## Lecture Notes in Computer Science

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

#### Editorial Board

David Hutchison Lancaster University, UK Takeo Kanade Carnegie Mellon University, Pittsburgh, PA, USA Josef Kittler University of Surrey, Guildford, UK Jon M. Kleinberg Cornell University, Ithaca, NY, USA Friedemann Mattern ETH Zurich, Switzerland John C. Mitchell Stanford University, CA, USA Moni Naor Weizmann Institute of Science, Rehovot, Israel Oscar Nierstrasz University of Bern, Switzerland C. Pandu Rangan Indian Institute of Technology, Madras, India Bernhard Steffen University of Dortmund, Germany Madhu Sudan Massachusetts Institute of Technology, MA, USA Demetri Terzopoulos University of California, Los Angeles, CA, USA Doug Tygar University of California, Berkeley, CA, USA Moshe Y. Vardi Rice University, Houston, TX, USA Gerhard Weikum Max-Planck Institute of Computer Science, Saarbruecken, Germany

# 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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007 Printed in Germany

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

## Keynote Address

Leaving Room for the Bad Guys (Abstract) Mike Bond	1
Payment Systems	
Vulnerabilities in First-Generation RFID-enabled Credit Cards Thomas S. Heydt-Benjamin, Daniel V. Bailey, Kevin Fu, Ari Juels, and Tom O'Hare	2
Conditional E-Cash Larry Shi, Bogdan Carbunar, and Radu Sion	15
A Privacy-Protecting Multi-Coupon Scheme with Stronger Protection Against Splitting Liqun Chen, Alberto N. Escalante B., Hans Löhr, Mark Manulis, and Ahmad-Reza Sadeghi	29
Panel	
Panel: RFID Security and Privacy (Abstract)	45
Position Statement in RFID S&P Panel: RFID and the Middleman Ross Anderson	46
Position Statement in RFID S&P Panel: Contactless Smart Cards Jon Callas	50
Position Statement in RFID S&P Panel: From Relative Security to Perceived Secure	53

## Anonymity

A Model of Onion Routing with Provable Anonymity	57
Joan Feigenbaum, Aaron Johnson, and Paul Syverson	
K-Anonymous Multi-party Secret Handshakes	72
Shouhuai Xu and Moti Yung	

## Authentication

Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer	88
Scalable Authenticated Tree Based Group Key Exchange for Ad-Hoc Groups	104
On Authentication with HMAC and Non-random Properties Christian Rechberger and Vincent Rijmen	119

## Anonymity and Privacy

Hidden Identity-Based Signatures	134
Aggelos Kiayias and Hong-Sheng Zhou	
Space-Efficient Private Search with Applications to Rateless Codes	148
George Danezis and Claudia Diaz	

## Cryptography and Commercial Transactions

Cryptographic Securities Exchanges Christopher Thorpe and David C. Parkes	163
Improved Multi-party Contract Signing Aybek Mukhamedov and Mark Ryan	179
Informant: Detecting Sybils Using Incentives N. Boris Margolin and Brian N. Levine	192

## **Financial Transactions and Web Services**

Dynamic Virtual Credit Card Numbers	208
Ian Molloy, Jiangtao Li, and Ninghui Li	
The Unbearable Lightness of PIN Cracking	224
Omer Berkman and Odelia Moshe Ostrovsky	

## Panel

Virtual Economies: Threats and Risks	239
Christopher Thorpe, Jessica Hammer, Jean Camp, Jon Callas, and	
Mike Bond	

## Invited Talk

Usable SPACE: Security, Privacy, and Context for the Mobile User	
(Abstract)	245
Dawn Jutla	

## System Presentation

Personal Digital Rights Management for Mobile Cellular Devices	246
Siddharth Bhatt, Bogdan Carbunar, Radu Sion, and Venu Vasudevan	

## Cryptography

Certificate Revocation Using Fine Grained Certificate Space	
Partitioning	247
Vipul Goyal	
An Efficient Aggregate Shuffle Argument Scheme Jun Furukawa and Hideki Imai	260

## Usable Security Workshop

Preface	277
Rachna Dhamija	

## **Full Papers**

An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks	281
Collin Jackson, Daniel R. Simon, Desney S. Tan, and Adam Barth	
WSKE: Web Server Key Enabled Cookies Chris Masone, Kwang-Hyun Baek, and Sean Smith	294
Usability Analysis of Secure Pairing Methods Ersin Uzun, Kristiina Karvonen, and N. Asokan	307
Low-Cost Manufacturing, Usability, and Security: An Analysis of Bluetooth Simple Pairing and Wi-Fi Protected Setup <i>Cynthia Kuo, Jesse Walker, and Adrian Perrig</i>	325
Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers Jens Grossklags and Nathan Good	341

## Short Papers

What Instills Trust? A Qualitative Study of Phishing Markus Jakobsson, Alex Tsow, Ankur Shah, Eli Blevis, and Youn-Kyung Lim	356
Phishing IQ Tests Measure Fear, Not Ability Vivek Anandpara, Andrew Dingman, Markus Jakobsson, Debin Liu, and Heather Roinestad	362
Mental Models of Security Risks Farzaneh Asgharpour, Debin Liu, and L. Jean Camp	367
Improving Usability by Adding Security to Video Conferencing Systems	378
A Sense of Security in Pervasive Computing—Is the Light on When the Refrigerator Door Is Closed? Jakob Illeborg Pagter and Marianne Graves Petersen	383
Erratum to: Financial Cryptography and Data Security Sven Dietrich and Rachna Dhamija	E1
Author Index	389