

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

George Danezis (Ed.)

Financial Cryptography and Data Security

15th International Conference, FC 2011
Gros Islet, St. Lucia, February 28 - March 4, 2011
Revised Selected Papers

Volume Editor

George Danezis
Microsoft Research Cambridge
Roger Needham Building
7 J J Thomson Avenue, Cambridge CB3 0FB, UK
E-mail: gdane@microsoft.com

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-27575-3 e-ISBN 978-3-642-27576-0
DOI 10.1007/978-3-642-27576-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011944281

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

© 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 15th International conference on Financial Cryptography and Data Security, held at the Bay Gardens Beach Resort, St. Lucia, February 28–March 4, 2011.

Financial cryptography and data security (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 26 papers and a panel on “The Future of Banking Security and Financial Transactions for the 21st Century.” The conference was opened by Jolyon Clulow, from Tesco Bank, with a keynote address on “What I Learnt When Trying to Build a Bank” and a closing talk by Markus Jakobsson from PayPal on “Why Mobile Security Is Not Like Traditional Security.”

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 56 full-length and 9 short submission. Each submission received at least three reviews from members of the Program Committee or outside experts – the vast majority of paper received four reviews. A further week-long discussion led to the selection of 16 full-length papers and 10 submissions as short papers to be included in the final program, on the basis of excellence, novelty and interest to the FC community.

The overall acceptance rate for full papers was 28%, while 40% of submissions were accepted at least as a short paper. The acceptance rate for full papers places FC in league with other competitive venues in computer security and cryptography. Yet, the generous time given to short papers ensures new ideas and promising work in progress have an opportunity to be heard.

This conference was made possible through the dedicated work of our General Chair, Steven Murdoch from the University of Cambridge, and our Local Arrangements Chair, Fabian Monrose from the University of North Carolina at Chapel Hill. The Program Chair would like to thank especially the Program Committee members and external reviewers for their expertise and dedication, both for selecting papers for the program as well as 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 due to the generosity of our sponsors.

Organization

The 15th International conference on Financial Cryptography and Data Security (FC 2011) was organized by the International Financial Cryptography Association (IFCA).

Organizers

General Chair

Steven Murdoch University of Cambridge, UK

Local Arrangements Chair

Fabian Monrose University of North Carolina Chapel Hill, USA

Program Chair

George Danezis Microsoft Research, UK

Program Committee

Ross Anderson	University of Cambridge, UK
Tuomas Aura	Helsinki University of Technology, Finland
Lucas Ballard	Google, USA
Adam Barth	UC Berkeley, USA
Elisa Bertino	Purdue University, USA
Kevin Butler	University of Oregon, USA
Srdjan Capkun	ETH Zurich, Switzerland
Veronique Cortier	CNRS / LORIA, France
Ernesto Damiani	University of Milan, Italy
Claudia Diaz	K.U. Leuven, Belgium
Roger Dingledine	The Tor Project, USA
Orr Dunkelman	Weizmann Institute of Science, Israel
Simone Fisher-Hubner	Karlstad University, Sweden
Craig Gentry	IBM T.J. Watson Research Center, USA
Dieter Gollmann	Technische Universität Harburg, Germany
Rachel Greenstadt	Drexel University, USA
Jean-Pierre Hubaux	Ecole Polytechnique Federale de Lausanne, Switzerland
Markus Jakobsson	Indiana University, USA
Jaeyeon Jung	Intel Research, USA
Stefan Katzenbeisser	Technische Universität Darmstadt, Germany
Angelos Keromytis	Columbia University, USA

Arjen Lenstra	Ecole Polytechnique Federale de Lausanne, Switzerland
Helger Lipmaa	Cybernetica AS, Estonia
Evangelos Markatos	FORTH, Greece
David Molnar	Microsoft Research, USA
Tyler Moore	Harvard University, USA
David Naccache	Ecole normale superieure, France
Thomas Ristenpart	University of Wisconsin, USA
Peter Ryan	Universite du Luxembourg, Luxembourg
Ahmad-Reza Sadeghi	Ruhr-University Bochum, Germany
Rei Safavi-Naini	University of Calgary, Canada
Nigel Smart	University of Bristol, UK
Jessica Staddon	Google, USA
Angelos Stavrou	George Mason University, USA
Paul Syverson	Naval Research Laboratory, USA
Nicholas Weaver	International Computer Science Institute, USA
Moti Yung	Google, USA

External Reviewers

Sadia Afroz	Seda Guerses	Qun Ni
Mina Askari	James Heather	Onur Ozen
Mira Belenkiy	Hans Hedbom	Daniel Page
Josh Benaloh	Mathias Humbert	Aanjhan Ranganathan
Stefan Berthold	Murtuza Jadliwala	Joel Reardon
Igor Bilogrevic	Dimitar Jetchev	Christian Rechberger
Joppe Bos	Ghassan Karamé	Alfredo Rial
Christina Brzuska	Emilia Kasper	Eleanor Rieffel
Dario Catalano	Dalia Khader	Mark Ryan
Liqun Chen	Michael Kirkpatrick	Nashad Safa
Richard Chow	Lara Letaw	Juraj Sarinay
Daniel Colascione	Harshana Liyanage	Thomas Schneider
Jean-Sebastien Coron	Hans Loehr	Steffen Schulz
Boris Danev	Roel Maes	Ben Smyth
Maria Dubovitskaya	Claudio Marforio	Tomas Toft
Ruchith Fernando	Catherine Meadows	Ashraful Tuhin
Aurelien Francillon	Mohamed Nabeel	Zhe Xia
Julien Freudiger	Kris Gagne	Davide Zanetti
Georg Fuchsbauer	Martin Narayan	Ge Zhang

Sponsors

Gold	Office of Naval Research Global
Silver	Research in Motion
Bronze	East Caribbean Financial Holding
	Google
In Kind	Lime
	WorldPay
	Financial Services Technology Consortium BITS

Table of Contents

Finacial Cryptography and Data Security (FC 2011)

Collective Exposure: Peer Effects in Voluntary Disclosure of Personal Data	1
<i>Rainer Böhme and Stefanie Pöttsch</i>	
It's All about the Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice	16
<i>Nicolas Christin, Serge Egelman, Timothy Vidas, and Jens Grossklags</i>	
Evaluating the Privacy Risk of Location-Based Services	31
<i>Julien Freudiger, Reza Shokri, and Jean-Pierre Hubaux</i>	
Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance	47
<i>Jeremy Clark and Urs Hengartner</i>	
Malice versus AN.ON: Possible Risks of Missing Replay and Integrity Protection	62
<i>Benedikt Westermann and Dogan Kesdogan</i>	
Absolute Pwnage: A Short Paper about the Security Risks of Remote Administration Tools	77
<i>Jay Novak, Jonathan Stribley, Kenneth Meagher, and J. Alex Halderman</i>	
A Protocol for Anonymously Establishing Digital Provenance in Reseller Chains (Short Paper)	85
<i>Ben Palmer, Kris Bubendorfer, and Ian Welch</i>	
Impeding Individual User Profiling in Shopper Loyalty Programs.....	93
<i>Philip Marquardt, David Dagon, and Patrick Traynor</i>	
Beyond Risk-Based Access Control: Towards Incentive-Based Access Control	102
<i>Debin Liu, Ninghui Li, XiaoFeng Wang, and L. Jean Camp</i>	
Authenticated Key Exchange under Bad Randomness	113
<i>Guomin Yang, Shanshan Duan, Duncan S. Wong, Chik How Tan, and Huaxiong Wang</i>	

Oblivious Outsourced Storage with Delegation	127
<i>Martin Franz, Peter Williams, Bogdan Carbunar, Stefan Katzenbeisser, Andreas Peter, Radu Sion, and Miroslava Sotakova</i>	
Homomorphic Signatures for Digital Photographs	141
<i>Rob Johnson, Leif Walsh, and Michael Lamb</i>	
Revisiting the Computational Practicality of Private Information Retrieval	158
<i>Femi Olumofin and Ian Goldberg</i>	
Optimal One Round Almost Perfectly Secure Message Transmission (Short Paper)	173
<i>Mohammed Ashraful Alam Tuhin and Reihaneh Safavi-Naini</i>	
A New Approach towards Coercion-Resistant Remote E-Voting in Linear Time	182
<i>Oliver Spycher, Reto Koenig, Rolf Haenni, and Michael Schl�pfer</i>	
An Attack on PUF-Based Session Key Exchange and a Hardware-Based Countermeasure: Erasable PUFs	190
<i>Ulrich R�hrmair, Christian Jaeger, and Michael Algasinger</i>	
Peeling Away Layers of an RFID Security System	205
<i>Henryk Pl�t� and Karsten Nohl</i>	
Might Financial Cryptography Kill Financial Innovation? – The Curious Case of EMV	220
<i>Ross Anderson, Mike Bond, Omar Choudary, Steven J. Murdoch, and Frank Stajano</i>	
hPIN/hTAN: A Lightweight and Low-Cost E-Banking Solution against Untrusted Computers	235
<i>Shujun Li, Ahmad-Reza Sadeghi, S�ren Heisrath, Roland Schmitz, and Junaid Jameel Ahmad</i>	
Certified Lies: Detecting and Defeating Government Interception Attacks against SSL (Short Paper)	250
<i>Christopher Soghoian and Sid Stamm</i>	
Proximax: Measurement-Driven Proxy Dissemination (Short Paper)	260
<i>Damon McCoy, Jose Andre Morales, and Kirill Levchenko</i>	
BNymble: More Anonymous Blacklisting at Almost No Cost (A Short Paper)	268
<i>Peter Lofgren and Nicholas Hopper</i>	

Towards Secure Bioinformatics Services (Short Paper)	276
<i>Martin Franz, Björn Deiseroth, Kay Hamacher, Somesh Jha,</i> <i>Stefen Katzenbeisser, and Heike Schröder</i>	
Quo Vadis? A Study of the Evolution of Input Validation Vulnerabilities in Web Applications	284
<i>Theodoor Scholte, Davide Balzarotti, and Engin Kirda</i>	
Re-evaluating the Wisdom of Crowds in Assessing Web Security	299
<i>Pern Hui Chia and Svein Johan Knapskog</i>	
Mercury: Recovering Forgotten Passwords Using Personal Devices	315
<i>Mohammad Mannan, David Barrera, Carson D. Brown,</i> <i>David Lie, and Paul C. van Oorschot</i>	
Author Index	331