CARDIS 2021

20th Smart Card Research and Advanced Application Conference
HYBRID CONFERENCE

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 20th edition of CARDIS is organized by the Institute for IT Security of the Universität zu Lübeck, Germany. The conference website is accessible at https://cardis2021.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
- White-box cryptography

Tools:

- Automated analysis
- Formal verification and secure design
- Machine 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=cardis2021. Submissions must be original, unpublished, anonymous and not submitted to journals or other conferences with proceedings.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 20 pages in total (including references and appendices). 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: ~~**June 25, 2021**~~ **July 5, 2021**
- Notification of acceptance: August 30, 2021
- Pre-proceedings paper due: September 27, 2021
- Conference dates: **November 11-12, 2021**
- Final version due: December 1, 2021

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

Organization

General Chair: Thomas Eisenbarth, Universität zu Lübeck, DE
Program Chairs: Vincent Grosso, CNRS/Université Jean Monnet, FR
Thomas Pöppelmann, Infineon Technologies, DE

Important Notice

In view of the current coronavirus disease (COVID-19) situation, CARDIS 2021 will be either a virtual conference or a hybrid conference with a physical meeting.

Program Committee

Diego Aranha
Aarhus University, DK
Josep Balasch
KU Leuven, BE
Davide Bellizia
Université catholique de Louvain, BE
Shivam Bhasin
NTU, SG
Ileana Buhan
Radboud University, NL
Eleonora Cagli
CEA-Leti, Université Grenoble Alpes, FR
Jan-Pieter D'Anvers
imec-COSIC, KU Leuven, BE
François Durvaux
Silex Insight and Université catholique de Louvain,BE
Domenic Forte
University of Florida, US
Benoît Gérard
DGA-MI, FR
Patrick Haddad
STM, FR
Kerstin Lemke-Rust
Bohn-Rhein-Sieg, DE
Pierre-Yvan Liardet
eShard, FR
Roel Maes
Intrinsic ID, NL
Cuauhtemoc Mancillas Lopez
CINVESTAV-IPN, MX
Nele Mentens
Leiden University, NL
Amir Moradi
Ruhr-Universität Bochum, DE
Debdeep Mukhopadhyay
IIT Kharagpur, IN
Colin O'Flynn
NewAE Technology Inc., CA
David Oswald
University of Birmingham, UK
Peter Pessl
Infineon Technologies, DE
Stjepan Picek
TU Delft, NL
Romain Poussier
NTU, SG
Francesco Regazzoni
University of Amsterdam, NL & Università della Svizzera italiana, CH
Thomas Roche
NinjaLab, FR
Pascal Sasdrich
Ruhr-University Bochum, DE
Tobias Schneider
NXP Semiconductors, AT
Peter Schwabe
MPI-SP, DE & Radboud University,NL
Johanna Sepulveda
Airbus, DE
Yannick Teglia
Thales, FR
Yuval Yarom
University of Adelaide and Data61, AU