Providing Access to TPM from Edge Containers

Motivation

Trusted Platform Module (TPM) is a crypto device present on some of the EVE hardware platforms. It is used for providing security features such as secure crypto keys, attestation, measured boot, disk encryption etc. Today EVE platform software uses TPM to provide device identity rooted to TPM[1], disk encryption[2] etc.

EVE, as you know, provides a virtualisation engine, where applications run as either Virtual Machines or Containers, or commonly Edge Containers as they are called. The Edge Container Applications themselves might need access to TPM for implementing security features in their applications. An example would be an Edge App creating its crypto keys used for signing, attestation etc using TPM device, for hardening security aspects of its authentication/attestation protocol with its Cloud counterpart.

Since TPM is a hardware device, EVE software needs to expose TPM capabilities to Edge Containers through the virtualisation layer, so that Edge Container Apps can continue to use TPM as they were in a bare-metal environment. While this can be addressed by emulating a full-fledged TPM device and present a virtual TPM device to Edge Containers, it provides us with the following challenges:

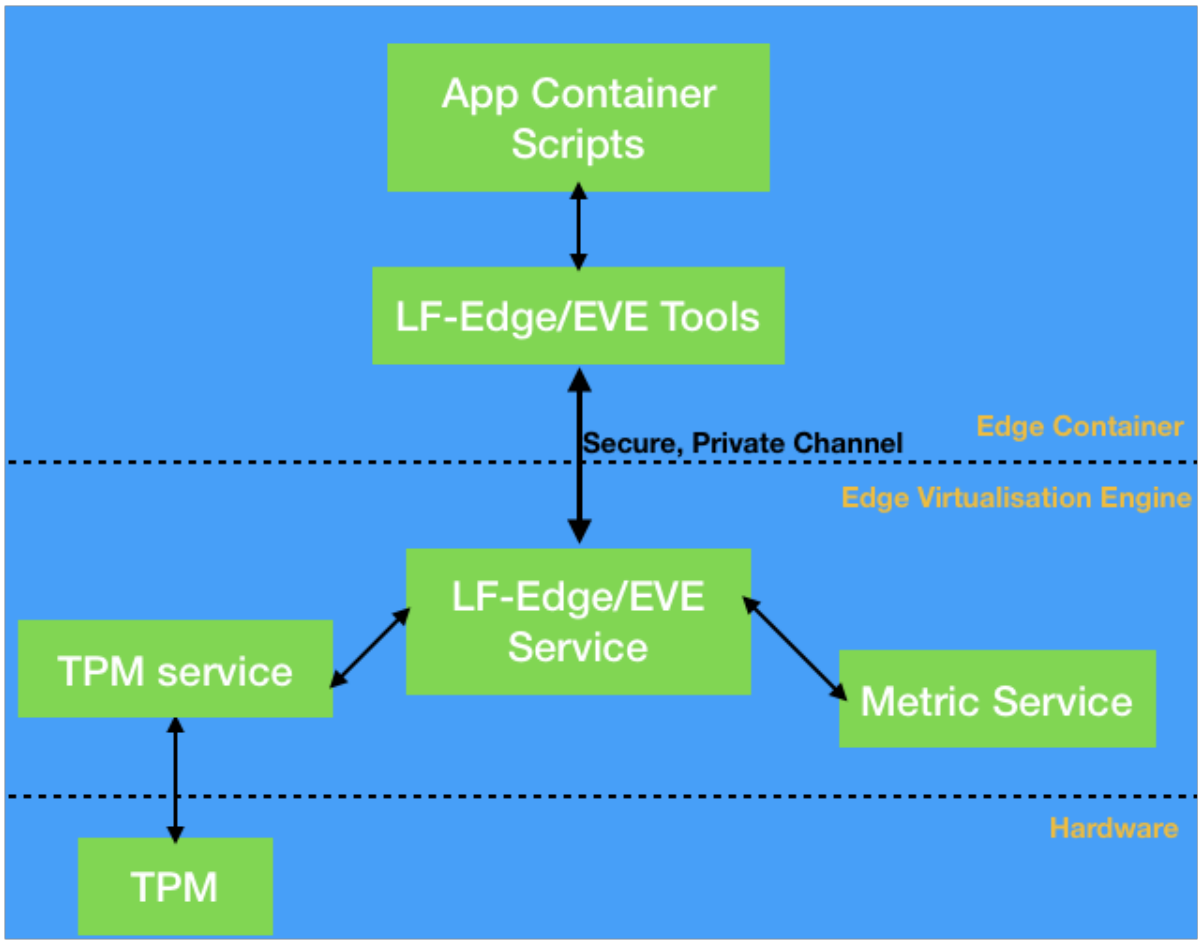
a) Implementing a secure vTPM backend across ARM and X86 architectures, protecting the data store of vTPMs

b) A mature, well-tested open source implementation of vTPM 2.0 in XEN/QEMU environment that we can leverage on EVE

both of which need significant time to be available/developed, and therefore an interim solution is needed till we get full-fledged vTPM working on EVE.

Proposal Description

Therefore, it is proposed to have an interim solution to address this TPM requirement by Edge Container Application developers, by providing a communication channel between EVE and Edge Containers, and have a well defined set of APIs to expose a set of(albeit limited) TPM operations on the TPM hardware, to the Edge Containers. The communication channel is described below:



The proposal is therefore,

a) To implement a microservice on EVE, which can listen to requests coming in from Edge Containers

b) Edge Container will have a set of tools - This can be installed via Cloud-init infrastructure when Edge Containers are deployed on EVE node. This is not new - Many hypervisors have similar set of tools for providing a way to communicate with the hypervisor and provide some services.

c) The tools will talk to the EVE microservice through a private RPC channel, for serving the Edge Container requirements.

d) The microservice will in turn talk to different pillar agents in the backend to service the actual request and get back the result

e) Edge Containers can use these tools for their TPM requirements; in the future the toolset can be extended to provide additional capabilities, like reading exact resource usage(Memory/CPU/Network) of the Edge Container as seen by the EVE virtualization layer, for their own reporting etc.

An Example Usage

Let's say a bare-metal edge application is using tpm2-tools to access its TPM for generating a pair of AIK keys, and using TPM for signing a document using the AIK key. The same application would do the following, when running on EVE:

```
#Create a AIK pair, with RSA as the algorithm
 eve_tools_tpm2_genaik -g 0x1
 AIK Pair generated at persistent handle 0x81010000

 #Get public key saved in a given file in .pem format
 eve_tools_tpm2_pubgetaik -k 0x81010000 -f ak.pem

 #Get a message signed by the handle, with SHA256 hashing:
 eve_tools_tpm2_sign -k 0x81010000 -m message.txt -g 0x00B -s sign.bin
```

References

1] Device Identity rooted at TPM

2] Encrypting Sensitive Information at Rest at the Edge