Trust-E OS v1.0 (Trusted Embedded Operating System)

1. ARM TrustZone security extension mechanism

The ARM TrustZone architecture is designed as an integrated security solution to for the Cortex-A processor family. As a low-level integrated hardware approach, TrustZone is integrated throughout the system bus. Therefore, not only does TrustZone provide for secure execution environment, it provides isolation and control of secure peripherals including memory, crypto blocks and I/O devices.

In the TrustZone architecture, software executes in one of two security modes. The first mode, “normal world” executes as a normal ARM processor. This is the normal execution mode of full-features operating systems, such as Android, and applications. The “secure world” mode is used to support execution of specific security services. Applications running in the normal world can call APIs that will request services from the secure world, but through well protected interfaces. Each world executes in separate addressed spaces.

To allow normal world application to invoke security services, TrustZone supports the Secure Monitor Call (SMC) instruction. When the CPU executes the SMC instruction, the hardware switches into the secure monitor, which saves the “normal world” context and performs a secure context switch into the secure world . In addition to the SMC instruction, TrustZone also implements the Secure Monitor Mode to facilitate communication between the worlds.

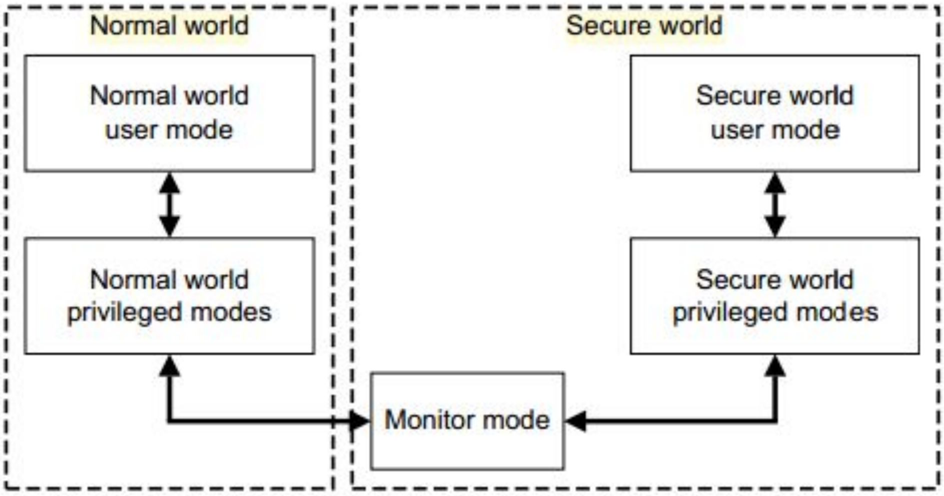

Figure 1 ARM processor with TrustZone security extended mechanism

2. Based on the Global Platform standard TEE software architecture

According to the International Security Chip Organization Global Platform released trusted execution environment (Trusted Execution Environment, TEE) documentation standards, including TEE system architecture, the internal API and API calls for common environment to build trusted operating system framework.

Global Platform released TEE Client API manual, which lists the client application calls TEE security services unified API interface for developers to help REE environment do not understand the current environment and the working mechanism of TEE easily use. As the TEE software developers, should be in accordance with the standard API interface is listed in this manual, to achieve the function of communication between REE (Rich Execution Environment) environment and TEE environment.

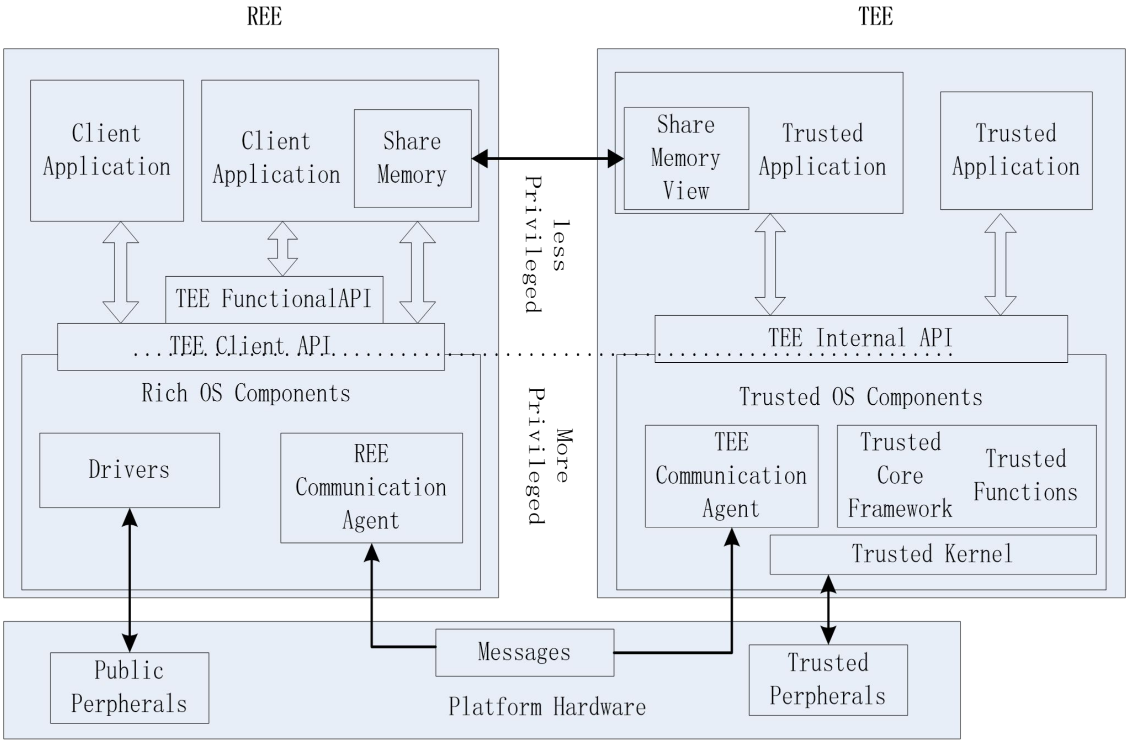

Figure 2 TEE System Architecture

TEE software architecture based on a trusted operating system is a trusted execution environment and by isolating the common execution environment, through the sensitive and critical data resources, its use and storage process is fully treated in the trusted execution environment, so that it can protect the security of data In the maximum degree.

3. Trusted Embedded operating system (Trust-E OS)

Referring to the GlobalPlatform TEE related documents and the kernel of the separation mechanism provided by ARM TrustZone technology, based on these standards to design our trusted embedded operating system architecture, to implement a trusted execution environment with a trusted embedded operating systems.

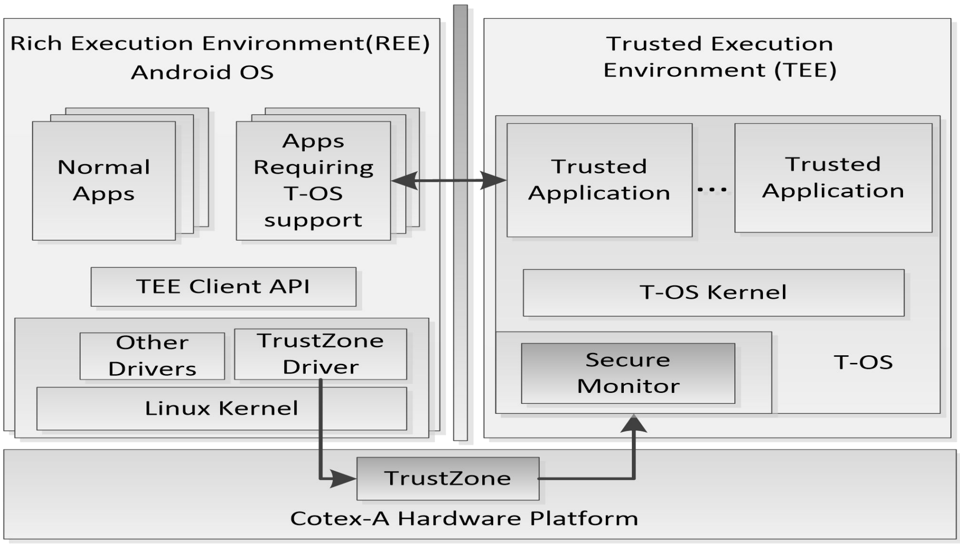

Figure 3 Trusted-E V1.0 embedded operating system architecture

TrustZone driver is loaded in the Linux Kernel, and data communication in the kernel through the underlying driver code and the monitor of trusted security execution environment, as an ordinary execution environment the only way to monitor switching.

T-OS Kernel is we designed a trusted execution environment in a trusted operating system, the operating system needs to provide task scheduling and memory management functions.

Trusted application services are applications that run in the T-OS kernel basis, each service has its own corresponding security service function, a TEE client application running in the rich execution environment, it can establish a session with a trusted application services mode after using the security services it provides.

The project uses a hardware platform development board SMDKV210, the processor is having a Cortex-A8 core S5PV210, Cortex-A8 core has ARM TrustZone security extension mechanism, a Cortex-A8 core can be virtualized as two logical cores, one of the safety of nuclear is used to secure execution environment, in addition to a common core for the general execution environment and its authority is limited to nuclear safety.

Trusted Embedded Operating System is just our initial version and define it as Trust-E OS v1.0, then our operating system will have richer service more comprehensive features will be added.

Design by University of Electronic Science and Technology of China of Embedded Real Time Computing Laboratory.

Contact Info :xyang@uestc.edu.cn