Fourth Workshop on

Cryptography and Security in Computing Systems

Co-located with HiPEAC 2018 Conference, Manchester 24 January 2018

http://www.cs2.deib.polimi.it

Workshop Organizers:
Gerardo Pelosi, Politecnico di Milano, Italy
Giovanni Agosta, Politecnico di Milano, Italy
Alessandro Barenghi, Politecnico di Milano, Italy
Israel Koren, University of Massachusetts Amherst, USA

Important Dates

- November 17, 2017 (Anywhere on Earth): Paper submission deadline
- December 18, 2017: Acceptance notification
- December 21, 2017: Final version of accepted papers for workshop proceedings

Scope of the Workshop

The wide diffusion of embedded systems, including multi-core, many-core, and reconfigurable platforms, poses a number of challenges related to the security of the operation of such systems, as well as of the information stored in them. Malicious adversaries can leverage unprotected communication to hijack cyber-physical systems, resulting in incorrect and potentially highly dangerous behaviours, or can exploit side channel information leakage to recover secret information from a computing system. Untrustworthy third party software and hardware can create openings for such attacks, which must be detected and removed or countered. The prevalence of multi/many core systems opens additional issues such as NoC security. Finally, the complexity on modern and future embedded and mobile systems leads to the need to depart from manual planning and deployment of security features. Thus, design automation tools will be needed to design and verify the security features of new hardware/software systems.
The CS^2 workshop is a venue for security and cryptography experts to interact with the computer architecture and compilers community, aiming at cross-fertilization and multi-disciplinary approaches to security in computing systems. Topics of interest include, but are not limited to, the following:

- Compiler and Runtime Support for Security
- Cryptography in Embedded and Reconfigurable Systems
- Design Automation and Verification of Security
- Efficient Cryptography through Multi/Many core Systems
- Engineering and efficient implementation of post-quantum cryptographic primitives
- Fault Attacks and Countermeasures, including interaction with Fault Tolerance
- Hardware Architecture and Extensions for Cryptography
- Hardware/Software Security Techniques
- Hardware Trojans and Reverse Engineering
- Physical Unclonable Functions
- Privacy in Embedded Systems
- Security of Embedded and Cyber-Physical Systems
- Security of Networks-on-Chips and Multi-core Architectures
- Side Channel Attacks and Countermeasures
- Trusted computing

The workshop seeks submissions from academia and industry, presenting novel research contributions and industrial case studies.

Submission Guidelines

All submissions must be written in English, and should be anonymized. All papers will be refereed (double blind). Regular submissions should be at most 6 pages in the ACM double-column format including bibliography.
Please, use the ACM template when preparing your manuscript. Authors must submit their papers (in PDF format) by the deadline indicated above, using the EasyChair web site.

Publication

Papers will be included in the ACM Digital Library, with a specific ISBN. At least one author of each accepted paper must register to the HiPEAC conference, by the early date indicated by the organizers, and present the paper.

If you have any question, please contact the program chairs at cs2chair@polimi.it