

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

Alfred Kobsa

University of California, Irvine, CA, 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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

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

© Springer-Verlag Berlin Heidelberg 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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

| | |
|---|-----|
| Social Authentication: Harder Than It Looks | 1 |
| <i>Hyoungshick Kim, John Tang, and Ross Anderson</i> | |
| The MVP Web-Based Authentication Framework (Short Paper) | 16 |
| <i>Sonia Chiasson, Chris Deschamps, Elizabeth Stobert, Max Hlywa, Bruna Freitas Machado, Alain Forget, Nicholas Wright, Gerry Chan, and Robert Biddle</i> | |
| A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs | 25 |
| <i>Joseph Bonneau, Sören Preibusch, and Ross Anderson</i> | |
| The Postmodern Ponzi Scheme: Empirical Analysis of High-Yield Investment Programs | 41 |
| <i>Tyler Moore, Jie Han, and Richard Clayton</i> | |
| Deploying Secure Multi-Party Computation for Financial Data Analysis (Short Paper) | 57 |
| <i>Dan Bogdanov, Riivo Talviste, and Jan Willemson</i> | |
| Cryptographic Rule-Based Trading (Short Paper) | 65 |
| <i>Christopher Thorpe and Steven R. Willis</i> | |
| Efficient Private Proximity Testing with GSM Location Sketches | 73 |
| <i>Zi Lin, Denis Foo Kune, and Nicholas Hopper</i> | |
| Metrics for Measuring ISP Badness: The Case of Spam (Short Paper) | 89 |
| <i>Benjamin Johnson, John Chuang, Jens Grossklags, and Nicolas Christin</i> | |
| Congestion-Aware Path Selection for Tor | 98 |
| <i>Tao Wang, Kevin Bauer, Clara Forero, and Ian Goldberg</i> | |
| Attacking the Washington, D.C. Internet Voting System | 114 |
| <i>Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman</i> | |
| Security Audits Revisited | 129 |
| <i>Rainer Böhme</i> | |
| Efficient, Compromise Resilient and Append-Only Cryptographic Schemes for Secure Audit Logging | 148 |
| <i>Attila A. Yavuz, Peng Ning, and Michael K. Reiter</i> | |

| | |
|---|-----|
| On Secure Two-Party Integer Division | 164 |
| <i>Morten Dahl, Chao Ning, and Tomas Toft</i> | |
| A Non-interactive Range Proof with Constant Communication | 179 |
| <i>Rafik Chaabouni, Helger Lipmaa, and Bingsheng Zhang</i> | |
| Privacy-Preserving Stream Aggregation with Fault Tolerance | 200 |
| <i>T.-H. Hubert Chan, Elaine Shi, and Dawn Song</i> | |
| Dynamic Accumulator Based Discretionary Access Control for Outsourced Storage with Unlinkable Access (Short Paper) | 215 |
| <i>Daniel Slamanig</i> | |
| Privacy Enhanced Access Control for Outsourced Data Sharing | 223 |
| <i>Mariana Raykova, Hang Zhao, and Steven M. Bellovin</i> | |
| Designing Privacy-Preserving Smart Meters with Low-Cost Microcontrollers | 239 |
| <i>Andres Molina-Markham, George Danezis, Kevin Fu, Prashant Shenoy, and David Irwin</i> | |
| Memory-Efficient Garbled Circuit Generation for Mobile Devices | 254 |
| <i>Benjamin Mood, Lara Letaw, and Kevin Butler</i> | |
| Oblivious Decision Programs from Oblivious Transfer: Efficient Reductions | 269 |
| <i>Payman Mohassel and Salman Niksefat</i> | |
| UC-Secure Searchable Symmetric Encryption | 285 |
| <i>Kaoru Kurosawa and Yasuhiro Ohtaki</i> | |
| CTL: A Platform-Independent Crypto Tools Library Based on Dataflow Programming Paradigm | 299 |
| <i>Junaid Jameel Ahmad, Shujun Li, Ahmad-Reza Sadeghi, and Thomas Schneider</i> | |
| A Cache Timing Attack on AES in Virtualization Environments | 314 |
| <i>Michael Weiß, Benedikt Heinz, and Frederic Stumpf</i> | |
| Softer Smartcards: Usable Cryptographic Tokens with Secure Execution | 329 |
| <i>Franz Ferdinand Brasser, Sven Bugiel, Atanas Filyanov, Ahmad-Reza Sadeghi, and Steffen Schulz</i> | |
| The PACE AA Protocol for Machine Readable Travel Documents, and Its Security | 344 |
| <i>Jens Bender, Özgür Dagdelen, Marc Fischlin, and Dennis Kügler</i> | |
| Oblivious Printing of Secret Messages in a Multi-party Setting | 359 |
| <i>Aleksander Essex and Urs Hengartner</i> | |

| | |
|--|-----|
| Reverse Fuzzy Extractors: Enabling Lightweight Mutual Authentication for PUF-Enabled RFIDs | 374 |
| <i>Anthony Van Herrewege, Stefan Katzenbeisser, Roel Maes, Roel Peeters, Ahmad-Reza Sadeghi, Ingrid Verbauwhede, and Christian Wachsmann</i> | |
| CommitCoin: Carbon Dating Commitments with Bitcoin (Short Paper) | 390 |
| <i>Jeremy Clark and Aleksander Essex</i> | |
| Bitter to Better — How to Make Bitcoin a Better Currency | 399 |
| <i>Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun</i> | |
| Author Index | 415 |