Notes in Computer Science 3570

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

Editorial Board

Andrew S. Patrick Moti Yung (Eds.)

Financial Cryptography and Data Security

9th International Conference, FC 2005
Roseau, The Commonwealth of Dominica
February 28 – March 3, 2005
Revised Papers

Volume Editors

Andrew S. Patrick
National Research Council of Canada
1200 Montreal Road, Ottawa, ON, Canada K1A 0R6
E-mail: Andrew.Patrick@nrc-cnrc.gc.ca

Moti Yung
RSA Laboratories and Columbia University
Computer Science, 1214 Amsterdam Ave., New York, NY, USA
E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2005928164

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

ISSN 0302-9743
ISBN-10 3-540-26656-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-26656-3 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11507840 06/3142 5 4 3 2 1 0

Preface

The 9th International Conference on Financial Cryptography and Data Security (FC 2005) was held in the Commonwealth of Dominica from February 28 to March 3, 2005. This conference, organized by the International Financial Cryptography Association (IFCA), continues to be the premier international forum for research, exploration, and debate regarding security in the context of finance and commerce. The conference title and scope was expanded this year to cover all aspects of securing transactions and systems. The goal is to build an interdisciplinary meeting, bringing together cryptographers, data-security specialists, business and economy researchers, as well as economists, IT professionals, implementers, and policy makers.

We think that this goal was met this year. The conference received 90 submissions and 24 papers were accepted, 22 in the Research track and 2 in the Systems and Applications track. In addition, the conference featured two distinguished invited speakers, Bezalel Gavish and Lynne Coventry, and two interesting panel sessions, one on phishing and the other on economics and information security. Also, for the first time, some of the papers that were judged to be very strong but did not make the final program were selected for special invitation to our Works in Progress (Rump) Session that took place on Wednesday evening. Three papers were highlighted in this forum this year, and short versions of the papers are included here. As always, other conference attendees were also invited to make presentations during the rump session, and the evening lived up to its colorful reputation.

Putting together such a strong program would not be possible without the hard work of the Program Committee, whose members are listed on a separate page. In addition, a large number of external reviewers were recruited because of their special expertise in particular areas, and their names are also listed in these proceedings. Each of the submissions was reviewed by at least three experts, who then engaged in vigorous online discussions. The selection process was difficult because there were many excellent papers that could not be fit into the program. We want to thank all the authors who submitted papers, and we hope that the feedback they received was useful for continuing to develop their work, whether their papers were accepted or not.

We also want to thank this year's General Chair, Stuart Schechter, for valuable assistance and for handling the arrangements in Dominica, and Ari Juels for moderating the rump session. Special thanks also go out to Aggelos Kiayias for setting up and operating the Web-based reviewing system that was essential for handling such a large number of submissions and reviewers.

We hope that this year's program was in the spirit of the conference goals as envisioned, and that the conference continues its colorful tradition as an interdisciplinary, high diversity meeting that helps foster cooperation and the fruitful exchange of ideas among its international participants.

April 2005 Andrew Patrick and Moti Yung

Financial Cryptography and Data Security 2005

Program Chairs: Andrew Patrick and Moti Yung
General Chair: Stuart Schechter

Program Committee

Colin Boyd	Queensland University of Technology
Suresh Chari	IBM
Liqun Chen	HP Labs
Lynne Coventry	NCR
Yvo Desmedt	University College London
Giovanni Di Crescenzo	Telcordia Technologies
Roger Dingledine	Moria Research Labs
Scott Flinn	National Research Council of Canada
Juan Garay	Bell Labs, Lucent Technologies
Dan Geer	Geer Risk Services
Craig Gentry	DoCoMo Labs USA
Mike Just	Treasury Board of Canada
Aggelos Kiayias	University of Connecticut
Helger Lipmaa	Helsinki University of Technology
David M'Raihi	Verisign
Kobbi Nissim	Microsoft
Satoshi Obana	Columbia University and NEC
Andrew Odlyzko	University Minnesota
Pascal Paillier	Gemplus
David Pointcheval	Ecole Normale Supérieure
Bart Preneel	Katholieke Universiteit Leuven
Angela Sasse	University College London
Berry Schoenmakers	Technische Universiteit Eindhoven
Sean Smith	Dartmouth College
Jessica Staddon	Palo Alto Research Center (PARC)
Michael Szydlo	RSA Laboratories
Jacques Traore	France Télécom
Gene Tsudik	University of California, Irvine
Alma Whitten	Google
Adam Young	Cigital
Bill Yurcik	NCSA

Sponsors

Gold Sponsor:	Interactive Investor (www.iii.co.uk)
Bronze Sponsors:	RSA Security
	France Télécom
In-Kind Sponsor:	Bibit Global Payment Services

External Reviewers

Michel Abdalla
Gildas Avoine
Alexandra Boldyreva
Calude Castelluccia
George Danezis
Alex Deacon
Glenn Durfee
Renwei Ge
Rosario Gennaro
Henri Gilbert
Marc Girault
David Goldberg
Philippe Golle
Juan Gonzalez
Rachel Greenstadt
Shai Halevi
Helena Handschuh
Yvonne Hitchcock
Kevin Soo Hoo
Markus Jakobsson
Stas Jarecki
Charanjit Jutla
Sébastien Kunz-Jacques
Joseph Lano
John Malone-Lee
Nick Mathewson
Sean Murphy
Steve Myers
Gregory Neven
Jean-Claude Pailles
Valeria de Paiva
Duong Hieu Phan
Tal Rabin
Yona Raekow
Zulfikar Ramzan
Josyula R. Rao
Jason Reid
Pankaj Rohatgi
Markku-Juhani O. Saarinen
Marius Schilder
Umesh Shankar
Vitaly Shmatikov
Paul Syverson
Jun'ichi Takeuchi
Yiannis Tsiounis
Yunlei Zhao
Hong-Sheng Zhou

Table of Contents

Privacy

Hardware Oriented Mechanisms

Supporting Financial Transactions

Systems, Applications, and Experiences

Message Authentication

Exchanges and Contracts

Auctions and Voting

Works in Progress

User Authentication