RaSTEES '19
1st workshop on Reliable and Secure Trusted ExEcution Systems
1st October 2019, Lyon, France

The 1st workshop on Reliable and Secure Trusted ExEcution Systems (RaSTEES ‘19) will take place on October 1, 2019, in Lyon, France, co-located with the SRDS 2019 conference (https://srds2019.projet.liris.cnrs.fr/).

Call for Papers

The reliability and security of distributed systems is a major concern. Indeed, distributed systems can involve multiple parties that mistrust each others and are subject to faults. This is a particularly important problem for many applications that have to handle sensitive and personal data, such as cloud storage, communication services, etc. A Trusted Execution Environment (TEE) is a practical solution to improving the reliability and security of applications running in an untrusted environment. Examples of TEEs include Intel SGX, ARM TrustZone and AMD SME/SEV. Unfortunately, using a TEE is not a straightforward task. Not only the hardware possesses several limitations, but there is also a lack of software support for implementing efficient and secure systems. Consequently many technical challenges need to be overcome. The 1st workshop on Reliable and Secure Trusted ExEcution Systems will focus on the design and implementation of TEEs (including system support and middleware) to enable the implementation of trustworthy systems. The goal is not only to add security to existing systems, but also to envision how TEEs should be designed and how they can be leveraged in order to create novel trustworthy systems.

Theme and goals

Topics of interest include but are not limited to:

- Architecture and implementation of trusted infrastructures
- Middleware for distributed trusted execution
- OS support for trusted execution
- Edge/IoT and trusted hardware
- Attestation and integrity verification
- Program analysis and hardening of trusted systems
- Cryptographic aspects of trusted and trustworthy computing
- Side channel as well as fault-injection attacks and defences
- Virtualization for trusted platforms
- Blockchain and smart contracts on trusted hardware
- Security policy and management of trusted computing
- Privacy aspects of trusted computing
- Trusted and secure Machine Learning
- Limitations of trusted computing

- Design of trusted hardware for accelerators (GPU, FPGA)
- Validation and performance evaluation of trusted hardware
- Formal verification of trusted hardware and software
- Byzantine fault tolerance and trusted hardware

The goal of the workshop is to foster collaboration and discussion among researchers and practitioners in this field.

Submission

RaSTEES welcomes submissions in two formats:

1. Regular research papers of at most 6 pages including references. Research papers should not be previously published or concurrently submitted elsewhere and will be published in the proceedings.
2. Short research statements of at most 1-2 pages. Research statements aim at fostering discussion and collaboration. Research statements may summarize research published elsewhere or outline new emerging ideas. Short research statements will not be published in the proceedings.

All submissions should be in PDF and must follow the same format as regular papers of the SRDS '19 conference. Submissions that do not respect the formatting requirement may be rejected without review. Reviewing is single-blind. This means that the names and affiliations of the authors must appear in the submitted papers. Each paper will receive at least three reviews from members of the program committee.

Submission will be done through the workshop website: https://plaublin.github.io/RaSTEES/ .

Important dates

- Submission Deadline: 21th Jun 2019
- Author Notification: 19th Jul 2019
- Camera Ready Submission: 2nd Aug 2019
- Workshop date: 1st October 2019