

General Chair

W. H. Robinson, Vanderbilt U.

Program Chair

S. Bhunia, U. of Florida

Vice-program Chair

R. Kastner, U. of California, San Diego

Finance Chair

A. Srivastava, U. Maryland

Publicity Chair

D. Forte, U. of Florida

Local Arrangements Chair

H. Salmani, Howard U.

Registration Chair

Y. Jin, U. of Central Florida

Panel Tutorial Chair

S. Fazzari, Booz Allen

Industrial Liaison

M. Tehranipoor, U. of Florida

G. Qu, U. of Maryland

Publications Chair

T. Huffmire, Naval Postgraduate School

Asia-Pacific Liaison

R. S. Chakraborty, IIT Kharagpur

Hardware Demo Chair

J. Plusquellic, U. of New Mexico

Call for Papers

Rapid proliferation of computing and communication systems with increasing computational power and connectivity into every sphere of modern life has brought security to the forefront of system design, test, and validation processes. The emergence of new application spaces for these systems in the internet-of-things (IoT) regime is creating new attack surfaces as well as new requirements for secure and trusted system operation. Additionally, the design, manufacturing and the distribution of microchip, PCB, as well as other electronic components are becoming more sophisticated and globally distributed with a number of potential security vulnerabilities. Therefore, hardware plays an increasingly important and integral role in system security with many emerging system and application vulnerabilities and defense mechanisms relating to hardware.

IEEE International Symposium on Hardware Oriented Security and Trust (HOST) aims to facilitate the rapid growth of hardware-based security research and development. HOST highlights new results in the area of hardware and system security. Relevant research topics include techniques, tools, design/test methods, architectures, circuits, and applications of secure hardware. **HOST 2016** invites original contributions related to, but not limited by, the following topics.

- **Hardware Trojan attacks and detection techniques**
- **Hardware-based security primitives (PUFs, RNGs)**
- **Side-channel attacks and protection**
- **Security, privacy, and trust protocols**
- **Metrics, policies, and standards related to hardware security**
- **Security of biomedical systems, e-health, and medicine**
- **Secure system-on-chip (SoC) architecture**
- **Hardware IP trust (watermarking, metering, trust verification)**
- **Trusted manufacturing including split manufacturing and 3D ICs**
- **Security analysis and protection of Internet of Things (IoT)**
- **Secure and efficient implementation of crypto algorithms**
- **Reverse engineering and hardware obfuscation**
- **Supply chain risks mitigation including counterfeit detection & avoidance**
- **Hardware tampering attacks and protection**
- **Hardware techniques that ensure software and/or system security**

To present at the symposium, submit an Acrobat (PDF) version of your paper on the symposium submission website (<https://easychair.org/conferences/?conf=host2016>). 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.

Also, for the first time at HOST, students can participate in a hardware demo session by submitting a 1-page proposal describing the research and features to be demonstrated on an FPGA or other hardware platform. Please email your proposal to the Hardware Demo Chair (jimp@ece.unm.edu) by March 15, 2016 to be considered for the session.

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.

SCHEDULE:

Registration of Title + Abstract:
Submission of Paper:
Notification of Acceptance:
Camera-ready Version:
Hardware Demo Proposal:

November 1, 2015
November 8, 2015
January 31, 2016
February 28, 2016
March 15, 2016

Technical Program: S. Bhunia

U. of Florida
Tel: +1 (352) 392-5989
E-mail: swarup@ece.ufl.edu

General Information: W. H. Robinson

Vanderbilt U.
Tel: +1 (615) 322-1507
Email: william.h.robinson@vanderbilt.edu

2016 sponsors:



IEEE
Computer Society
Technical Committee on
Security and Privacy