关于本文TEE的信息主要来自论文[1]

TEE定义

可信执行环境(Trusted Execution Environment)简称TEE，是CPU中的安全区域，可以保护其中的程序或者数据的机密性和完整性，防止被操作系统或者其它程序窥测或者篡改。定义如下

> 可信执行环境（TEE）是一个在分离内核上运行的防篡改执行环境。它保证执行代码的真实性、运行状态（如CPU寄存器、内存和敏感的I/O）的完整性，以及其代码、数据和存储在持久性内存中的数据的保密性。此外，它应能提供远程证明，证明其对第三方的可信度。TEE的内容不是静态的；它可以被安全地更新。

TEE架构

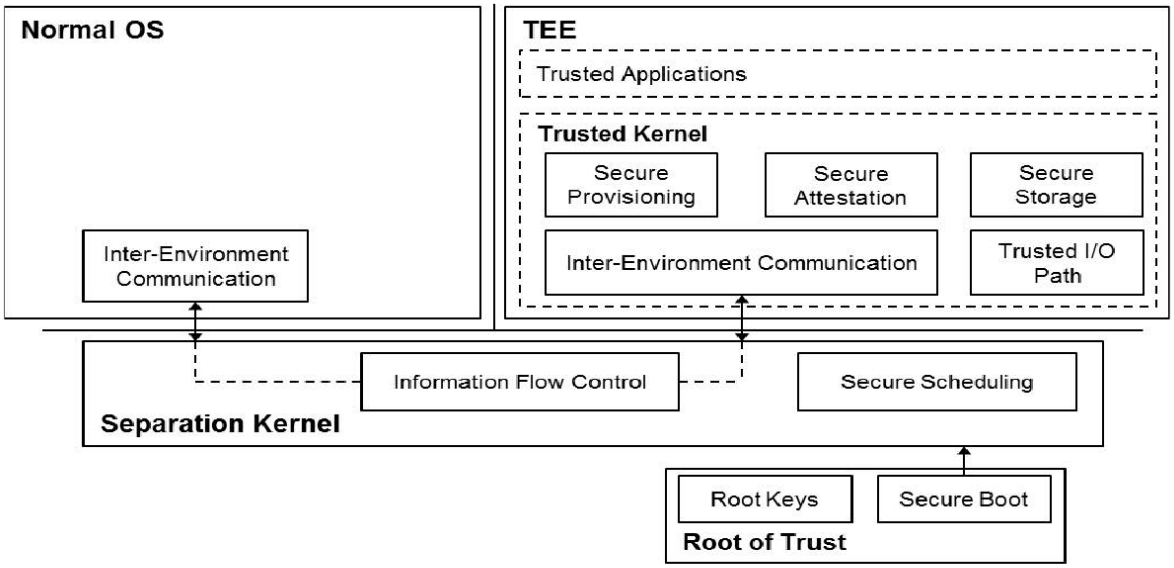

Fig. 1. An Overview of TEE Building Blocks

- **Separatiion Kernel**是TEE的基础组件，它是保证隔离执行特性的元素。分离内核是一个用于模拟分布式系统的安全内核
- **Secure Boot**保证了只有满足了某种属性的代码可以被加载进入TEE。 如果检测到有故意修改，Bootstrap过程就会中断， 初始启动代码受到防篡改硬件模块的保护
- **Secure Scheduling**保证了TEE和系统其他部分之间的 "平衡 "和 "有效 "协调
- **Inter-Environment Communication**定义了一个接口，允许TEE与系统的其他部分进行通信。尽管它有许多好处，但它也引入了新的威胁，例如消息过载攻击，以及系统中不被信任的部分无响应导致的无限等待。 三种通信模式：(1) GlobalPlatform TEE客户端API；(2) Secure RPC（远程程序调用）[6]；(3) SafeG的实时RPC
- **Secure Storage**是指存储数据的保密性、完整性和新鲜度（即防止重放攻击和**保证执行状态连续性，即FastBFT中计数值**）得到保证的存储，并且只有授权实体可以访问数据
- **Tursted I/O Path**保护TEE和外围设备（如键盘或传感器）之间通信的真实性和机密性

TEE产品

主流计算平台均集成了自己的TEE服务，例如Intel SGX，ARM TrustZone。

TEE	Author laboratory/company	License	TCB Size	Supported Normal World	Supported Hardware Platform
ObC	Nokia	Close	10kB	Symbian OS	300 MHz OMAP 2420
<t-base	Trustonic	Close	Unknown	Android	Samsung Exynos platforms
Andix OS	TU Graz University of Technology	Open-source	Unknown	Linux	iMX53 QSB
TLK	NVidia	Open-source	128kB	Android	Tegra SoCs
TLR	Microsoft	Close	152.7 KLOC	.NET CLR	Tegra 250 Dev Kit
SafeG	Nagoya University	Open-source	1.96 kB	TOPPERS/ASP	PB 1176 JZF-S board

TABLE I
AN OVERVIEW OF THE COMPARED TEES

1. https://ieeexplore.ieee.org/document/7345265 ↩