Overview of ARM TrustZone Trusted Execution Environment (TEE)

A Trusted Execution Environment (TEE) [1] is a technology, which aims to create an isolated execution environment, in which critical operations can be executed and secrets can be securely stored. An example TEE implementation is TrustZone [2] on ARM.

The aim of this work is to:

- conduct a literature review for ARM TrustZone for different ARM processors (ARMv7, ARMv8),
- list the advantages and disadvantages,
- and to compare with each other.

References:


Contact

Request Topic

Advisors

Utku Budak