PhD Student: Anum Khurshid, RISE Cybersecurity, Stockholm <anum.khurshid@ri.se>

Main Supervisor: Shahid Raza, RISE Cybersecurity

Title: Hardware-based Trusted Execution Environment for Resource-constrained IoT

Abstract:

Trusted Execution Environments (TEE) provide software security to critical operations and sensitive data by isolating them from the rest of the system. The system is partitioned into two domains (i.e., non-secure world and secure world) where we can store, process and protect security critical resources. The memory regions and peripherals in a TEE can be grouped into secure world and non-secure world where only secure code can access secure memory and peripherals. The context switch between the two worlds is handled by the processor to maintain latency. These mechanisms are targeted at securing user assets and keys and isolating execution of services like mobile payments and Digital Rights Management (DRM). The recent introduction of TrustZone into ARM Cortex-M processors (specifically Cortex-M23 and Cortex-M33) makes it possible for resource-constrained IoT devices to process critical operations securely.

The fact that IoT devices are not designed with security in mind has made them vulnerable to numerous attacks. Since the Mirai Botnet attack in 2016, the focus of the research community on IoT security has increased exponentially and recent research on IoT security has already begun to utilize TrustZone-M for isolated execution of security-critical resources in IoT systems. The aim of this research is to enable security to the software components in Cortex-M based IoT devices. Our approach to achieve this outcome is through Trusted Execution Environments. We begin by discovering vulnerabilities in Trusted Execution Environments targeting resource-constrained IoT and exploring scalable and efficient solutions with respect to the devices available in the market. To achieve this goal we attempt to answer questions like “What are the vulnerabilities in Trusted Execution Environments that threaten the security critical operations in IoT devices?”, “How can these vulnerabilities be fixed to make the system resilient against attack?” and “How can the proposed framework/solutions be made efficient considering the limited processing capabilities of these devices?”.

This work is done in collaboration with Uppsala University and is partly funded by SSF aSSIsT and partly by EU Horizon 2020 CONCORDIA, a project that is building an EU cybersecurity center of excellence.