TEEP Use Case for Confidential Computing in Network 02

IETF 115
TEEP Meeting

Issue1 Cloud scenario should be included

The **Abstract** of this draft has been changed to:

> This document is a use case and extension of TEEP and could provide guidance for cloud computing, MEC and other scenarios to use confidential computing in network.

Issue2 security of confidential container should be clarified

The CCC common-terminology defined the confidential contianer as in the below. This means the container process is protected by CC, and other components like runc, container-shim don’t have to be protected by CC. If a SEV-SNP CPU maintains a container in a VM, then this is a confidential VM rather than a confidential container.

> confidential container: the entrypoint process of an Open Container Initiative (OCI)-compliant 2 container image launched by an OCI container runtime such that the process is executed inside a hardware-based TEE, and it is protected from other confidential containers and any hosting environment in the TEE.

Issue3 specify or refer to secure channel in other document

TBD.

Haven’t found a definition of secure channel in IETF. Maybe *“Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)”* (draft-fossati-tls-attestation-01) could be used.

Issue4 typo and format correction

1, acronyms explanation about "MEC", "CAN" in page 1

2, expand CPU to computing units in page 2

3, reference missing about CCC white paper in page 4

4, replace SEV by SEV-SNP

5, etc.

Issue5 provision steps in 4.1: UA, TA and PD are bundled as a package

Original text: 3. TAM requests remote attestation to the TEEP Agent, TEEP Agent then response thesends evidence to TAM. The TAM works as the relying party and forwards the attestation result to network user.

4. After verification, the network user transfers the package to TAM and let TAM to transfer the package to TEEP Agent.

5. Network user establishes secure channel with TEEP agent via TAM, and transfers decryption key to TEEP Agent.

***Comments**: The network user could transfer encrypted package before attestation for efficiency.*

Either the user and TEEP agent could use some attested TLS protocol for key release that doesn't involve the TAM, or else the key could be considered as separate PD where the user is its own TAM for that piece, and use the TEEP protocol between TEEP Agent and network user to transfer the decryption key.

3. TAM requests remote attestation to the TEEP Agent, TEEP Agent then sends the evidence to TAM. The TAM works as Verifier in RATs architecture .

4. After verification, Network User works as Relying Party to receive the attestation result. If positive, Network User establishes secure channel with TEEP Agent, and transfers this package to TEEP Agent.

5. TEEP Agent deploys TA and personalization data in TEE, then deploy UA in REE

Issue6 provision steps in 4.2: PD is a separate package, TA and UA are separate or integrated

Original text: 3. Network user transfers UA and TA to confidential computing resource via TAM. TAM then deploys these two applications in REE and TEE respectively. (In SGX, UA must be deployed first, then let the UA to deploy TA in SGX.) 4. TAM requests remote attestation to the TEEP Agent, TEEP Agent then sends the evidence to TAM. The TAM works as the relying party and forward the attestation result to network user

Comments: Clarify "deploy" and "load" in this case.

3. Network User transfers UA and TA to confidential computing device via TAM. TAM then deploys these two applications in REE and TEE respectively. (In SGX, UA must be deployed first, then let the UA to load TA in SGX.)

4. TAM requests remote attestation to the TEEP Agent, TEEP Agent then sends the evidence to TAM. The TAM works as Verifier in RATs architecture.

5. After verification, Network User works as Relying Party to receive the attestation result. If positive, Network User establishes secure channel with TA, and deploys personalization data to the TA.

Issue7 provision steps in 4.3: TA and PD are bundled as a package, and UA is a separate package

Original text: 3. 1. Network user requests for confidential computing resource to the network M/OC. 2. TAM in M/OC orchestrates confidential computing device to undertake the request. 3. Network user transfers UA to TAM.

Comments: TAM is not in the path of UA distribution.

3. Network User deploys UA in REE.

4. TAM requests remote attestation to the TEEP Agent, TEEP Agent then sends the evidence to TAM. The TAM works as Verifier in RATs architecture.

5. After verification, Network User works as Relying Party to receive the attestation result. If positive, the Network User establishes secure channel with TEEP Agent and transfers the TA and PD package to TEEP Agent.

6. TEEP Agent deploys TA and PD.

Issue 8 & 10 introduction improvement

Comments: the introduction can improved by describing early on what the users represent in this scenario, and where the TEEs are located in the network fabric. Similar to the abstract - what is the motivation for doing this? Simply having it possible is not enough of a reason.

Related to issue 10, trying to use MPC to explain this usecase, TBD.

Issue9 specify data owner

data owner has been replaced by Network User:

Network User: Network User possesses personalization data and applications that need to be deployed on confidential computing device. For example in MEC, the autonomous vehicles could deploy private applications and data on confidential computing device to calculate onvehicle and destination road information without knowing by MEC platform.

Issue11 loosen deployment options

see issue 5,6,7

Issue12 The UA may be tampered and this may cause DoS attack or even DDoS attack

My personal opinion is that since UA is defined as untrusted, TEEP architecture cannot make sure its trustworthiness. So in some sense it seems the DOS attack cannot be totally denied. But if we could create secure channel betwen TEE and TAM or use some encryption format like COSE to encode the network data, the server side of this TEE device could discard those malicious network flow. As to TEEP broker, since it is for transparent forwarding and is also not trusted, it maybe not reliable to block malicious traffic.

Issue13 scope of this document

The scope of this document should not only include edge computing scenario. The scope could be any confidential computing environment which need to be configured by network.

Thanks