Call for Papers

Sixteenth Smart Card Research and Advanced Application Conference

CARDIS 2017

Lugano, Switzerland, 13-15 November 2017

https://2017.cardis.org/

Since its creation, CARDIS has provided a space for security experts from industry and academia to exchange on the security of smart cards and related applications. Those objects are part of our daily life for years now: banking cards, SIM cards, electronic passports, etc. But the world is changing; the smartcard, as a secure element is more and more often the hardware root of trust of bigger systems. Their applications and use cases are also increasing through M2M and massive IoT. As such, smartcard-security is key since the security of entire systems relies on it. With the growing use of smartcard technology, the attack surface is also increasing, from physical attacks to logical attacks, from local attacks to remote attacks. Combined attacks are also to be considered. It is more important than ever that we understand how smart cards, and related systems, can be secured.

The sixteenth Smart Card Research and Advanced Application Conference is organized by ALaRI and will be held in Lugano, Switzerland on November 13-15, 2017.
The program committee is seeking original papers on all aspects of the security of smart cards and embedded systems as well as their applications. 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:

- Physical attacks and countermeasures
- Reverse engineering of secure embedded systems
- Efficient cryptographic implementations for smart cards and embedded systems
- Smart cards and their applications (identification, mobile payment, access controls, pay TV)
- Security of automotive devices and applications
- Security of IoT devices and applications
- Security of Systems on Chip (SoC)
- Security of mobile connected devices (mobile handset, Set Top Boxes, ...)
- Trusted computing (TPMs, TEE, Whitebox Cryptography, ...)
- Hardware architectures for secure embedded systems
- Software architectures for secure embedded systems (operating systems, µ-kernel, hypervisors, virtual machines, ...)
- PUFs, anti-cloning and anti-counterfeiting technologies
- Software security

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=cardis2017

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, strictly follow Springer LNCS format (with default margins, font size, etc.) and should be at most 15 pages, excluding references. 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 21, 2017, 23:59 GMT
Notification of acceptance:	September 12, 2017
Pre-proceedings due:	October 13, 2017
Workshop date:	November 13-15, 2017
Final version of papers:	December 15, 2017