Call for Papers: IEEE International Symposium on Hardware Oriented Security and Trust (HOST) 2022

Important Dates:

Call for Work-in-Progress Papers

Deadline
Full Paper Submission: Jan. 15, 2022
Notification: Feb. 15, 2022
Camera-ready: Feb. 25, 2022

Tutorial Proposal Submission (Notification): No new submissions are accepted

HW Demo Proposal Submission (Notification): Jan. 30, 2022 (Feb. 15, 2022)

All submission information and topic details can be found at http://www.hostsymposium.org/call-for-paper2022.php

---

IEEE International Symposium on Hardware Oriented Security and Trust (HOST) – the premier event that aims to facilitate the rapid growth of hardware-based security research and development and highlight new results in hardware security – **has opened a call for contributions for Work-in-Progress (WiP) papers**. The 15th annual HOST conference will be held June 27-30, 2022, in Washington D.C.

Submissions are due Jan. 15, 2022, and should be at most four pages including references. The intention of a WiP paper is to share with the community ongoing work which may not have reached maturity, and as such the usual requirement for strong experimental validation is reduced. All submissions will be anonymously reviewed with at least one review per submission, and accepted WiP papers will appear in IEEE Explore as a peer-reviewed publication. Each WiP paper has to be presented at HOST 2022 and requires one registration.

HOST 2023 will call for paper submissions in the summer of 2022 with a tentative deadline in the month of October 2022 (HOST 2023 is scheduled for May 2023). Paper submissions for HOST 2023 may include extended full 10-page paper submissions from the WiP HOST 2022. The new submissions and WiP extended submissions will go through same double blind review process, so the authors are required to keep their identities anonymous.

HOST 2022 invites original Work-in-Progress (WiP) contributions in all areas of overlap between hardware and security. This includes but is not limited to the following:

HARDWARE

- Security primitives
- Computer-aided design (CAD) tools
- Emerging and nanoscale devices

- Trojans and backdoors
- Side-channel attacks and mitigation
- Fault injection and mitigation
- (Anti-)Reverse engineering and physical attacks
- Anti-tamper
- Anti-counterfeit

ARCHITECTURE

- Trusted execution environments
- Cache-side channel attacks and mitigation
- Privacy-preserving computation
- System-on-chip (SoC)/platform security
- FPGA and reconfigurable fabric security
- Cloud computing
- Smart phones and smart devices

SYSTEM

- Internet-of-things (IoT) security
- Sensors and sensor network security
- Smart grid security
- Automotive/autonomous vehicle security
- Cyber-physical system security
- (Adversarial) Machine learning and cyber deception

Paper submission link will be updated on the HOST webpage soon. The page limit is **4 pages**, double column, IEEE format, with a minimum font size of 11 pt.

For more information on HOST visit: http://www.hostsymposium.org/