Zero Trust Hardware Architectures Workshop

Co-located with 2023 International Conference on Computer-Aided Design (ICCAD)

Thursday, November 2, 2023

San Francisco, California, USA

CALL FOR PAPERS

https://zerotrustworkshopiccad.github.io

In recent times, there has been a major push and urgency to adopt the zero-trust model for cybersecurity. The zero-trust model is based on the principle of "never trust, always verify" and is aimed at eliminating all implicit trust in a system. While adopting a zero-trust model, the underlying hardware needs to be trusted and secured as well. Thus, novel approaches for building zero trust architectures, from systems all the way down to silicon, is one of the big challenges for next generation hardware system design.

Traditionally, research on establishing trust and security in hardware has primarily focused on the host and its associated memory subsystems. However, in modern system architectures such as edge/cloud computing, composable systems and chiplet based integrated circuits, the realm of trust needs to be extended beyond the host system and incorporate many hardware devices and IPs. In view of threats such as compromised supply chain integrity, counterfeit chips, hardware trojan implants, malicious firmware, malware, etc., it is important to establish trust in hardware components and to communicate trust between different components of a system. Thus, a new set of protocols that can work to establish trust and security in these new types of system architectures has become necessary. The focus of this workshop will be on all aspects of security and trust required to create zero-trust hardware architectures for heterogeneous computing systems.

The areas of interest include but are not limited to:

- Extending confidential computing or Trusted Execution Environments to peripherals
- Building trust in novel computing architectures such as composable processors/composable systems
- Enabling trust in novel packaging technologies such as Heterogeneous Integration/System-in-Package/Chiplets
- Secure and trusted integration of AI cores or AI chiplets in heterogeneous systems/circuits
- Supply chain security of hardware and firmware
- Hardware-Enabled security for Cloud and Edge computing
- Role of open-source designs and standards for security and trust
- Other emerging topics in security and trust such as post-quantum cryptography, homomorphic encryption, secure multi-party computation etc.

Important dates:

- Talk Abstract Submission Deadline: ~~**September 17, 2023 (AOE)**~~ **September 24, 2023**
- Notification: October 1, 2023
- In-Person Workshop: November 2, 2023

Submission:

We welcome proposals for a 30-minute presentation on the topics of interest. Presentations will be recorded and published on the workshop website. Each talk abstract must be no more than 2 pages including a title, abstract and bio.

Organizers: Sandhya Koteshwara, Mengmei Ye and Hubertus Franke, IBM Research, USA