Asrin Abdollahi

Industrial PhD Student at RISE

Short Presentation

Title:

Trusted Execution Environment (TEE) for Low-Power RISC-V Devices

Abstract:

Securing IoT devices can be challenging due to their small size, limited battery power, and resource constraints. Protecting RISCV devices at the hardware level is necessary to mitigate the attack surface. RISC-V offers an open-source architecture, license-free, and customizability, making it ideal for small IoT devices and custom designs. A lightweight TEE can protect sensitive data and code by creating a private operating environment within the processor, isolated from the main operating system (OS). TEE is a hardware-based security mechanism that provides a private execution environment for sensitive tasks which prevents unauthorized access and exploitation. A secure monitor with privileged access can ensure that only trusted applications with approved tasks are executed in the enclave (the secure world). This can be achieved using RISC-V features, including a well-defined isolation through Physical Memory Protection (PMP) controlled by the secure monitor. The work is around the low-level hardware programming stage using a Renode simulator. In the case of Real-World evaluation, the novel system design is tested on an FPGA board, such as the Arty A7. The secure design shall show the integrity and confidentiality of the data and code within TEE.