Call for Papers

CARDIS has been the venue for security experts from industry and academia to exchange on security of smart cards and related applications since 1994. Smart cards play an increasingly important role in our day-to-day life through their use in banking cards, SIM cards, electronic passports, and IoT devices. It is thus naturally of utmost importance to understand their security features and to develop sound protocols and countermeasures while keeping reasonable performance. In this respect, CARDIS aims to gather security experts from industry, academia, and standardization bodies to make steps forward in the field of embedded security.

The 19th edition of CARDIS is organized by the Institute for IT Security of the Universität zu Lübeck, Germany. The conference website is accessible at https://cardis2020.its.uni-luebeck.de/

The program committee is seeking original papers on the design, development, deployment, evaluation, penetration testing and application of smart cards and secure embedded systems. Submissions across a broad range of the development phase are encouraged, from exploratory research and proof of-concept studies to practical applications and deployment. Topics of interest include, but are not limited to:

Security and applications of:

- Smart cards: identification, access control, pay TV
- IoT devices: automotive, medical, mobile payment, mobile connected devices
- Trusted computing: mobile TPM, Trusted Execution Environments
- Embedded systems: operating systems, memory, virtual machines

Attacks and countermeasures:

- Side-channel (timing, power, cache) attacks and countermeasures
- Fault and combined attacks and countermeasures
- Reverse engineering, (anti-)cloning, (anti-)tempering, (anti-)counterfeiting

Cryptographic implementations of:

- Lightweight cryptographic algorithms
- Post-quantum cryptographic algorithms
- Random number generators, PUFs

Tools:

- Automated analysis
- Formal verification and secure design
- Deep learning analysis

Paper Submission

Authors are invited to submit papers electronically in PDF format using the submission form available on https://easychair.org/conferences/?conf=cardis2020. Submissions must be original, unpublished, anonymous and not submitted to journals or other conferences with proceedings. Submissions must be written in English and should be at most 15 pages in total. Papers not meeting these guidelines risk rejection without consideration. All submissions will be blind-refereed. Submission implies the willingness of at least one of the authors to register and present the paper. The proceedings will be published in the Springer Lecture Notes in Computer Science (LNCS) series. Both submissions and accepted papers must follow the LNCS default author instructions accessible on the Springer webpage: https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines.

Important Dates

- Submission deadline: ~~**July 3, 2020**~~ **July 14, 2020**
- Notification of acceptance: September 4, 2020
- Pre-proceedings paper due: October 4, 2020
- Conference dates: **November 18-19, 2020**
- Final version due: December 6, 2020

All deadlines are 23:59:59 Anywhere on Earth (AoE).

Organization

General Chair: Thomas Eisenbarth, Universität zu Lübeck, DE
Program Chairs: Pierre-Yvan Liardet, STMicroelectronics, FR
Nele Mentens, Leiden University, NL, and KU Leuven, BE

Important Notice

In view of the current coronavirus disease (COVID-19) situation, the CARDIS organization decided to make CARDIS 2020 a virtual conference.

Program Committee

Diego Aranha
Aarhus University, DK
Josep Balasch
KU Leuven, BE
Alessandro Barenghi
Politecnico Di Milano, IT
Sonia Belaïd
CryptoExperts, FR
Begül Bilgin
Rambus-Cryptography Research, NL
Billy Bob Brumley
Tampere University, FI
Ileana Buhan
Riscure, NL
Jeroen Delvaux
Open Security Research, CN
Jean-Bernard Fischer
Nagravision, CH
Domenic Forte
University of Florida, US
Dahmun Goudarzi
PQShield, UK
Vincent Grosso
LHC Université Jean Monnet, FR
Daniel Gruss
TU Graz, AT
Tim Güneysu
Ruhr-University Bochum, DE
Annelie Heuser
CNRS/IRISA, FR
Kerstin Lemke-Rust
Bohn-Rhein-Sieg, DE
Roel Maes
Intrinsic ID, NL
Amir Moradi
Ruhr-Universität Bochum, DE
Debdeep Mukhopadhyay
IIT Kharagpur, IN
Colin O'Flynn
NewAE Technology Inc., CA
Stjepan Picek
TU Delft, NL
Thomas Pöppelmann
Infineon, DE
Francesco Regazzoni
ALaRi, CH
Thomas Roche
NinjaLab, FR
Kazuo Sakiyama
Univ. of Electro-Communications, JP
Fareena Saqib
Univ. of N. Carolina at Charlotte, US
Erkay Savas
Sabanci University, TR
Tobias Schneider
NXP Semiconductors, AT
Peter Schwabe
Radboud University, NL
Yannick Teglia
Thales, FR
Aurélien Vasselle
Eshard, FR
Yuval Yarom
University of Adelaide and Data61, AU