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

Main Supervisor: Shahid Raza, RISE Cybersecurity

Title: Hardware-Based Trusted Execution Environment for Resource-Constrained IoT Devices - Focused on ARM TrustZone Cortex-M family

Abstract:

TrustZone provides Trusted Execution Environment (TEE) for isolated execution of security sensitive resources by partitioning the system 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 very interesting for us, since these processors are designed for resource-constrained (low-power/battery powered) IoT devices. 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. However, isolation of execution may not be enough to properly protect resources since the communication channel between the two worlds is vulnerable to man-in-the-middle attack and number of other attacks. This situation puts the data transferred through the channel between the two worlds in jeopardy, as it can be manipulated or modified by attackers. We are working on the vulnerability of this channel and devising an architecture to overcome it.

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