2022 IEEE International Symposium on Secure and Private Execution Environment Design (SEED)

Selected papers will be considered for publication in a special issue of IEEE Micro.

SEED invites manuscripts that present original unpublished research with focus on the design of architectural and system primitives that provide secure and private execution environments for applications, containers, or virtual machines. SEED primarily focuses on research topics spanning across the boundaries of computer architecture, systems, and security. Papers are solicited on a range of topics, including (but not limited to):

- Architecture, operating systems, and programming models and language for supporting secure and private execution
- Novel Designs for secure and private execution environments for GPUs, accelerators, and FPGAs
- Architectural support for new security primitives
- Novel cryptographic hardware designs for secure and private execution
- Models and analysis of performance-security trade-offs in the design of a secure execution environment
- Evaluation of security vulnerabilities in post-Moore's Law technologies, e.g., persistent memory, quantum computing
- Demonstration and mitigation of architectural side channels, covert channels, and other security vulnerabilities
- Metrics for measuring architecture-related security vulnerabilities
- Compiler and code generation techniques for mitigating architecture-induced side and covert channels and other vulnerabilities

Deadlines

Abstract: June 3, 2022
Full paper: June 10, 2022, 11:59pm AOE (EXTENDED DEADLINE)
Notification: July 29, 2022
Camera-ready paper: September 2, 2022

SEED will accept one of three types of submissions:

- **Regular papers**: The primary focus of the regular papers should be to describe new research ideas overlapping computer architecture/systems and security, supported by experimental implementation and evaluation of the proposed research ideas. Promising designs, initial development, and preliminary evaluation of new ideas critical to the security of future architecture/systems are also welcome. Contributions from industry, that bring awareness to a new security problem and/or lay vision for sound architecture/systems security principles, are encouraged.
- **Systemization of Knowledge**: Systemization of Knowledge (SoK) papers are also welcome and should be submitted as regular papers.
- **Work in Progress**: Additionally, we accept Work-in-Progress (WiP) submissions that should describe novel secure systems designs supported by experiments. For submissions accepted under WiP category, the authors will make a presentation and include the title and a brief abstract on the conference website. The WiP submissions will not be included in the official proceedings of the Symposium.

Submissions can be at most 11 pages for regular and SoK type, and 6 pages for WiP type. If you can express your contributions in fewer pages than the page-limit, the PC encourages you to do so. Manuscripts must be submitted in printable PDF format, not including references, and must use the two-column IEEE Proceedings format. There is no page limit for references. References must include all authors to facilitate the reviewing process (no et al.). Text must be minimum 10pt Times font. Please number the pages of your submission. **Double-blind** submission guidelines apply to the submissions in all categories.