Lecture Notes in Computer Science 6035

Dieter Gollmann Jean-Louis Lanet
Julien Iguchi-Cartigny (Eds.)

Smart Card Research and Advanced Application

9th IFIP WG 8.8/11.2 International Conference
CARDIS 2010
Passau, Germany, April 14-16, 2010
Proceedings

Springer

Volume Editors

Dieter Gollmann
Hamburg University of Technology
Institute for Security in Distributed Applications
21071 Hamburg, Germany
E-mail: diego@tu-harburg.de

Jean-Louis Lanet
Julien Iguchi-Cartigny
University of Limoges, XLIM
87000 Limoges, France
E-mail: {jean-louis.lanet, julien.cartigny}@unilim.fr

Library of Congress Control Number: 2010924121

CR Subject Classification (1998): E.3, C.2, K.6.5, D.4.6, H.4, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-12509-3 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-12509-6 Springer Berlin Heidelberg New York

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

These proceedings contain the papers selected for presentation at CARDIS 2010, the 9th IFIP Conference on Smart Card Research and Advanced Application hosted by the Institute of IT-Security and Security Law (ISL) of the University of Passau, Germany. CARDIS is organized by IFIP Working Groups WG 8.8 and WG 11.2. Since 1994, CARDIS has been the foremost international conference dedicated to smart card research and applications. Every second year leading researchers and practitioners meet to present new ideas and discuss recent developments in smart card technologies.

The fast evolution in the field of information security requires adequate means for representing the user in human–machine interactions. Smart cards, and by extension smart devices with their processing power and their direct association with the user, are considered the first choice for this purpose. A wide range of areas including hardware design, operating systems, systems modelling, cryptography, and distributed systems contribute to this fast-growing technology.

The submissions to CARDIS were reviewed by at least three members of the Program Committee, followed by a two-week discussion phase held electronically, where committee members could comment on all papers and all reviews. Finally, 16 papers were selected for presentation at CARDIS.

There are many volunteers who offered their time and energy to put together the symposium and who deserve our acknowledgment. We want to thank all the members of the Program Committee and the external reviewers for their hard work in evaluating and discussing the submissions. We are also very grateful to Joachim Posegga, the General Chair of CARDIS 2010, and his team for the local conference management.

Last, but certainly not least, our thanks go to all the authors who submitted papers and all the attendees. We hope you find the proceedings stimulating.

March 2010

Jean-Louis Lanet
Dieter Gollmann

Organization

General Chair

Joachim Posegga	University of Passau, Germany

Program Chairs

Jean-Louis Lanet	Université de Limoges, France
Dieter Gollmann	Hamburg University of Technology, Germany

Program Committee

Liqun Chen	Hewlett-Packard, UK
Christophe Clavier	XLIM, France
Wolfgang Effing	Giesecke & Devrient, Germany
Benoit Feix	Inside Contactless, France
Benedikt Gierlichs	COSIC Leuven, Belgium
Louis Goubin	Université de Versailles, France
Gilles Grimaud	Université de Lille, France
Marc Joye	Technicolor, France
Josef Langer	CDE Hagenberg, Austria
Cédric Lauradoux	INRIA Rhône-Alpes, Equipe SWING, France
Kostas Markantonakis	Royal Holloway, UK
Vaclav Matyas	Masaryk University, Czech Republic
Bernd Meyer	Siemens AG, Germany
Wojciech Mostowski	University of Nijmegen, The Netherlands
Pierre Paradinas	INRIA, France
Emmanuel Prouff	Oberthur Technology, France
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
Jean Marc Robert	Ecole de technologie supérieure Montréal, Canada
Jean-Jacques Vandewalle	Gemalto, France

Additional Reviewers

Lejla Batina
Samia Bouzefrane
Guillaume Dabosville
Elke De Mulder
Simon Duquennoy
Hermann Drexler
Junfeng Fan
Lars Hoffmann
Jan Krhovjak
François-Xavier Marseille
Nathalie Mitton
Kenny Paterson

Michael Roland
Martin Seysen
Petr Svenda
Hugues Thiebeauld
Vincent Verneuil
Colin Walter
Marc Witteman

Local Organization

Arne Bilzhause
Sigline Böck
Bastian Braun
Agnes Grützner
Peter Häring
Daniel Hausknecht
Michael Kaeufl
Markus Karwe
Guido Lenk-Blochowitz
Simon Niechzial
Henrich Pöhls
Daniel Schreckling
Martin Steininger
Marita Ward

Table of Contents

Mathematical Algorithms

Side Channel Analysis

Systems

Logical Attacks

Fault Analysis

Privacy