Lecture Notes in Computer Science 3928

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

Editorial Board

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

Springer

Volume Editors

Josep Domingo-Ferrer
Universitat Rovira i Virgili, Departament d'Enginyeria Informatica i Matematiques,
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

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

Table of Contents

Smart Card Applications

Side Channel Attacks

Smart Card Networking

Cryptographic Protocols

RFID Security

Formal Methods