Call for Papers

A wide range of applications, from secure RFID tagging to high-end trusted computing, relies on dedicated and trusted hardware platforms. The security and trustworthiness of such hardware designs are critical to their successful deployment and operation. Recent advances in tampering and reverse engineering show that important challenges lie ahead. For example, secure electronic designs may be affected by malicious circuits, Trojans that alter system operation. Furthermore, dedicated secure hardware implementations are susceptible to novel forms of attack that exploit side-channel leakage and faults. Third, the globalized, horizontal semiconductor business model raises concerns of trust and intellectual-property protection. HOST 2012 is a forum for novel solutions to address these challenges. Innovative test mechanisms may reveal Trojans in a design before they are able to do harm. Implementation attacks may be thwarted using side-channel resistant design or fault-tolerant designs. New security-aware design tools can assist a designer in implementing critical and trusted functionality, quickly and efficiently.

The IEEE International Symposium on Hardware Oriented Security and Trust seeks original contributions in the area of hardware-oriented security. This includes tools, design methods, architectures, and circuits. In addition, novel applications of secure hardware are especially welcome. HOST 2012 seeks contributions based on, but not limited to, the following topics.

- Trojan detection and isolation
- Implementation attacks and countermeasures
- Side channel analysis and fault analysis
- Intellectual property protection and metering
- Hardware architectures for cryptography
- Hardware security primitives: PUFs and TRNGs
- Applications of secure hardware
- Interaction of secure hardware and software
- Tools and methodologies for secure hardware design

To present at the symposium, submit an Acrobat (PDF) version of your paper on the symposium submission website: [https://www.easychair.org/account/signin.cgi?conf=host-2012](https://www.easychair.org/account/signin.cgi?conf=host-2012)

The page limit is 6 pages, double column, IEEE format, with a minimum font size of 10 points. Submissions must be anonymous and must not identify the submitting authors, directly or indirectly, anywhere in the manuscript.

**SCHEDULE:**

- Submission of Title and Abstract: January 20, 2012
- Submission of Full Paper: January 27, 2012
- Notification of Acceptance: March 23, 2012
- Submission of Camera Ready Paper: April 13, 2012

**For students:**

- Best paper award for a paper whose first author is a full-time student at the submission time.
- Best presentation award for a speaker who is a full-time student at the presentation time.
- Travel grants for undergraduate and graduate students.

**Travel grants for undergraduate and graduate students.**

**Technical Program:**

- Ramesh Karri
- Polytechnic Institute of New York U.
- Tel: (718)260-3596, cell: (917) 363-9703
- E-mail: rkarri@poly.edu

**General Information:**

- Ken Mai
- Carnegie Mellon University
- Tel: (412)268-8383
- Email: kenmai@ece.cmu.edu

**2011 sponsors:**

- IEEE
- Computer Society
- Technical Committee on Security and Privacy