DEFINITION

trusted execution environment (TEE)

By Corinne Bernstein

What is a trusted execution environment (TEE)?

A trusted execution environment (TEE) is an area on the main processor of a device that is separated from the system's main operating system (OS). It ensures data is stored, processed and protected in a secure environment. TEEs provide protection for anything connected, such as a trusted application (TA), by enabling an isolated, cryptographic electronic structure and end-to-end security. This includes the execution of authenticated code, confidentiality, authenticity, privacy, system integrity and data access rights.

As demand for digital trust grows and concern over securing connected devices rises, TEEs have gained significance. The concept of a TEE is not brand-new, but it is no longer confined to use in high-end technology. TEEs are used widely in complex devices, such as smartphones, tablets and set-top boxes. TEEs are also used by manufacturers of constrained chipsets and internet of things (IoT) devices in sectors such as industrial automation, automotive and healthcare, which recognize its value in protecting connected things.

Running parallel to the OS and using both hardware and software, a TEE is intended to be more secure than the traditional processing environment. This is sometimes referred to as a rich operating system execution environment, or REE, where the device OS and applications run.

Why is TEE important?

Often, especially in the case of smartphones, devices hold a combination of personal and professional data. For example, mobile devices with apps surrounding

payment transactions will hold sensitive data. TEEs can help solve significant problems for anyone concerned with protecting data and play an increasingly central role in preventing hacking, data breaches and use of malware.

In any situation where sensitive data is being held on a device, TEEs can play an important role in ensuring a secure, connected platform with no additional limitations on device speed, computing power or memory.

How does TEE work?

Even though a TEE is isolated from the rest of the device, a trusted application that runs in a TEE will typically have access to the full power available of a device's processor and memory. In addition, contained applications within a TEE will be separated through software and cryptographic functions. A TEE can also be set to only accept previously authorized code.

How a TEE is implemented will differ depending on the use case, such as mobile payments, mobile identity, IoT or content protection. Still, the fundamental concepts stay the same -- trust, security and isolation of sensitive data.

Although a secure element requires no industry standards, a TEE does employ a set of industry standards to manage many remote devices at one time. These standards relate to the operations of encryption key management, end-to-end security and lifecycle applications. Service providers, mobile network operators, OS developers, application developers, device manufacturers, platform providers and silicon vendors are all contributing to efforts to standardize TEEs.

Following the TEE isolation philosophy, TEE remote management is designed so that specific remote managers can receive control of a subset of applications, but cannot interfere with the rest of those in the TEE. For example, an original equipment manufacturer and a bank could manage their TAs, but neither could interfere with the others.

Applications and services

Applications inside the TEE are considered trusted applications. The data stored on and processed by TAs is protected, and interactions -- whether between applications or the device and end user -- are executed securely.

TEEs enable the following services:

- **Secure peripheral access.** TEEs can directly access and secure peripherals such as the touchscreen or display, offering protection for fingerprint sensors, cameras, microphones and speakers.
- **Secure communication with remote entities.** These environments can secure data, communications and cryptographic operations. Encryption private and public keys are stored, managed and used only within the secure environment.
- **Trusted device identity and authentication.** Some TEEs use Roots of Trust, which enable the legitimacy of a device to be verified by the connected service with which it is trying to enroll.

How TEE was developed

TEEs were created to further secure previously trusted platforms. In the mid-2000s, the implementation of TEEs began to become a standards-based approach for internet-connected devices. More organizations began developing TEEs, such as Trusted Logic and Texas Instruments in 2004. In 2006, Arm developed a commercialized product for TEE called TrustZone. That same year, the Open Mobile Terminal Platform wrote the first set of requirements for trusted environments, which were revised again in 2008.

The 2010s saw a growth in the use of TEEs. In 2012, GlobalPlatform and the Trusted Computer Group began working together to create another set of specifications for TEE, used in conjunction with the Trusted Platform Module. Since then, GlobalPlatform has been the driving force behind TEE standardization.

TEE current and future uses

TEE is not an emerging technology. For example, apps such as Samsung Pay or WeChat Pay, and many of the leading Android device makers' flagship phones, all use a TEE. In this way, TEE has become a central concept when considering sensitive data security in smartphones.

The increased use of IoT is also expanding the need for trusted identification to new connected devices. TEE is one technology helping manufacturers, service providers and consumers to protect their devices, intellectual property and sensitive data.

The trusted execution environment is already bringing value to a range of device types and sectors. The technology opens up a number of options and possibilities for hardware isolation. For example, developers can add additional value to their

services by using TEEs with complementary technologies such as digital holograms that sit alongside TEEs to add value for service providers and device makers.

This was last updated in March 2023

Continue Reading About trusted execution environment (TEE)

- Trusted execution environments: What, how and why?
- How public cloud vendors tackle confidential computing
- Confidential computing promises secure cloud apps
- Consider IoT TPM security to augment existing protection

Related Terms

Electronic Data Interchange (EDI)

Electronic Data Interchange (EDI) is the transfer of data from one computer system to another by standardized message formatting ... See complete definition

virtual reality

Virtual reality, or VR, is a simulated three-dimensional (3D) environment that lets users explore and interact with a virtual ... See complete definition

virtualization sprawl (VM sprawl)

Virtualization sprawl is a phenomenon that occurs when the number of virtual machines (VMs) on a network reaches a point where ... See complete definition

Dig Deeper on Systems automation and orchestration