Zero Trust Hardware Architectures Workshop

Co-located with 2024 Cryptographic Hardware and Embedded Systems (CHES)

Wednesday, September 4, 2024

Halifax, Canada

CALL FOR PAPERS

https://zerotrustworkshop.github.io/

With an ever-increasing number of attacks on the software, firmware and hardware stacks of systems, there is an urgent need to adopt a zero-trust model for cybersecurity. Cryptography to perform authentication, verification and provide confidentiality are core technologies to enable the foundations of zero trust. Thus, devising novel approaches for building zero-trust architectures with efficient cryptographic implementations, from systems all the way down to silicon, is one of the big challenges for next generation hardware design. Traditionally, research on establishing trust and security in hardware has primarily focused on the host CPU and its associated memory subsystems. In modern embedded and non-embedded system architectures, such as edge/cloud computing, composable systems, and chiplet based integrated circuits, trust needs to be extended beyond the host to incorporate other hardware devices and the intellectual property (IP) models used to design them. The focus of this workshop will be on all aspects of security and trust required to create zero-trust hardware architectures for traditional and embedded systems, and their components.

The areas of interest include but are not limited to:

- Extending confidential computing or TEEs to embedded devices, components and peripherals
- Building security and trust through cryptography in novel computing architectures such as composable processors/composable systems
- Enabling security and trust through cryptography 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
- Dynamic or runtime verification/reverification.
- Trusted computing and cryptographic implementation challenges of real-time hardware for IoT and autonomous vehicles
- Supply chain security of hardware and firmware
- Threat models for applications of zero-trust architecture
- 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: **June 21, 2024**
- Notification: July 19, 2024
- In-Person Workshop: September 4, 2024

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