TEEP Use Case for Confidential Computing in Network

IETF 114
TEEP Meeting

Motivation

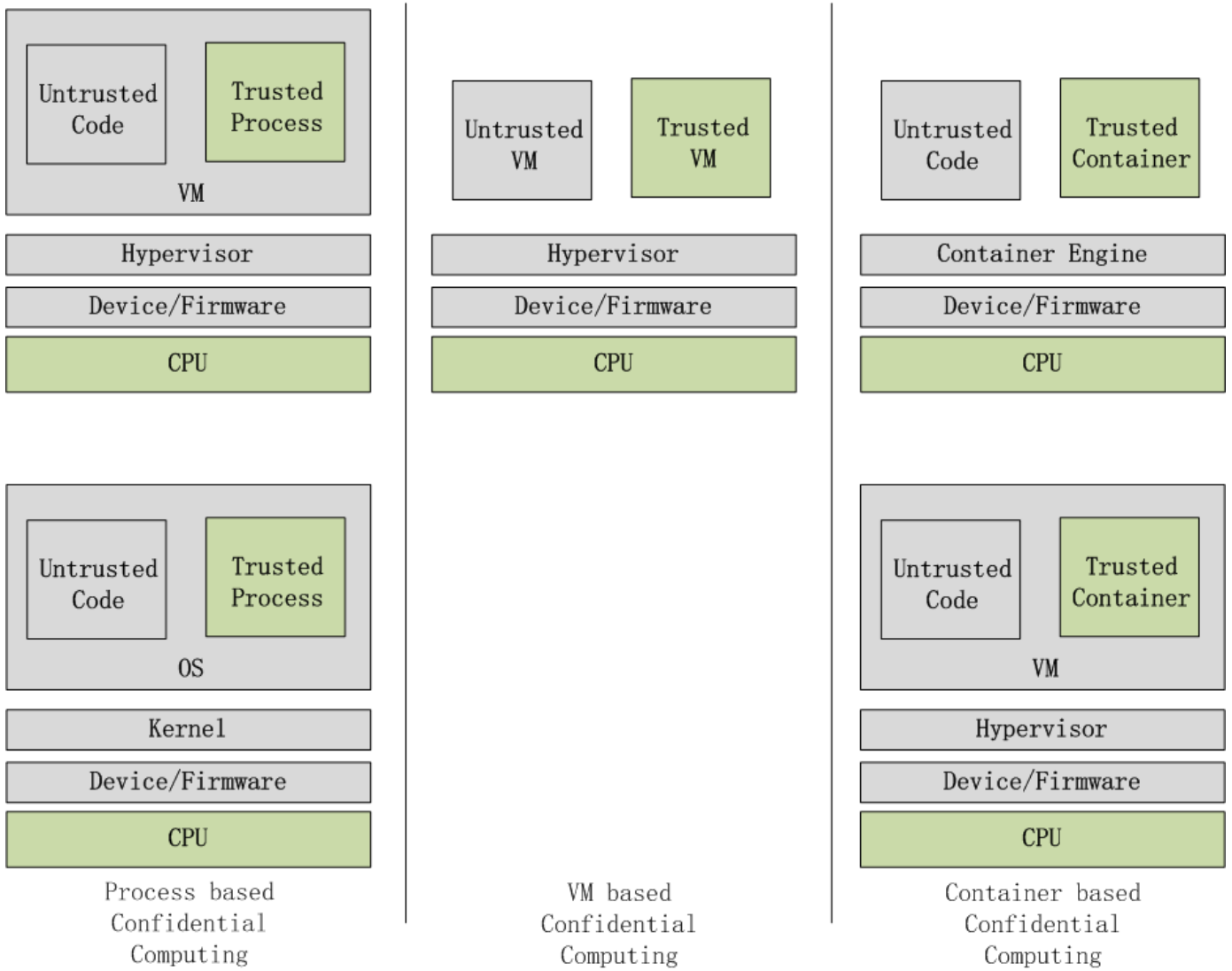
Confidential computing is the protection of data in use by hardware based trusted execution environment.

When using confidential computing in network, some issues need to be clarified:

- What is the architecture of confidential computing in network
- What kind of application packages a network user should use.
- What kind of steps network user should follow to deploy application packages

This draft uses TEEP architecture and protocol to illustrate confidential computing in network, includes the **notional architecture**, the **relevant package type of application** and the **deploy steps**.

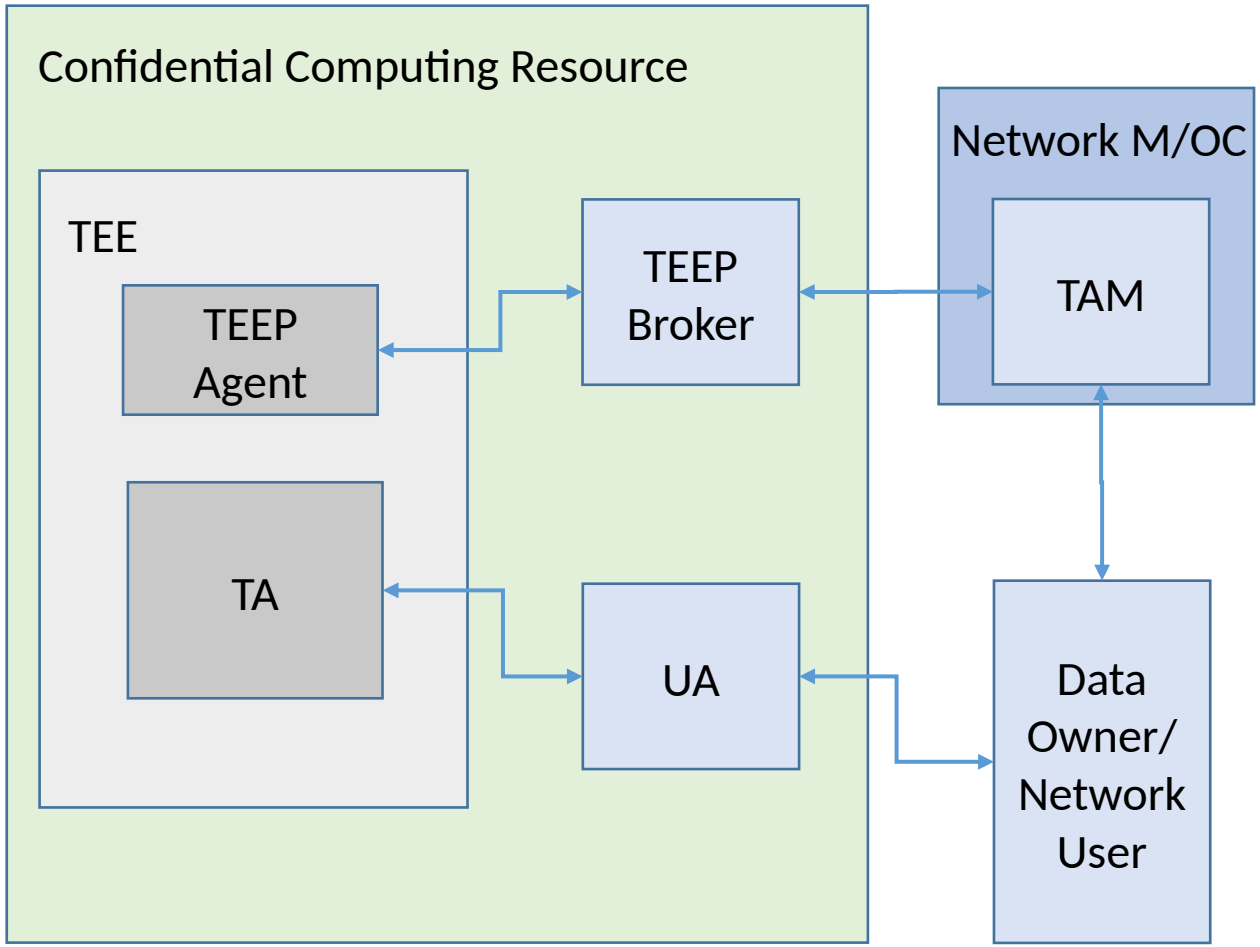
Confidential Computing Instance Type



In general, three kinds of confidential computing instance type could be exist in network :

- **Process based**: the process is protected by TEE, like SGX, TrustZone.
- **VM based**: the whole VM is protected by TEE, like SEV-SNP, TDX. (Processes and containers in this VM are also confidential)
- **Container based**: the container is protected by TEE.

Notional architecture



- TAM: Trusted application manager in Network M/OC.
- Data Owner: The network user who owns personalization data.
- TA: Trusted application (could be process, container, and VM)
- UA: Untrusted application
- TEEP Broker: Communication between TEEP Agent and TAM.
- TEEP Agent: Communication with TEEP Broker, deploy TA in TEE.

App Packages and Deploy Steps

Principle 1: Personalization Data can only be processed by TA after remote attestation;

Principle 2: Personalization Data must be transferred securely (encrypted or during secure channel).

Package Mode	(UA, TA, PD)		
CC Instance	Process in physical or virtual machine	Container in physical or virtual machine	VM
Hardware Architecture	TrustZone SGX	TrustZone SEV CCA TDX	SEV CCA TDX
Deploy Steps	{att TEEP Agent TA->Trusted Process PD->TA UA->REE}	{att TEEP Agent TA->Trusted Container, PD->TA, UA->REE}	{att TEEP Agent, TA->Trsuted VM, PD->TA, UA->REE}

App Packages and Deploy Steps

Package Mode	(UA, TA), (PD) or （UA 、TA 、PD）		
CC Instance	Process in physical or virtual machine	Container in physical or virtual machine	VM
Hardware Architecture	TrustZone、SGX	TrustZone、SGX、SEV、CCA、TDX	SEV、CCA、TDX
Deploy Steps	{UA->REE， TA->Trusted Process， att TEEP Agent， PD->TA}	{UA->REE， TA->Trusted Container att TEEP Agent, PD->TA}	{UA->REE, TA->Trusted VM, att TEEP Agent, PD->TA}

Package Mode	（TA、PD）或 UA		
CC Instance	Process in physical or virtual machine	Container in physical or virtual machine	VM
Hardware Architecture	TrustZone、SGX	TrustZone、SGX、SEV、CCA、TDX	SEV、CCA、TDX
Deploy Steps	{UA->REE， Att TEEP Agent， TA&PD->Trusted Process}	{UA->REE， Att TEEP Agent, TA&PD->Trusted Container}	{UA->REE, Att TEEP Agent, TA&PD->Trusted VM}

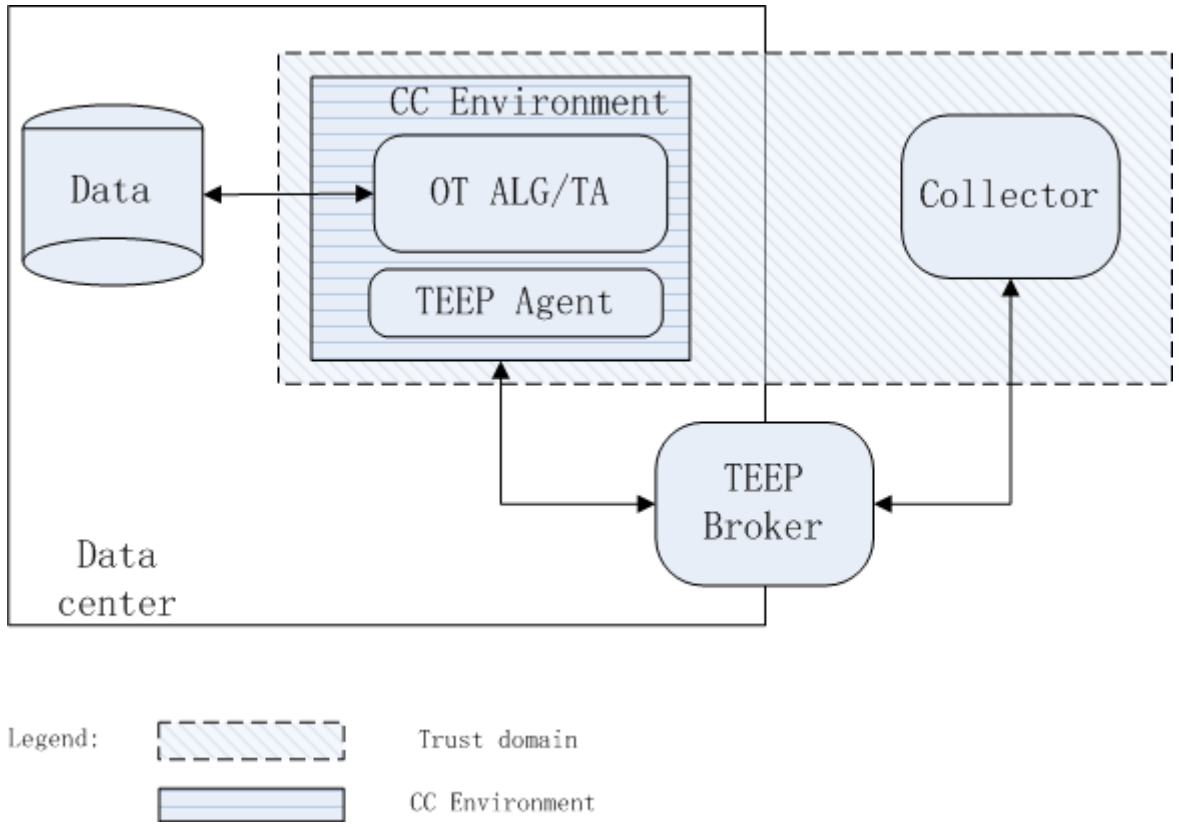
App Packages and Deploy Steps

Package Mode	【TA】【PD】		
CC Instance	Process in physical or virtual machine	Container in physical or virtual machine	VM
Hardware Architecture	TrustZone、SGX	TrustZone、SGX、SEV、CCA、TDX	SEV、CCA、TDX
Deploy Steps	{TA->Trusted Process, att TEEP Agent、PD->TA}	{TA->Trusted Container、att TEEP Agent, PD->TA}	{TA->Trusted VM、att TEEP Agent, PD->TA}

Package Mode	【TA, PD】		
CC Instance	Process in physical or virtual machine	Container in physical or virtual machine	VM
Hardware Architecture	TrustZone、SGX	TrustZone、SGX、SEV、CCA、TDX	SEV、CCA、TDX
Deploy Steps	{att TEEP Agent、TA&PD->Trusted Process}	{att TEEP Agent, TA&PD->Trusted Container}	{att TEEP Agent, TA&PD->Trusted VM}

One Interesting Scenario

With this use case, TEEP and confidential computing could be introduced to different scenarios like oblivious transfer.



Original OT : The Collector(Network User) queries certain information from Data center. The Data center cannot know the specific query information.

In order to do that, OT algorithm will create lots of redundant query result to puzzle Data center.

This will cause lots of network overhead to transfer this redundant query result to Collector.

CC OT : deploy OT algorithm (TA) to Data Center, replace the network overhead by memory access, only transfer the correct query result to Collector.

Summary

- This use case is trying to use TEEP architecture and protocol to illustrate how to use confidential computing in network and lists out the relevant steps and package mode.

- Some issues remain open or not in this draft's scope:

  E.g. How to process remote attestation and how to create "secure channel" about confidential computing are still under discussion, maybe covered by other groups like RATs.

- In the end, we would like this draft to be adopted as WG draft.

Thanks