

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

Josep Domingo-Ferrer Joachim Posegga
Daniel Schreckling (Eds.)

Smart Card Research and Advanced Applications

7th IFIP WG 8.8/11.2 International Conference, CARDIS 2006
Tarragona, Spain, April 19-21, 2006
Proceedings

Volume Editors

Josep Domingo-Ferrer

Universitat Rovira i Virgili, Departament d'Enginyeria Informàtica i Matemàtiques,
Av. Paisos Catalans 26, 43007 Tarragona, Catalonia, Spain

E-mail: josep.domingo@urv.net

Joachim Posegga

Daniel Schreckling

Universität Hamburg

Arbeitsbereich Sicherheit in Verteilten Systemen (SVS)

Fachbereich Informatik

Vogt-Kölln-Str. 30, 22527 Hamburg, Germany

E-mail: {posegga,schreckling}@informatik.uni-hamburg.de

Library of Congress Control Number: 2006922624

CR Subject Classification (1998): E.3, K.6.5, C.3, D.4.6, K.4.1, E.4, C.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-540-33311-8 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-33311-1 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

© 2006 IFIP International Federation for Information Processing, Hofstr. 3, A-2361 Laxenburg, Austria
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11733447 06/3142 5 4 3 2 1 0

Preface

Smart cards are an established security research area with a very unique property: it integrates numerous subfields of IT Security, which often appear scattered and only loosely connected. Smart card research unites them by providing a common goal: advancing the state of the art of designing and deploying small tokens to increase the security in Information Technology.

CARDIS has a tradition of more than one decade, and has established itself as the premier conference for research results in smart card technology. As smart card research is unique, so is CARDIS; the conference successfully attracts academic and industrial researchers without compromising in either way. CARDIS accommodates applied research results as well as theoretical contributions that might or might not become practically relevant. The key to making such a mixture attractive to both academia and industry is simple: quality of contributions and relevance to the overall subject.

This year's CARDIS made it easy to continue this tradition: we received 76 papers, nearly all of them relevant to the focus of CARDIS and presenting high-quality research results. The Program Committee worked hard on selecting the best 25 papers to be presented at the conference.

We are very grateful to the members of the Program Committee and the additional referees for generously spending their time on the difficult task of assessing the value of submitted papers. Daniel Schreckling provided invaluable assistance in handling submissions, managing review reports and editing the proceedings. The assistance of Jordi Castellà in handling practical aspects of the conference preparation is also greatly appreciated.

Financial support by the following organizations is gratefully acknowledged: IEEE Spain Section, Rovira i Virgili University (ETSE, DEIM) and Spain's Ministry of Science and Education.

Finally, we would also like to thank all those who have submitted papers to IFIP CARDIS 2006, and encourage them to stay with CARDIS in subsequent years. The authors of the accepted papers certainly deserve the highest respect, since it is they who wrote this book.

January 2006

Josep Domingo-Ferrer
Joachim Posegga

Organization

CARDIS 2006 was organized by the Universitat Rovira i Virgili, Catalonia, Spain.

Conference Organization

Conference General Chair

Josep Domingo-Ferrer
(Universitat Rovira i Virgili,
Catalonia, Spain)

Program Committee Chair

Joachim Posegga
(University of Hamburg, Germany)

Advisory Committee

José A. Delgado-Penín
(IEEE Spain Section Chair, Spain)

Program Committee

Boris Balacheff
(Hewlett-Packard Labs, UK)

Bertrand du Castel
(Axalto, USA)

Josep Domingo-Ferrer
(Universitat Rovira i Virgili,
Catalonia, Spain)

Dieter Gollmann
(TU Hamburg-Harburg, Germany)

Louis Guillou
(France Télécom, France)

Pieter Hartel
(University of Twente, Netherlands)

Peter Honeyman
(University of Michigan, USA)

Dirk Husemann
(IBM Research, Switzerland)

Eduardo de Jong
(Sun Microsystems, USA)

Jean-Louis Lanet
(Gemplus Labs, France)

Javier Lopez
(University of Malaga, Spain)

Bernd Meyer
(Siemens AG, Germany)

Mike Montgomery
(Axalto, USA)

Pierre Paradinas
(CNAM, France)

Jean-Jacques Quisquater
(Université Catholique de Louvain,
Belgium)

Francesc Sebé
(Universitat Rovira i Virgili,
Catalonia, Spain)

François-Xavier Standaert
(Université Catholique de Louvain,
Belgium)

Jean-Jacques Vandewalle
(Gemplus Labs, France)

Additional Referees

A. Ali	J.B. Fischer	A. Martínez-Ballesté
V. Benjumea	C. Fontaine	A. Muñoz E. Peeters
D. Bolzoni	P. Girard	H.C. Pöhls
E. Brier	B. Gonzalvo	E. Prouff
R. Brinkman	D. Gross-Amblard	R. Roman
I. Buhan	H. Handschuh	A. Saptawijaya
M. Casassa-Mont	K. Harrisson	D. Schreckling
J. Castellà-Roca	Z. HuanGuo	J. Seedorf
J. Cederquist	M. Johns	D. Simplot-Ryl
L. Chen	M. Joye	A. Solanas
M. Ciet	A. Kargl	A. Viejo-Galicia
R. Corin	K. Lu	L.Y. Wei
M. Czenko	F. Macé	A. Zych
M. Dekker	A. Maña	
G.M. de Dormale	W. Mao	

Table of Contents

Smart Card Applications

Design, Installation and Execution of a Security Agent for Mobile Stations

*William G. Sirett, John A. MacDonald, Keith Mayes,
Konstantinos Markantonakis* 1

Towards a Secure and Practical Multifunctional Smart Card

Idir Bakdi 16

Implementing Cryptography on TFT Technology for Secure Display Applications

Petros Oikonomakos, Jacques Fournier, Simon Moore 32

A Smart Card-Based Mental Poker System

Jordi Castellà-Roca, Josep Domingo-Ferrer, Francesc Sebé 48

A Smart Card Solution for Access Control and Trust Management for Nomadic Users

*Daniel Díaz Sánchez, Andrés Marín Lopez,
Florina Almenárez Mendoza* 62

Smart Cards and Residential Gateways: Improving OSGi Services with Java Cards

*Juan Jesús Sánchez Sánchez, Daniel Díaz Sánchez,
José Alberto Vigo Segura, Natividad Martínez Madrid,
Ralf Seepold* 78

Zero Footprint Secure Internet Authentication Using Network Smart Card

Asad M. Ali 91

An Optimistic NBAC-Based Fair Exchange Method for Arbitrary Items

Masayuki Terada, Kensaku Mori, Sadayuki Hongo 105

Side Channel Attacks

Generic Cryptanalysis of Combined Countermeasures with Randomized BSD Representations

Tae Hyun Kim, Dong-Guk Han, Katsuyuki Okeya, Jongin Lim 119

Amplifying Side-Channel Attacks with Techniques from Block Cipher Cryptanalysis <i>Raphael C.-W. Phan, Sung-Ming Yen</i>	135
---	-----

Power Analysis to ECC Using Differential Power Between Multiplication and Squaring <i>Toru Akishita, Tsuyoshi Takagi</i>	151
---	-----

Smart Card Networking

Designing Smartcards for Emerging Wireless Networks <i>Pascal Urien, Mesmin Dandjinou</i>	165
--	-----

Smartcard Firewalls Revisited <i>Henrich C. Pöhls, Joachim Posegga</i>	179
---	-----

Multi-stage Packet Filtering in Network Smart Cards <i>HongQian Karen Lu</i>	192
---	-----

Cryptographic Protocols

Anonymous Authentication with Optional Shared Anonymity Revocation and Linkability <i>Martin Schaffer, Peter Schartner</i>	206
---	-----

SEA: A Scalable Encryption Algorithm for Small Embedded Applications <i>François-Xavier Standaert, Gilles Piret, Neil Gershenfeld, Jean-Jacques Quisquater</i>	222
---	-----

Low-Cost Cryptography for Privacy in RFID Systems <i>Benoît Calmels, Sébastien Canard, Marc Girault, Hervé Sibert</i>	237
--	-----

Optimal Use of Montgomery Multiplication on Smart Cards <i>Arnaud Boscher, Robert Naciri</i>	252
---	-----

Off-Line Group Signatures with Smart Cards <i>Jean-Bernard Fischer, Emmanuel Prouff</i>	263
--	-----

RFID Security

Analysis of Power Constraints for Cryptographic Algorithms in Mid-Cost RFID Tags <i>Tobias Lohmann, Matthias Schneider, Christoph Ruland</i>	278
---	-----

Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags <i>Claude Castelluccia, Gildas Avoine</i>	289
MARP: Mobile Agent for RFID Privacy Protection <i>Soo-Cheol Kim, Sang-Soo Yeo, Sung Kwon Kim</i>	300

Formal Methods

Certifying Native Java Card API by Formal Refinement <i>Quang-Huy Nguyen, Boutheina Chetali</i>	313
A Low-Footprint Java-to-Native Compilation Scheme Using Formal Methods <i>Alexandre Courbot, Mariela Pavlova, Gilles Grimaud, Jean-Jacques Vandewalle</i>	329
Automatic Test Generation on a (U)SIM Smart Card <i>Céline Bigot, Alain Faivre, Christophe Gaston, Julien Simon</i>	345
Author Index	359