



CARDIS 2016

Call For Papers

Fifteenth Smart Card Research and Advanced Application Conference (CARDIS 2016)

Cannes, France, 7 – 9 November 2016

<http://www.cardis.org>

General Chair

Aurélien Francillon,
EURECOM, FR

Program Chairs

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

Program Committee

Guillaume Barbu
Oberthur Technologies, France
Lejla Batina
Radboud University Nijmegen, Netherlands
Guido Bertoni
STM, Italy
Elke De Mulder
Cryptography Research France, France
Hermann Drexler
Giesecke&Devrient, Germany
Thomas Eisenbarth
WPI, USA
Wieland Fischer
Infineon Technologies, Germany
Benedikt Gierlichs
KU Leuven, Belgium
Christophe Giraud
Oberthur Technologies, France
Cezary Glowacz
T-Systems, Germany
Sylvain Guilley
Telecom-ParisTech & Secure-IC, France
Tim Güneysu
University of Bremen, Germany
Johann Heyszl
Fraunhofer AISEC, Germany
Naofumi Homma
Tohoku University, Japan
Yuichi Komano
Toshiba Corporation, Japan
Jean-Louis Lanet
University of Limoges, France
Roel Maes
Intrinsic-ID, Netherlands
Stefan Mangard
TU Graz, Austria
Keith Mayes
Royal Holloway, UK
Marcel Medwed
NXP Semiconductors, Netherlands
Amir Moradi
Ruhr University Bochum, Germany
Svetla Nikova
KU Leuven, Belgium
Pedro Peris-Lopez
University of Madrid, Spain
Axel Poschmann
NXP Semiconductors, Germany
Emmanuel Prouff
Safran Identity and Security, France
Francesco Regazzoni
ALaRI - USI (Switzerland), Switzerland
Patrick Schaumont
Virginia Tech, USA
Francois-Xavier Standaert
UCL Crypto Group, Belgium
Takeshi Sugawara
Mitsubishi Electric Corporation, Japan
Carolyn Whitnall
University of Bristol, UK

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 conferences gather 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 in to other areas, such as TPMs, HSMs, mobile phones and the Internet of Things. It is more important than ever that we understand how smart cards, and related systems, can be secured. The fifteenth Smart Card Research and Advanced Application Conference is organized by Eurecom and will be held in Cannes on the French Riviera on November 7-9, 2016.

The program committee is seeking original papers on all aspects of the security of smart cards and embedded systems. Submissions across a broad range of the development phases are encouraged, from exploratory research and proof-of-concept studies to practical applications and deployment of smart cards and related technologies. Topics of interest include, but are not limited to:

- Hardware architectures for secure embedded systems*
- Physical attacks and countermeasures*
- Efficient cryptographic implementations for smart cards and embedded systems*
- True random number generators*
- Smart cards and their applications*
- Security of mobile devices and their applications*
- Security of RFID/NFC systems and sensor nodes*
- Security for access control, identification, mobile payment, transportation tokens.*
- Security for the Internet of Things*
- Identity, privacy and trust issues*
- Trusted computing (mobile TPMs, TrustZone, Trusted Execution Environments, ...)*
- Software for secure embedded systems (operating systems, virtual machines, ...)*
- Anti-cloning and anti-counterfeiting technologies*
- Hardware trojans implementation and detection*
- Reverse engineering of secure embedded systems*
- Evaluation and certification of secure embedded systems*

Authors are invited to submit papers (PDF format) with novel contributions electronically using the submission form available on the following web site: <https://easychair.org/conferences/?conf=cardis2016> Submitted papers must be original, unpublished, anonymous and not submitted to journals or other conferences/workshops that have 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. Accepted papers must follow the LNCS default author instructions at <http://www.springer.de/comp/lncs/authors.html>.

Important Dates

Submission of papers:	July 15, 2016, 23:59 GMT
Notification of acceptance:	September 8, 2016
Pre-proceeding version:	October 7, 2016
Workshop date:	November 7 – 9, 2016
Final version:	January 15, 2017

CARDIS 2016 is organized by

