Pervasive computing is now penetrating a wider range of domains and applications, including many safety-critical cyber-physical systems that we increasingly depend on. Trusted hardware platforms make up the backbone for successful deployment and operation of these systems. However, recent advances in tampering and reverse engineering show that important challenges in guaranteeing the trust of these components await us. For example, malicious alterations inserted into electronic designs can allow for backdoors into the system. Furthermore, new forms of attacks that exploit side-channel signals are being developed. Third, intellectual-property protection is becoming a major concern in the globalized, horizontal semiconductor business model. HOST 2013 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, circuits, and novel applications of secure hardware. HOST 2013 seeks contributions based on, but not limited to, the following topics.

- Counterfeit detection and avoidance
- Cyber-physical security and trust
- 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
- Reliability-security optimization and tradeoffs
- Applications of secure hardware
- Tools and methodologies for secure hardware design

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.

To present at the symposium, submit an Acrobat (PDF) version of your paper using the following website: https://www.easychair.org/account/signin.cgi?conf=host2013. 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 authors, directly or indirectly, anywhere in the manuscript.

**SCHEDULE:**
- Submission of Abstract: December 10, 2012
- Submission of Paper: December 17, 2012
- Notification of Acceptance: January 4, 2013

**General Information:**
- General Chair: R. Karri, Polytechnic Inst., New York U.
- Program Chair: F. Koushanfar, Rice U
- Vice-program Chair: M. Hsiao, Virginia Tech
- Panel Chair: K. Mai, CMU
- Publicity Chair: S. Bhunia, Case Western Reserve U.
- Registration Chair: J. Plusquelllic, U. of New Mexico
- Publication Chair: T. Huffmire, Naval Postgraduate School
- Finance Chair: W. Robinson, Vanderbilt

**Steering Committee:**
- M. Tehranipoor (chair), U. Connecticut
- J. Plusquelllic, U. of New Mexico
- F. Koushanfar, Rice University
- M. Potkonjak, UC Los Angeles

2012 sponsors:
- IEEE Computer Society
- Technical Committee on Security and Privacy