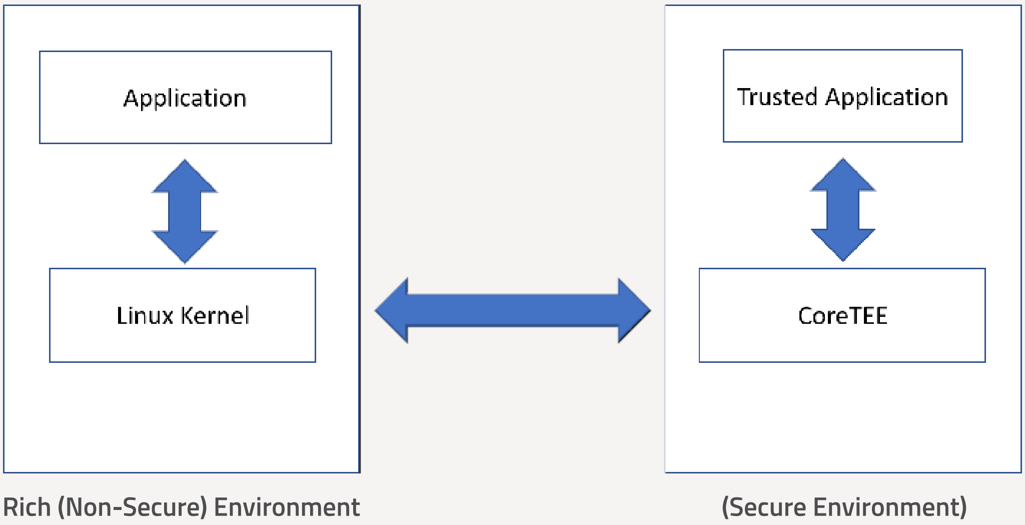
Protecting Intellectual Property (AI / ML Algorithms) at the Edge with EmSPARK™ Security Suite

Many IoT products implement Artificial Intelligence (AI) or Machine Learning (ML) to perform tasks that require them to act without being specifically programmed. The algorithms and models that deliver this functionality represent critical intellectual property (IP), and create significant value for the products and their vendors. These algorithms and models simply cannot be compromised; theft of this kind of intellectual property can create long-term damage to a company's revenue and brand.

Critical applications, such as AI/ML, can be protected by housing them in a secure area with restricted access. Using Arm TrustZone™ architecture, a System-on-Chip's (SOC) memory can be partitioned into a Rich (Non-secure) Environment and a Secure Environment. The Rich Environment is larger in memory size—typically hundreds of Megabytes—and houses known (public) software, such as Linux kernels and open source supporting applications (e.g., OpenSSL). The Secure Environment has a small memory size—less than a Megabyte—and houses the following:

1. The Trusted Execution Environment (TEE) secure operating system (Sequitur Labs' product is called the CoreTEE™).
2. Applications that need to be protected, along with applications that support the securing process (e.g., key / certificate management and secure data storage). These are known as Trusted Applications or TAs.

Shared memory allows access between the two environments.



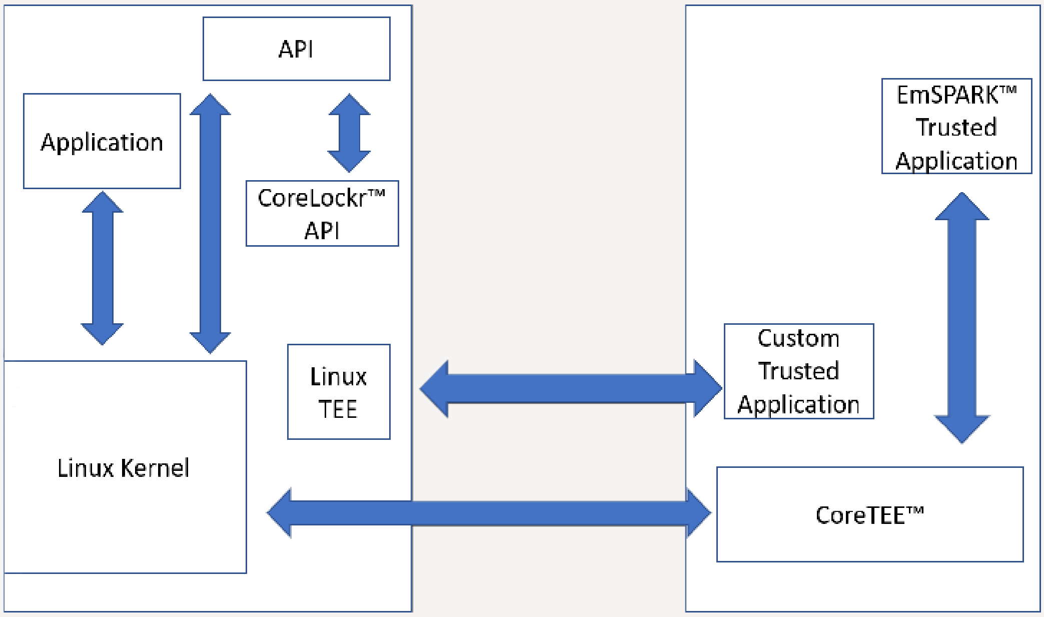
In this architecture, the secure application process works as follows:

1. The IoT device's application, running in the Rich (Non-secure) Environment, makes a request to the Linux kernel to access the Secure Environment.
2. The Linux kernel is suspended on one of the SoC's cores, giving access to CoreTEE™; CoreTEE™ resumes from suspension and invokes the requested Trusted Application.
3. CoreTEE™ accesses the non-secure memory (RAM) and acquires data through the shared memory between the two environments.

Sequitur Labs provides four Trusted Applications to support the secure environment:

1. **Crypto TA:** encryption and hashing algorithms
2. **Certificate Management TA:** for managing credentials
3. **Secure Storage TA:** for storing critical data in the Secure Environment
4. **TLS TA:** secure sockets for communication with external servers

While this architecture works well for housing public applications—e.g., an open source web server—in the Rich Environment, an open OS, such as a Linux kernel, is often a collection of very versatile and powerful tools. This makes the OS, and its housed applications, prone to vulnerabilities. To protect a business-critical application such as an AL/ML algorithm, it is recommended that it be developed as a Trusted Application (TA) and housed in the Secure Environment.



In the architecture illustrated above, both the customer's application and the supporting Trusted Applications are housed in the Secure Environment. The customer's application is accessed using the Rich Environment's Trusted Execution Environment (TEE) interface (e.g., a Linux TEE driver). Sequitur Labs' Trusted Applications (TAs) are accessed by Sequitur's CoreLockr™ APIs. IoT Device Vendors can develop Trusted Applications supporting their critical algorithms using Sequitur Labs' Software Developer's Kit (SDK).

Learn More

Download the free evaluation kits and user's guide for more details and code examples

Download "Surviving The IoT Wave: EmSPARK™ Security Suite" Whitepaper

©2020 Sequitur Labs Inc. All rights reserved.
Photo by John Salvino on Unsplash.
MSBEm-0003-Rev A. Printed in the U.S.A.