Lecture Notes in Computer Science 11833

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

Sonia Belaïd · Tim Güneysu (Eds.)

Smart Card Research and Advanced Applications

18th International Conference, CARDIS 2019
Prague, Czech Republic, November 11–13, 2019
Revised Selected Papers

Springer

Editors
Sonia Belaïd
CryptoExperts
Paris, France

Tim Güneysu
Ruhr-Universität Bochum
Bochum, Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-42067-3 ISBN 978-3-030-42068-0 (eBook)
https://doi.org/10.1007/978-3-030-42068-0

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 18th International Conference on Smart Card Research and Advanced Applications (CARDIS 2019), held in Prague, Czech Republic, during November 11–13, 2019. The conference was organized by the Faculty of Information Technology of the Czech Technical University in Prague, Czech Republic.

CARDIS provides a space for security experts from industry and academia to exchange ideas on security of smart cards and related applications. Those objects have been part of our daily life for years: banking and SIM cards, electronic passports, etc. But the world is constantly changing; a secure element, such as smart cards, is now being implemented in many cases, for example as a hardware root of trust for larger systems. As such, smartcard security and core ingredients such as applied cryptography is a key enabler for the security of the entire system. At the same time, and with the growing use of smartcard technology, the attack surface is increasing, from physical attacks to logical attacks, from local attacks to remote attacks, and more recently combined attacks. It is more important than ever that we understand how smart cards and related systems, can be secured.

This year, CARDIS received 31 papers from a large number of international countries. Each paper was reviewed by three independent reviewers. The selection of 15 papers to fill the technical program was accomplished based on 142 written reviews. This task was performed by the 31 members of the Program Committee with the help of 28 external reviewers. The technical program also featured two invited talks. The first invited speaker, Peter Schwabe (Radboud University in Nijmegen, The Netherlands), presented "Post-quantum crypto on ARM Cortex-M" and the second speaker, Gilles Barthe (Max-Planck Institute in Bochum, Germany, and IMDEA Software Institute, Spain), presented "Formal Verification of Side-Channel Resistance." We would like to thank the general chair, Martin Novotný, for the great venue and smooth operation of the conference.

We would also like to thank the Program Committee and the external reviewers for their thorough work, which enabled the technical program to be of high quality, as well as 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 would like to thank the sponsors Thales, Infineon, Rambus, PQSHIELD, NewAE, Riscure NAGRA and FortifyIQ, CryptoExperts, ima, and KAOS for their support and collaboration. Furthermore, we would like to thank the authors who submitted their work to CARDIS 2019, without whom the conference would not have been possible.

January 2020

Sonia Belaïd
Tim Güneysu

Organization

Program Committee

Josep Balasch	Katholieke Universiteit Leuven, Belgium
Alessandro Barenghi	Politecnico di Milano, Italy
Sonia Belaïd	CryptoExperts, France
Begül Bilgin	Cryptography Research, USA
Thomas De Cnudde	Katholieke Universiteit Leuven, Belgium
Elke De Mulder	Cryptography Research, USA
Thomas Eisenbarth	WPI, USA
Junfeng Fan	Open Security Research, The Netherlands
Jean-Bernard Fischer	NagraVision, Switzerland
Domenic Forte	University of Florida, USA
Dahmun Goudarzi	PQShield, UK
Daniel Gruss	Institute for Applied Information Processing and Communications, Graz University of Technology, Austria
Tim Güneysu	Ruhr-Universität Bochum and DFKI, Germany
Annelie Heuser	CNRS, IRISA, France
Kerstin Lemke-Rust	Bonn-Rhein-Sieg University of Applied Sciences, Germany
Roel Maes	Intrinsic ID, USA
Amir Moradi	Ruhr-Universität Bochum, Germany
Debdeep Mukhopadhyay	IIT Kharagpur, India
Colin O'Flynn	NewAE Technology Inc., Canada
Axel Poschmann	xen1thLabs, UAE
Emmanuel Prouff	ANSSI, France
Thomas Pöppelmann	Infineon Technologies AG, Germany
Francesco Regazzoni	ALaRI – USI, Switzerland
Thomas Roche	NinjaLab, France
Kazuo Sakiyama	The University of Electro-Communications, Japan
Erkay Savas	Sabanci University, Turkey
Tobias Schneider	NXP Semiconductors, The Netherlands
Peter Schwabe	Radboud University, The Netherlands
Carolyn Whitnall	University of Bristol, UK
Yuval Yarom	The University of Adelaide and Data61/CSIRO, Australia
Rina Zeitoun	IDEMIA, France

Additional Reviewers

Andreeva, Elena
Barbu, Guillaume
Bermudo Mera, Jose Maria
Bouffard, Guillaume
Bronchain, Olivier
Cao, Yang
Costa Massolino, Pedro Maat
Cuong, Bien
De Meyer, Lauren
Fritzmann, Tim
Fritzsch, Clemens
Giner, Lukas
Gonzalez, Ruben
Hara-Azumi, Yuko
Kannwischer, Matthias
Kavun, Elif Bilge
Li, Yang
Maniatakos, Mihalis
Pelletier, Hervé
Rebeiro, Chester
Richter, Bastian
Saha, Sayandeep
Seker, Okan
Tunstall, Mike
Villegas, Karine
Wood, Tim
Yao, Yuan

Contents