SWITS Abstract

Asrin Abdollahi is a PhD student of cybersecurity unit at RISE Research Institutes of Sweden AB, along with Mälardalens University (MDU).

Building a Secure Open-Source Hardware Architecture with Trusted Execution Environments (TEEs)

In today's open-source hardware architecture world, such as RISC-V, where integrity and confidentiality of sensitive data are crucial, the Trusted Execution Environment (TEE) creates a secure enclave where high-security applications and critical processes can be run privately from the host kernel. TEE enables a safe environment for running vital code or loading sensitive data by providing the next level of security through several types of isolation utilizing IOMMU (Input/Output Memory Management Unit) and memory management units (MMUs). Furthermore, TEE offers two key security principles: confidentiality and integrity. To verify the validation of these, attestation plays a crucial role by creating and forwarding a challenge-request to the TEE. Attestation can be performed by a TEE's user application, an external TPM, or an in-built TPM, e.g., MARS (Measurement and Attestation RootS). RISC-V, as an open-source instruction set architecture (ISA) in processor architecture, provides a link between hardware and software, granting IoT numerous benefits. Moreover, RISC-V supports physical memory protection (PMP) to control and define permissions for various memory regions. After all, the main purpose is to build a safe environment for open-source hardware architectures to protect sensitive data and code while in process.

Note: 10 minutes will be sufficient for my presentation.