

Call for Participation

The Embedded Systems Challenge, 2011 (ESC 2011)

<http://www.poly.edu/csaw-embedded>

Organized by

Polytechnic Institute of New York University, Brooklyn, NY 11201

November 11, 2011

Main sponsor: Air Force Research Labs

Organizers:

R Karri
NYU Poly
F Koushanfar
Rice Univ.
N. Potlapally
Intel
JV Rajendran
NYU Poly
M Majzoobi
Rice Univ.
E Gavas
NYU Poly

Sponsors:



Intel Corporation

Deadlines:

Registration:
September 10, 2011
Finalists selection:
September 20, 2011
Final:
November 11, 2011

Trusted computing relies on dedicated and trusted hardware platforms. The security and trustworthiness of hardware platforms is critical to several applications ranging from credit cards to traffic monitoring systems to missile control. Recent attacks on hardware platforms such as tampering, reverse engineering, and malicious circuits insertion highlight the importance of designing secure and trustworthy hardware.

The annual Embedded Systems Challenge (ESC) focuses on the red-team blue-team approach to assessing the trustworthiness of hardware. Teams are invited to participate in this challenge and attack a target hardware platform. They will discover vulnerabilities in the target platform and exploit them by using their hardware design skills. Such attacks lead to a better understanding of the vulnerabilities in hardware platforms and thereby enable designers to build trustworthy hardware that can thwart such attacks.

The 2011 edition of ESC will start in September 2011 and culminate in a final event on November 11, 2011 at NYU Poly, Brooklyn, New York, USA. Teams can participate in any one or both of the following challenges:

1. **Attacking an embedded processor (8051):** Insert malicious components into a processor (8051) on an FPGA. This processor will run a set of instructions that perform an encryption. These instructions will be stored in a RAM. Teams can modify the components either in the processor, memory, or the communication lines or all of them. Attacks may not be limited to leaking secret key or performing a denial-of-service attacks. Innovative and practical attacking mechanisms will be greatly appreciated by the judges.

2. **Design an efficient Physical Unclonable Functions (PUF):** PUFs are low-cost security primitives required to protect intellectual properties in an IC. In this challenge, teams have to design a secure and reliable PUF on the given FPGA. The quality of the PUF will be evaluated by different metrics such as Hamming distance between the responses when a bit in a challenge is flipped, distribution of 1's and 0's in the response bits, response uniqueness across different instantiations. In addition, the power, delay, and area occupied by the PUF will be considered.

In order to participate, teams have to register themselves at <http://www.poly.edu/csaw2011/csaw-embedded/register> before **September 10, 2011**. Teams have to submit an initial report on their possible ideas; attacking the processor and/or designing the PUF. Based on the report, finalists will be selected.

Selected finalists will attend the ESC final in New York City (travel+accommodation will be paid for US participants). Cash prizes will be awarded to winners and first-place runners-up. Scholarships will be awarded to all finalists to attend NYU-Poly. Finalists can interact with recruiters from the sponsoring agencies. A special issue of a journal/special session of a conference will be organized (ESC 2010 papers are appearing as a special session of the IEEE ICCD 2011).