2024 IEEE International Symposium on Secure and Private Execution Environment Design (SEED)

Preliminary symposium dates: early Feb, 2024
Location: Orlando, Florida

SEED invites manuscripts that present original unpublished research with focus on the design of architectural and system primitives that provide secure and private execution environments for applications, containers,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
- New architectural attacks targeting CPUs, GPUs, memory or other components of computing systems
- Metrics for measuring architecture-related security vulnerabilities
- Tools and techniques for automated vulnerability discovery
- Compiler and code generation techniques for mitigating architecture-induced side and covert channels and other vulnerabilities
- End-to-end applications and demonstrations of microarchitectural attacks

Deadlines

Full research paper: Oct 27th, 2023, 11:59pm AOE
Notification: Dec 15th, 2023
Camera-ready paper: Jan 5th, 2024

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.
- **Wild and emerging ideas (WEI)**: Additionally, we accept submissions that describe ideas that are unconventional or emerging. A submission should include the title and a brief abstract (2 pages total, including references).

Submissions can be at most 11 pages for regular papers, and 2 pages for WEI papers. 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 and must use the two-column IEEE Proceedings format. For regular papers, there is no page limit for references. References must include all authors to facilitate the reviewing process (no et al.). Text must be in minimum 10pt Times font. Please number the pages of your submission. **Double-blind** submission guidelines apply to the submissions in all categories.