Workgroup: Internet Engineering Task Force
Internet-Draft: draft-yang-teep-ccican-00
Published: March 2022
Intended Status: Informational
Expires: 3 September 2022
Authors: P. Yang China Mobile
M. Chen China Mobile
L. Su China Mobile

architecture of confidential computing in computing aware network

Abstract

Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment. Especially in virtualization environments, confidential computing could protect data and applications from access or tampering by hypervisor or other privileged users. In Computing-Aware network, computing resource is an essential element to provide computing services for network users' applications. Introducing confidential computing in Computing-Aware network could mitigate the distrust of computing resource efficiently. This document provides the architecture of confidential computing in Computing-Aware network management plane to provide confidentiality and integrity for applications.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 2 September 2022.

Copyright Notice

Table of Contents

1. Introduction

The Confidential Computing Consortium defined the concept of confidential computing as "Confidential Computing is 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 processing data or running code will be protected from any illegal access or tampering. In cloud computing scenario, CPU with confidential computing feature could be used to protect users' applications and data from access or tampered by hypervisor, privileged users or other attackers in the cloud platform. In hardware industry, Intel, AMD, ARM and other chip venders have already released their confidential computing CPU series.

In Computing-Aware network, cloud-based computing resource prepared for applications is from different places like edge or data center. If the edge or data center is outsourced or even distributed in different security domains, not only the network administrator but also the application owner cannot trust the computing environment. The potential leakage of secret data or intellectual property will

restrict the range of applications. With the protection of confidential computing, users could trust the computing environment and make sure their sensitive data and intellectual property will not be leaked.

This document introduces confidential computing to Computing-Aware network and illustrates the general architecture in network management plane. Computing-Aware network designers and users could use this document as a information reference to enhance their security.

1.1. Terminology

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].

CC: Confidential Computing

CCR: Confidential Computing Resource

TEE: Trust Execution Environment

CCM: Confidential Computing Management

CCI: Confidential Computing Instance

TEEP: Trust Execution Environment Provisioning

TAM: Trusted Application Management

2. Motivation and Scope

2.1. Motivation

In Computing-Aware network, there is a suspicion about how to protect users' application and data efficiently. Computing resource in Computing-Aware network is more decentralized and ambiguous than regular cloud computing. The network may distribute users' applications in different computing platforms maintained by different administrators. If the computing platform is malicious, secret data and application intellectual property could be easily stolen or tampered. Confidential computing provides a new security model in where network users only need to trust the confidential computing hardware, firmware and the applications provided by users themselves, any other hypervisor or software in computing platform do not have to be trusted.

2.2. Scope

This document mainly focuses on the unique features of confidential computing in network management plane. Other network planes like control/forwarding/data which have no direct interaction with confidential computing features will be ignored.

3. General Architecture of Confidential Computing in Computing-Aware Network

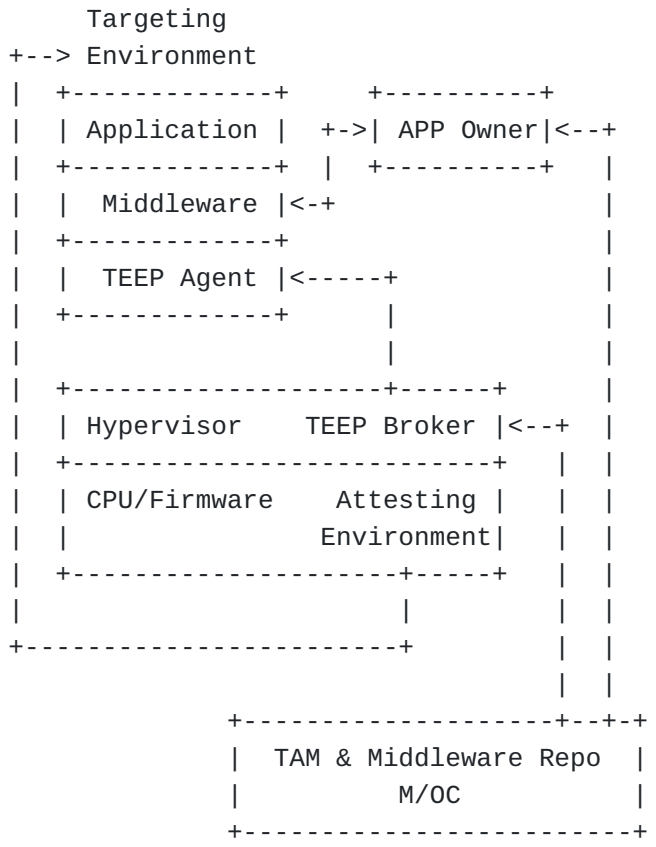

Figure 1: Architecture of Confidential Computing in Computing-Aware Network

Figure 1 shows the basic architecture of confidential computing in Computing-Aware Network. This architecture refers to RATs [I-D.ietf-rats-architecture] arch and TEEP[I-D.ietf-teep-architecture] arch for remote attestation and trust execution environment provisioning. Confidential computing needs the support of CPU, in which MUST have the function of generating isolated execution environment and attesting environment. The layer of Hypervisor is for virtualization.

(1) Targeting Environment

Targeting Environment is the computing environment e.g. virtual machine, process that could provide confidentiality and integrity for applications. When used for remote attestation, the Targeting Environment will be attested by application owner. Targeting environment includes Application, Middleware, and TEEP Agent.

(2) Application

Application which runs in Computing-Aware network.

(3) Middleware

Middleware in CC has two functions: enable remote attestation and environment provisioning; provide a user-friendly environment. Some confidential computing CPU like SGX needs to use middleware to provide a environment in where applications don't have to change their source code, e.g. Enarx [Enarx] and Occlum [Occlum].

(4) TEEP Agent

TEEP Agent is a module for provisioning middleware and application in Targeting Environment.

(5) TEEP Broker

TEEP Broker is only for communication between TEEP Agent and TAM, it doesn't have to know any confidential information.

(6) Attesting Environment

Attesting Environment is hardware based component, like Intel Quote SGX, AMD SEV-SP, etc. This component is a part of TCB, and is used to collect targeting environment evidence for remote attestation.

(7) M/OC

M/OC is the manage and orchestration console of Computing-Aware Network.

(8) TAM

Trust Application Management, this entity is for provisioning of application and relevant middleware.

(9) Middleware Repository

This repository keeps a variety of middleware packages, which is for TAM to access based on Application type and confidential computing hardware type.

4. Environment Provisioning

When deploying applications in Computing-Aware network, TAM will choose confidential computing environment and relevant Middleware to fit their applications. Meanwhile, Computing-Aware Network needs to provide the secure procedure of provisioning middleware and applications. This document uses TEEP as reference to provision Middleware and applications in Computing-Aware network.

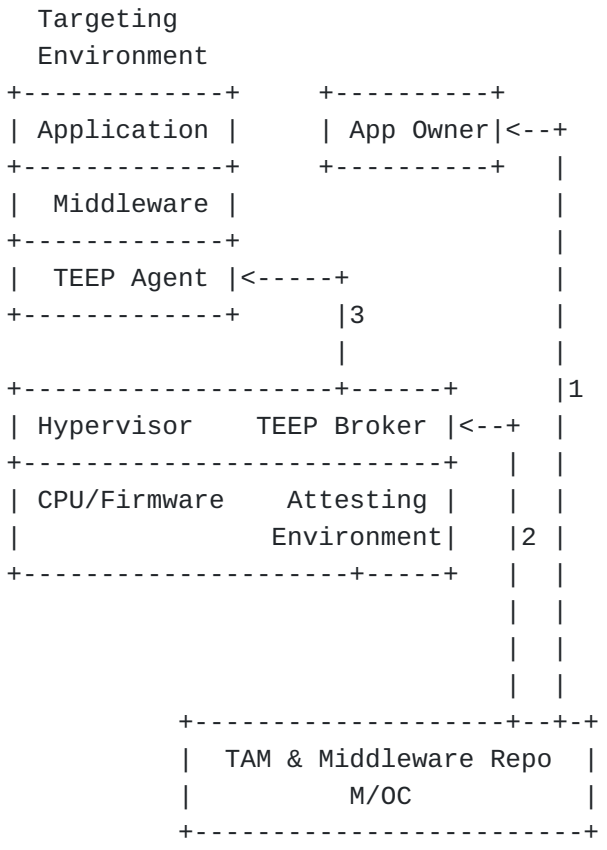

Figure 2: Application and Middleware Provisioning in Computing-Aware Network

The Provisioning steps in Computing-Aware Network are illustrated below.

(1) First, Application owner requests for confidential computing resource in Computing-Aware Network. Second, based on the request and confidential computing resource type, TAM will chose appropriate middleware.

(2) TAM establishes connections with TEEP Broker to transfer provisioning information.

(3) TEEP Broker triggers the confidential computing platform to create Targeting Environment with TEEP Agent. Then TEEP Broker

establishes connections with TEEP agent. TEEP agent receives the provisioning information and unpacks it as Middleware.

Need to clarify that at this stage the Middleware dosen't contain any secret information. The secret information of application should be provisioned after remote attestation. The specific mechanism of building targeting environment is based on specific CPU and is out of scope of this document.

5. Remote Attestation

In Computing-Aware Network, remote attestation is used for application owner to appraise if the Targeting Environment is trusted. Only after remote attestation, application owner could trust the confidential computing environment and deploy secret information. The general architecture of remote attestation in Computing-Aware Network is shown below.

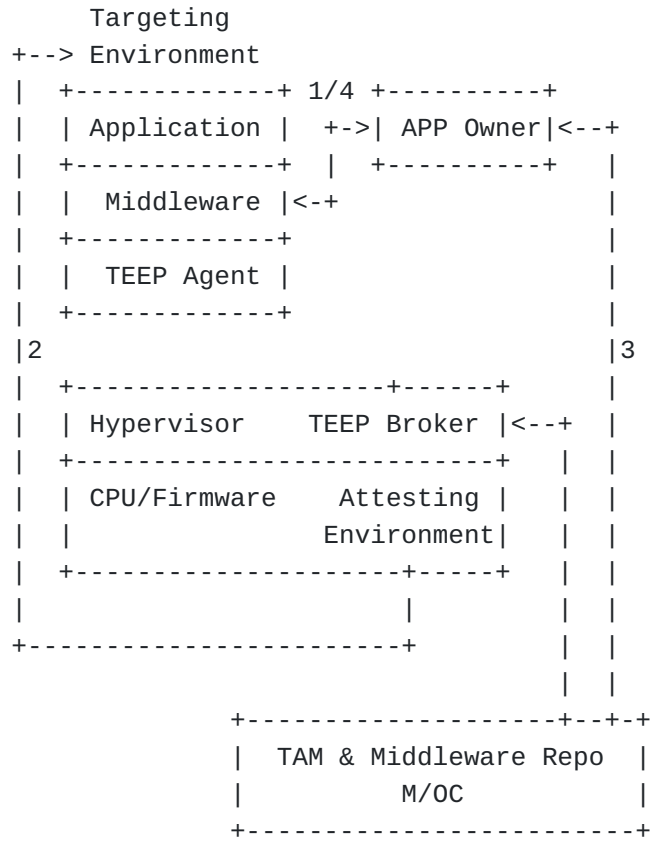

Figure 3: Remote Attestation in Computing-Aware Network

The remote attestation steps in Computing-Aware Network are shown below. After appraising the remote attestation evidence, the application owner could deploy secret data in Targeting Environment.

(1)

Application owner establishes secure connection with middleware and launches remote attestation request with certain parameters like nonce.

(2) Targeting Environment launches evidence collection by Middleware. Middleware sends request to Attesting Environment for remote attestation evidence. After generating evidence by Attesting Environment, the evidence will be sent back to Middleware.

(3) The Application Owner requests for TEEP agent and middleware source code to generate reference value and appraise the remote attestation evidence.

(4) The Targeting Environment sends the evidence to Application Owner. After appraising, Application Owner sends its application and private data to Targeting Environment.

6. Use Case

Confidential computing provides confidentiality and integrity of data and applications in the running stage. This document depicts the abstract architecture of confidential computing from the perspective of Computing-Aware Network. The following are some use cases of confidential computing in Computing-Aware Network.

VR/AR Application: Users wants to use Computing-Aware Network to host VR communication and interaction with other user. They don't want their conversation to be awared by the network. And it is hard to encrypt all the VR context because of unacceptable cost. So, the users choose confidential computing to protect their privacy. After the remote attestation of computing environment, the users could transfer and process private information in Computing-Aware Network.

Medical Imaging Aalysis: A medical institute wants to use Computing-Aware Network to share and process medical images in different branches. One primary concern is that they don't want the patients' medical images to be leaked. So they choose confidential computing to process these images.

7. Security Considerations

The root of trust of confidential computing is the CPU hardware. Application Owner could use the certificate or signature in remote attestation information to verify the identity of CPU. The connections between Application Owner and their applications are protected by security protocols like TLS.

8. Acknowledgements

The author would like to thank Eric Voit, Mike Bursul and Dave Thaler in CCC group who have provided valuable supports and suggestions.

9. IANA Considerations

This memo includes no request to IANA.

10. References

10.1. Normative References

[I-D.ietf-rats-architecture] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote Attestation Procedures Architecture", Work in Progress, Internet-Draft, draft-ietf-rats-architecture-15, 8 February 2022, <https://www.ietf.org/archive/id/draft-ietf-rats-architecture-15.txt>.

[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-16, 28 February 2022, <https://www.ietf.org/archive/id/draft-ietf-teep-architecture-16.txt>.

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

10.2. Informative References

[CCC-White-Paper] Confidential Computing Consortium, "Confidential Computing: Hardware-Based Trusted Execution for Applications and Data", 2021, <https://confidentialcomputing.io/wp-content/uploads/sites/85/2021/03/confidentialcomputing_outreach_whitepaper-8-5x11-1.pdf>.

[Enarx] Profian, Inc., "Enarx", 2022, <https://enarx.dev/docs/Technical/Introduction>.

[Occlum] Occlum, "Occlum", 2022, <https://occlum.io/>.

Authors' Addresses

Penglin Yang

China Mobile

Email: yangpenglin@chinamobile.com

Meiling Chen
China Mobile

Email: chenmeiling@chinamobile.com

Li Su
China Mobile

Email: suli@chinamobile.com