Workgroup: TEEP Working Group
Internet-Draft:
draft-yang-teep-usecase-for-cc-in-network-01
Published: 3 August 2022
Intended Status: Informational
Expires: 4 February 2023

Authors: P. Yang, China Mobile
M. Chen, China Mobile
L. Su, China Mobile
T. Pang, Huawei Technology Co.,Ltd.

TEEP Usecase for Confidential Computing in Network

Abstract

Confidential computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment. Confidential computing could provide integrity and confidentiality for users who want to run application and process data in that environment. When confidential computing is used in network like MEC and CAN which provide computing resource to network users, TEEP protocol could be used to provision network user's data and application in TEE environment in confidential computing resource. This document focuses on using TEEP to provision network user's data and application in confidential computing in such network. This document is a use case and extension of TEEP and could provide guidance for MEC, CAN and other scenarios to use confidential computing.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Confidential Computing Consortium defined the concept of confidential computing as the protection of data in use by performing computation in a hardware-based Trusted Execution Environment" [CCC-White-Paper]. In detail, CPU with confidential computing feature could generate an isolated hardware-protected area, in which data and applications will be protected from illegal access or tampering.

In the scenario of confidential computing in network, network users will attest the TEE in confidential computing and provision private data and applications to that TEE by network. This network could be a MEC[MEC], CAN or other network that provide computing resource to users.

TEEP architecture [I-D.ietf-teep-architecture] defined the design and standardization of a protocol for managing the lifecycle of trusted applications running inside a TEE. In confidential computing, this TEE can also be provisioned and managed by TEEP protocol.

This document illustrates how a network user uses the TEEP protocol to provision its private data in confidential computing resource. The intended audiences for this use case are network users and operators who are interested in using confidential computing in network.

2. Terminology

2.1. Terms

TA: Trusted Application

UA: Untrusted Application

PD: Personalization Data

2.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Notional Architecture of using confidential computing in network

As shown in figure 1 is the architecture of using confidential computing in network. Two new components Network User and Network M/OC are introduced in this document. Interactions of all components in this scenario are described in the following paragraphs.

```
+--------------------------------------+
| Confidential Computing Resource      |
|                       +--------+     |
|  +-------------+      |        |     |   +------------+
|  | TEE         |      | TEEP   |     |   | +-------+  |
|  | +--------+  |  +---> Broker <----------->       |  |
|  | | TEEP   |  |  |   |        |     |   | |  TAM  |  |
|  | | Agent  |<----+   |        |     |   | |       |  |
|  | +--------+  |      |        <--+  |   | +---^---+  |
|  |             |      +--------+  |  |   +-----|------+
|  | +--------+  |                  |  |         |
|  | |   TA   |  |      +-------+   |  |         |
|  | |        |<-------->       |<--+  |         |
|  | +--------+  |      |  UA   |      |   +-----V------+
|  +-------------+      |       |<---------> Data Owner |
|                       +-------+      |   +------------+
+--------------------------------------+
```

Figure 1: notional architecture of confidential computing in network

*Network user possesses private data and application that need to be deployed in confidential computing resource. For example in MEC, the autonomous vehicles could deploy private application and data to confidential computing resource to calculate on-vehicle and destination road information without knowing by MEC platform.

*Network Management/Orchestration Center exists in the management and orchestration layer of network. Network user will use the M/OC to request for computing resource. The TAM is inside the M/OC to provide management function to TEEP agent via TEEP broker.

*Confidential Computing Resource is composed by confidential computing devices that connected by the network and can provide service to network user.

*Package which will be mentioned in the following Usecases section is a unit that is signed or encrypted by Data Owner and could be deployed in TEE/REE or treated as application data. TA (Trusted Application) in confidential computing could be an application, or packaged with other components like library, TEE shim or even Guest OS. The specific package of confidential computing application could refers to the wihte paper of common terminology of CCC(reference needed).

The connection between network user and M/OC depends on the implementation of specific network. The connection between network user and UA (Untrusted Application) or TA depends on the implementation of application. The connection between TAM, TEEP

Broker and TEEP Agent refers to the TEEP protocol [I-D.ietf-teep-protocol].

4. Usecases

The basic process of how a network user uses confidential computing is shown below. In confidential computing, the bundle of an UA, TA, and PD (Personalization Data) refers to case 1,2,3,4 of TEEP architecture section 4.4. Case 5 and 6 are new cases that possible in implementation. At present, the main instances types exist in industry of confidential computing are confidential process,confidential container and confidential VM.

4.1. UA, TA and PD are bundled as a package

This use case refers to the case 1 of TEEP architecture. If the network user provides this package, the process of TEEP is as follow. Whenever PD is involved in a package, this package must be encrypted, similarly hereinafter.

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. TAM requests remote attestation to the TEEP Agent, TEEP Agent then response the evidence to TAM. The TAM works as the relying party and forward 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.

6. TEEP Agent deploys TA and personalization data, then deploy UA in REE via TEEP Broker.

As for inform network users to develop their applications, the mapping of UA, TA and implementations are shown in figure 2. This document gathers the main hardware architectures that support confidential computing, which include TrustZone, SGX, SEV, CCA and TDX.

The brace means the operation steps to deploy packages. The arrow means deploy package to a destination.

Package Mode	Case 1 (UA, TA, PD)		
Instance Type	Process in Physical or Virtual Machine	Container in Physical or Virtual Machine	VM
Hardware Architecture	TrustZone	TrustZone, SEV, CCA, TDX	SEV,CCA,TDX
Load Sequence	{att TEEP Agent, TA->TEE, PD->TA, UA->REE}	{att TEEP Agent, TA->Trsuted Container, PD->TA, UA->REE}	{att TEEP Agent, TA->Trsuted VM PD->TA, UA->Untrusted VM}

Figure 2: TEEP Implementation of Case 1

4.2. PD is a separate package, TA and UA are separate or integrated

This usecase refers to the case 2 and case 3 of TEEP architecture. The PD is a separate package, the UA and TA could be separated or integrated as a package. If the network user provides packages like this, the process of TEEP is as follow.

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 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 response the evidence to TAM. The TAM works as the relying party and forward the attestation result to network user.

5. Network user establishes secure channel with TA (via UA or via TAM or directly), and deploys personalization data to the TA.

The mapping of UA, TA and implementations are shown in figure 3.

Package Mode	Case 2 (UA, TA) (PD), Case 3 (UA) (TA) (PD)		
Instance Type	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
Load Sequence	{TA->TEE, att TEEP Agent, PD->TA, UA->REE}	{UA->REE, TA->trusted Container, att TEEP Agent, PD->TA}	{UA->untrusted VM, TA->trusted VM, att TEEP Agent, PD->TA}

Figure 3: TEEP Implementation of Case 2/3

4.3. TA and PD are bundled as a package, and UA is a separate package

In this case, the process of TEEP is as follow.

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.

4. TAM requests remote attestation to the TEEP Agent, TEEP Agent then response the evidence to TAM. The TAM works as the relying party and forward the attestation result to network user.

5. Network user transfers encrypted TA and PD to TAM. Then TAM transfers this package to TEEP Agent. Network user creates secure channel with TEEP agent (via TAM) and transfers the decryption key to TEEP agent.

6. TEEP agent decrypts this package and deploys TA and PD.

Package Mode	Case 4 (TA, PD) (UA)		
Instance Type	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
Load Sequence	{UA->REE, att TEEP Agent, TA&PD->TEE}	{UA->REE, att TEEP Agent, TA&PD->trusted Container}	{UA->untrusted VM, att TEEP Agent, TA->trusted VM}

Figure 4: TEEP Implementation of Case 4

4.4. TA and PD as a package, no UA

In this case, network user provides TA and PD as a package with no UA attached. The process of TEEP in this case is as follow.

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. TAM requests remote attestation to the TEEP Agent, TEEP Agent then response the evidence to TAM. The TAM works as the relying party and forward the attestation result to network user.

4. Network user transfers this package to TAM, and the TAM transfers this package to TEEP agent.

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

6. TEEP Agent decrypts this package and deploys TA and PD.

Package Mode	Case 5 (TA, PD)		
Instance Type	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
Load Sequence	{att TEEP Agent, TA&PD->TEE}	{att TEEP Agent, TA&PD->trusted Container}	{att TEEP Agent, TA->trusted VM}

Figure 5: TEEP Implementation of Case 5

4.5. TA and PD are separate packages, no UA

In this case, network user provides TA and PD as separate packages with no UA attached. The process of TEEP in this case is as follow.

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 transfer TA to TAM, and TAM deploys this TA to TEE through TEEP Agent.

4. TAM requests remote attestation to the TEEP Agent, TEEP Agent then response the evidence to TAM. The TAM works as the relying party and forward the attestation result to network user.

5. Network user establishes secure channel with TA (directly or via TAM) and transfers PD to it.

Package Mode	Case 6 (TA), (PD)		
Instance Type	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
Load Sequence	{TA->TEE, att TEEP Agent, PD->TA}	{TA->trusted Container, att TEEP Agent, PD->TA}	{TA->trusted VM, att TEEP Agent, PD->TA}

Figure 6: TEEP Implementation of Case 6

5. References

5.1. Normative Reference

[I-D.ietf-teep-architecture] Pei, M., Tschofenig, H., Thaler, D., and D. Wheeler, "Trusted Execution Environment Provisioning (TEEP) Architecture", Work in Progress, Internet-Draft, draft-ietf-teep-architecture-18, 11 July 2022, <https://www.ietf.org/archive/id/draft-ietf-teep-architecture-18.txt>.

[I-D.ietf-teep-protocol] Tschofenig, H., Pei, M., Wheeler, D., Thaler, D., and A. Tsukamoto, "Trusted Execution Environment Provisioning (TEEP) Protocol", Work in Progress, Internet-Draft, draft-ietf-teep-protocol-10, 28 July 2022, <https://www.ietf.org/archive/id/draft-ietf-teep-protocol-10.txt>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", DOI 10.17487/RFC2119, BCP 14, RFC 2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

5.2. Informative Reference

[CCC-White-Paper] Confidential Computing Consortium, "Confidential Computing: Hardware-Based Trusted Execution for

Applications and Data", January 2021, <https://confidentialcomputing.io/white-papers-reports/>.

[MEC] ETSI, "Multi-access Edge Computing (MEC);Framework and Reference Architecture", March 2022, <https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/03.01.01_60/gs_MEC003v030101p.pdf>.

[SGX] Intel, "Overview of Intel Software Guard Extension", June 2016, <https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/overview.html>.

Appendix A. Submodules in TEEP Agent

The original design of TEEP only includes TEEP Agent and TA inside TEE. While in confidential computing implementation, other submodules may also be involved in the TEE. In TEEP, these submodules could be covered by TEEP Agent.

In SGX based confidential computing, submodule could provide convenient environment or API in which TA does not have to modify its source code to fit into SGX instructions. Submodules like Gramine and Occlum .etc are examples that could be included in TEEP agent. If there is no submodule in TEEP agent, the TA and UA need to be customized applications which fit into the SGX architecture.

In SEV and other architectures that support whole guest VM as a TEE, TEEP agent doesn't have to use extra submodule to work as a middleware or API. However with some submodules like Enarx which works as a runtime JIT compiler, TA could be deployed in a hardware independent way. In this scenario, TA could be deployed in different hardware architecture without re-compiling.

Authors' Addresses

Penglin Yang
China Mobile
32 Xuanwumen West Street, Xicheng District
Beijing
100053
China

Email: yangpenglin@chinamobile.com

Meiling Chen
China Mobile
32 Xuanwumen West Street, Xicheng District
Beijing
100053
China

Email: chenmeiling@chinamobile.com

Li Su
China Mobile
32 Xuanwumen West Street, Xicheng District
Beijing
100053
China

Email: suli@chinamobile.com

Ting Pang
Huawei Technology Co.,Ltd.
127 Jinye Road, Yanta District
Xi'an
710077
China

Email: pangting@huawei.com