Lecture Notes in Computer Science 11389

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

Begül Bilgin · Jean-Bernard Fischer (Eds.)

Smart Card Research and Advanced Applications

17th International Conference, CARDIS 2018 Montpellier, France, November 12–14, 2018 Revised Selected Papers

Springer

Editors

Begül Bilgin
Rambus - Cryptography Research
Rotterdam, Zuid-Holland, The Netherlands

KU Leuven
Leuven-Heverlee, Belgium

Jean-Bernard Fischer
Nagravision
Cheseaux-sur-Lausanne, Vaud, Switzerland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-15461-5 ISBN 978-3-030-15462-2 (eBook)
https://doi.org/10.1007/978-3-030-15462-2

Library of Congress Control Number: 2019933892

LNCS Sublibrary: SL4 – Security and Cryptology

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

Preface

These proceedings contain the papers selected for presentation at the 17th Smart Card Research and Advanced Applications Conference (CARDIS 2018), which was held in Montpellier, France, during November 12–14, 2018, and organized by the Montpellier Laboratory of Informatics, Robotics and Microelectronics (LIRMM).

Since 1994, CARDIS has provided a forum for experts from industry and academia to exchange ideas on the security of smart cards and related applications. The smart card object has been part of our daily life for so many years in the form of personal devices (banking cards, SIM cards, electronic IDs, etc.) that we do not remember a life without it. In relation to smart card security, the root of trust of embedded solutions is becoming key as Machine-to-Machine (M2M) and Internet of Things (IoT) applications are increasing massively. This increased exposure naturally widens the attack space, whether physical or logical, local or remote. It is more important than ever to understand how smart cards and other embedded devices can be secured by discussing all aspects of their design, development, deployment, evaluation, and application.

This year, CARDIS received 28 valid submissions from 12 countries. Each paper was double-blind reviewed by at least three independent reviewers. We selected 13 papers based on 102 written reviews from the 30 members of the Program Committee with the help of 35 external reviewers. The technical program also featured three invited talks: Frank Piessens from KU Leuven in Belgium presented "Security Specifications for the Hardware/Software Interface"; Benoit Feix from eshard in France presented "Exploiting a New Dimension in Side-Channel Analysis: Scatter on Symmetric and Asymmetric Embedded Cryptography"; and Wyseur Brecht from Nagravision in Switzerland presented "Challenges in Securing Industrial IoT and Critical Infrastructure." A free tutorial was held co-located with the conference: "Understanding Leakage Detection" organized by the REASSURE Consortium.

We would like to thank the general chair, Philippe Maurine, for the great venue and smooth operation of the conference. We would also like to express our gratitude to the Program Committee and the external reviewers for their thorough work, which enabled the technical program to be of such 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; we thank the sponsors: ANSSI, CNRS, Gemalto, Nagra-Kudelski, LETI-CEA, LIRMM, Rambus, STMicroelectronics, University of Montpellier. Last but not least, we would like to thank all the authors who submitted their work to CARDIS 2018.

January 2019

Begül Bilgin
Jean-Bernard Fischer

Organization

General Chair

Philippe Maurine	University of Montpellier, France

Program Chairs

Begül Bilgin	Rambus-Cryptography Research, The Netherlands and KU Leuven, Belgium
Jean-Bernard Fischer	Nagravision, Switzerland

Steering Committee

François-Xavier Standaert (Chair)	UC Louvain, Belgium
Thomas Eisenbarth	Worcester Polytechnic Institute, USA
Aurélien Francillon	EURECOM, France
Edouard de Jong	De Jong Frz. Holding BV
Marc Joye	NXP Semiconductors, USA
Konstantinos Markantonakis	Royal Holloway University of London, UK
Amir Moradi	Ruhr University Bochum, Germany
Svetla Nikova	KU Leuven, Belgium
Pierre Paradinas	Inria and CNAM, France
Jean-Jacques Quisquater	UC Louvain, Belgium
Francesco Regazzoni	University of Lugano, Switzerland
Yannick Teglia	Gemalto, France

Program Committee

Josep Balasch	KU Leuven, Belgium
Guillaume Barbu	IDEMIA, France
Alessandro Barenghi	Politecnico di Milano, Italy
Sonia Belaïd	CryptoExperts, France
Thomas De Cnudde	KU Leuven, Belgium
Jeroen Delvaux	Nanyang Technological University, Singapore
Thomas Eisenbarth	Universität zu Lübeck, Germany
Benoix Feix	eshard, France
Domenic Forte	University of Florida, USA
Aurélien Francillon	Eurecom, France
Elke De Mulder	Rambus-Cryptography Research, USA
Hannes Gross	TU Graz, Austria

Vincent Grosso	Radboud University, The Netherlands
Annelie Heuser	CNRS/IRISA, France
Marc Joye	NXP Semiconductors, USA
Kerstin Lemke-Rust	Bonn-Rhein-Sieg University, Germany
Roel Maes	Intrinsic ID, The Netherlands
Oliver Mischke	Infineon, Germany
Amir Moradi	Ruhr University Bochum, Germany
Debdeep Mukhopadhyay	IIT Kharagpur, India
Axel Y. Poschmann	DarkMatter, UAE
Emmanuel Prouff	ANSSI, France
Francesco Regazoni	ALaRi, Switzerland
Kazuo Sakiyama	University of Electro-Communications, Japan
Erkay Savaş	Sabanci University, Turkey
Tobias Schneider	UC Louvain, Belgium
Yannick Teglia	Gemalto, France
Yuval Yarom	University of Adelaide, and Data61, Australia
Carolyn Whitnall	University of Bristol, UK
Marc Witteman	Riscure, The Netherlands

Additional Reviewers

Alberto Battistello
Ryad Benadjila
Shivam Bhasin
Manuel Bluhm
Olivier Bronchain
Giovanni Camurati
Nicolas Debande
David El-Baze
Berk Gulmezoglu
Christoph Herbst
James Howe
Malika Izabachene
Angshuman Karmakar
Elif Bilge Kavun
Albert Levi
Marco Martinoli
Ahmet Can Mert
Marius Muench
Erdinc Ozturk
Jungmin Park
Sikhar Patranabis
Thomas Pöppelmann
Bastian Richter
Debapriya Basu Roy
Okan Seker
Rémi Strullu
Shahin Tajik
Benjamin Timon
Lucille Tordella
Rei Ueno
Aurelien Vasselle
Nikita Veshchikov
Junwei Wang
Felix Wegener
Jan Wichelmann

Contents