Lecture Notes in Computer Science **10146**

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

More information about this series at http://www.springer.com/series/7410

Kerstin Lemke-Rust · Michael Tunstall (Eds.)

Smart Card Research and Advanced Applications

15th International Conference, CARDIS 2016 Cannes, France, November 7–9, 2016 Revised Selected Papers

Springer

Editors
Kerstin Lemke-Rust
Bonn-Rhein-Sieg University
of Applied Sciences
St. Augustin
Germany

Michael Tunstall
Cryptography Research
San Francisco, CA
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-54668-1 ISBN 978-3-319-54669-8 (eBook)
DOI 10.1007/978-3-319-54669-8

Library of Congress Control Number: 2017932792

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

These proceedings contain the papers selected for presentation at the 15th International Conference on Smart Card Research and Advanced Applications (CARDIS 2016), held during November 7–9 and application of smart. The conference was organized by EURECOM and held at the Hôtel Barrière Le Gray d'Albion.

CARDIS has provided a forum for presenting exceptional research on smart cards and related technologies since 1994. Smart cards play an important role in our day-to-day lives, from bank cards to GSM SIMs, and security is vital to keep these systems functioning correctly. The CARDIS conference gathers researchers and technologists who focus on all aspects of the design, development, deployment, evaluation, and application of smart cards and secure elements in secure platforms or systems. The technology used in smart cards, and hence the attack vectors, are expanding to other areas, such as TPMs, HSMs, mobile phones, and the Internet of Things. It is, therefore, more important than ever that we understand how smart cards, and related systems, can be secured.

This year, CARDIS received 29 papers from 17 countries. Each paper was reviewed by at least three independent reviewers. The selection of 15 papers to fill the technical program was accomplished based on 114 written reviews. This task was performed by the 30 members of the Program Committee with the help of 38 external reviewers. The technical program also featured three invited talks. The first invited speaker, Eric Vétillard, from Prove & Run, France, presented "Three Views on IoT Security"; the second speaker, Ventzislav Nikov, from NXP Semiconductors, Belgium, presented "Security Outside the Black-Box Model: Challenges and Countermeasures"; and the third speaker, David Oswald, from the University of Birmingham, UK, presented "Breaking Automotive Remote Keyless Entry Systems, or: Why Your Car Is not a Safe Box."

We would like to thank the general chair, Aurélien Francillon, and the local Organizing Committee chairs, Ludovic Apvrille and Florian Lugou. We would also like to thank the Program Committee and the external reviewers for their thorough work, which enabled the technical program to achieve such a high quality, and the Steering Committee for giving us the opportunity to serve as program chairs at such a prestigious conference. The financial support of all the sponsors was highly appreciated and greatly facilitated the organization of the conference. In particular, we would like to thank the gold sponsors: NXP Semiconductors, Labex UCN and the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Furthermore, we would like to thank the authors who submitted their work to CARDIS 2016, without whom the conference would not have been possible.

January 2017

Keratin Lemke-Rust
Michael Tunstall

CARDIS 2016

15th International Conference on Smart Card Research and Advanced Applications

Cannes, France
November 7–9, 2016

General Chair

Aurélien Francillon	EURECOM, France

Local Arrangements Chair

Ludovic Apvrille	Telecom ParisTech, France

Web Chair

Florian Lugou	Telecom ParisTech, France

Program Chairs

Kerstin Lemke-Rust	Bonn-Rhein-Sieg University of Applied Sciences, Germany
Michael Tunstall	Cryptography Research, USA

Program Committee

Guillaume Barbu	Oberthur Technologies, France
Lejla Batina	Radboud University Nijmegen, The Netherlands
Guido Bertoni	ST Microelectronics, Italy
Elke De Mulder	Cryptography Research, USA
Hermann Drexler	Giesecke & Devrient, Germany
Thomas Eisenbarth	Worcester Polytechnic Institute, USA
Wieland Fischer	Infineon Technologies, Germany
Benedikt Gierlichs	Katholieke Universiteit Leuven, Belgium
Christophe Giraud	Oberthur Technologies, France
Cezary Glowacz	T-Systems, Germany
Sylvain Guilley	GET/ENST and CNRS/LTCI, France
Tim Güneysu	University of Bremen and DFKI, Germany
Johann Heyszl	Fraunhofer AISEC, Germany
Naofumi Homma	Tohoku University, Japan

Yuichi Komano	Toshiba Corporation, Japan
Jean-Louis Lanet	Inria-RBA, France
Roel Maes	Intrinsic-ID, The Netherlands
Stefan Mangard	University of Graz, Austria
Keith Mayes	Royal Holloway University of London, UK
Marcel Medwed	NXP Semiconductors, The Netherlands
Amir Moradi	Ruhr University Bochum, Germany
Svetla Nikova	Katholieke Universiteit Leuven, Belgium
Pedro Peris-Lopez	Carlos III University of Madrid, Spain
Axel Poschmann	NXP Semiconductors, Germany
Emmanuel Prouff	Safran Identity & Security, France
Francesco Regazzoni	ALaRI–USI, Switzerland
Patrick Schaumont	Virginia Tech, USA
François-Xavier Standaert	Université Catholique de Louvain, Belgium
Takeshi Sugawara	Mitsubishi Electric Corp., Japan
Carolyn Whitnall	University of Bristol, UK

Steering Committee

Aurélien Francillon	EURECOM, France
Marc Joye	NXP Semiconductors, USA
Jean-Louis Lanet	University of Limoges, France
Stefan Mangard	University of Graz, Austria
Konstantinos Markantonakis	Royal Holloway University of London, UK
Amir Moradi	Ruhr University Bochum, Germany
Svetla Nikova	Katholieke Universiteit Leuven, Belgium
Pierre Paradinas	Inria and CNAM, France
Emmanuel Prouff	Safran Identity & Security, France
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
Vincent Rijmen	Katholieke Universiteit Leuven, Belgium
Pankaj Rohatgi	Cryptography Research, USA
François-Xavier Standaert	Université Catholique de Louvain, Belgium

Additional Reviewers

Florian Bache	Lukasz Chmielewski
Josep Balasch	Guillaume Dabosville
Sven Bauer	Thomas De Cnudde
Elif Bilge Kavun	Nicolas Debande
Joppe Bos	Hannes Gross
Martin Butkus	Annelie Heuser
Cong Chen	Thomas Korak
Eloi de Cherisey	Jake Longo Galea

Filippo Melzani
Shoei Nashimoto
Tobias Oder
Matheus Oliveira
Conor Patrick
Markus Peschina
Peter Pessl
Romain Poussier
Jürgen Pulkus
Joost Renes
Oscar Reparaz
Okan Seker
Victor Servant
Pascal Sasdrich
Ruggero Susella
Daisuke Suzuki
Rei Ueno
Felipe Valencia
Vincent Verneuil
Tobias Wagner
Erich Wenger
Ville Yli-Mäyry

Contents