Secure Bootloader for Confidential Computing

Jiewen Yao, Intel
Ken Lu, Intel
Notices & Disclaimers

• Intel technologies may require enabled hardware, software or service activation.

• No product or component can be absolutely secure.

• All product plans and roadmaps are subject to change without notice.

• The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

• Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.
Agenda

• Measurement and Trust Chain
• Attestation and Disk Decryption
Confidential Computing in Cloud Usage

Confidential VM Use Case

VM Guest
- VM Workloads in VM OS
- Kernel/Initrd
- Bootloader (shim/grub)
- OVMF (Open Virtual Machine Firmware)

Bare Metal Host
- Libvirt
- Qemu

Confidential Container Use Case

Simplified VM Guest
- Container
- Kernel/Initrd
- TD-shim

Bare Metal Host
- Cloud Hypervisor

Tenant
CSP

Cloud Hypervisor

Container
Remote Attestation Server

Confidential Guest VM

Quote Agent

Workload

Bootloader, Kernel, initrd

Open Virtual Machine Firmware (OVMF)

FwCfg, VirtIO

QEMU

TCB

Host

\[ \text{Quote} = \text{Sign} \left( \sum M_{TCB} + M_{OVMF} + M_{OS} \right) \]

* OS: means bootloader (like shim/grub), kernel, initrd. It can be also extended for more runtime measurement like dynamic kernel module.
TDREPORT and Measurement

Confidential Guest VM
- Kernel, initrd
- Bootloader
  - TDX Virtual Firmware (OVMF)
    - Boot Firmware Volume
    - Configuration Firmware Volume
- TD-Hob
- QEMU/KVM
- SEAM
- Host

Launch: MROwner/MRConfig/MROwnerConfig

Refer: https://github.com/tianocore/edk2/blob/master/MdePkg/Include/IndustryStandard/Tdx.h
UEFI Confidential Computing Interface

• **Interface**
  • EFI_CC_MEASUREMENT_PROTOCOL
    • Abstract the measurement for virtual firmware in confidential computing environment.
    • Similar to TPM2: EFI_TCG2_PROTOCOL
  • CCEL ACPI Table
    • Provide the CC event log to the operating system.
    • Similar to TPM2: TPM2 ACPI table

• **Code**
  • EDKII - CcMeasurement
    • [https://github.com/tianocore/edk2/blob/master/MdePkg/Include/Protocol/CcMeasurement.h](https://github.com/tianocore/edk2/blob/master/MdePkg/Include/Protocol/CcMeasurement.h)
  • Shim Enabling (Thanks Robbie Harwood)
    • [https://github.com/rhboot/shim/commit/4fd484e4c29364b4fdf4d043556fa0a210c5fdfe](https://github.com/rhboot/shim/commit/4fd484e4c29364b4fdf4d043556fa0a210c5fdfe)
  • Grub Enabling (Thanks Daniel Kiper)
    • [https://git.savannah.gnu.org/cgit/grub.git/commit/?id=4c76565b6cb885b7e144dc27f3612066844e2d19](https://git.savannah.gnu.org/cgit/grub.git/commit/?id=4c76565b6cb885b7e144dc27f3612066844e2d19)

• **Specification**
  • Intel GHCI specification (published)
    • [https://cdrdv2.intel.com/v1/dl/getContent/726790](https://cdrdv2.intel.com/v1/dl/getContent/726790)
  • UEFI Confidential Computing Extension
    • UEFI 2.10 - [https://uefi.org/specs/UEFI/2.10/38_Confidential_Computing.html#confidential-computing](https://uefi.org/specs/UEFI/2.10/38_Confidential_Computing.html#confidential-computing)
    • ACPI 6.5 - [https://uefi.org/specs/ACPI/6.5/05_ACPI_Software_Programming_Model.html#cc-event-log-acpi-table](https://uefi.org/specs/ACPI/6.5/05_ACPI_Software_Programming_Model.html#cc-event-log-acpi-table)
CC Measurement Flow in Pre-Boot

OVMF (virtual FW)

CCEL ACPI


Produce

EFI_CC_MEASUREMENT_PROTOCOL

TDX MR


TCG PCR Register

0 1 2-6 7 8-15 >=16

Produce

SHIM Measured Objects

Secure Boot Keys Variable

Grub2 Measured Objects

Kernel Initrd Grub Module

Consume

Linux Bootloader Phase

Boot time or Runtime Attestation

Consume

SHIM

OVMF Measured Objects

Variable Qemu Cfg VMM Hob ...

Consume

Grub2

Produce

Consume

Associate
Dump CC Event Log

---- TDX Event Log Entry - 71 [0x1C331F50] ----

RTMR   : 2
Type   : 0xD (EV_IPL)
Length : 161
 Algorithms ID : 12 (TPM_ALG_SHA384)
Digest[0] :
00000000 E8 09 21 B2 EE 7B D3 C9 24 2D 7D 2B 60 CA D2 8A ...
0000010 7F E6 BE 4C BE A3 5A AE F3 E6 21 81 3B 60 E8 FF ...
0000020 BE BE 2A AF ED 50 03 23 BE D6 4E 99 B9 71 6A 70 ...
 RAW DATA: ---------------------------------
1C331F50 03 00 00 00 0D 00 00 00 01 00 00 0C 00 E8 09 ............
1C331F60 21 B2 EE 7B D3 C9 24 2D 7D 2B 60 CA D2 8A 7F E5 ...
1C331F70 8E 4C BE A3 5A AE F3 E6 21 81 3B 60 E8 FF BE ...
1C331F80 2A AF ED 50 03 23 BE D6 4E 99 B9 71 6A 70 5F 00 ...
1C331F90 00 00 67 72 75 62 5F 63 6D 64 20 69 6E 69 74 72 ...
. 1C331FA0 d (hd0,msdos3)/b
1C331FB0 06 6F 74 2F 69 6E 69 74 72 61 6D 73 2D 35 2E ...
1C331FC0 31 35 2E 30 30 53 50 52 2E 4D 56 50 5E 43 2E ...
1C331FD0 76 31 30 3E 34 2E 6D 76 78 34 30 2E 65 6C 38 2E ...
1C331FE0 78 38 36 5F 36 34 32 28 67 75 73 74 2E 69 6D 67 ...
1C331FF0 00

 RAW DATA: ---------------------------------------------


- Event log example for Direct Boot
- Event log example for Grub2 Boot
Measurement in Td-Shim

- Td-Shim: a lightweight TDX shim firmware
  - Support confidential container or service TD
  - Support kernel direct boot
Agenda

• Measurement and Trust Chain
• Attestation and Disk Decryption
Attestation for Confidential Computing

Remote Key Management Server
- Key for runtime usage
- Key for launch-time Usage

**OS Runtime**
- Decryption Agent (AI Model)
- Attestation Agent

**Launch-Time**
- Decryption Agent (VM Image)
- Attestation Agent

**Host**
- Encrypted VM disk Image

- **Launch Time** (Pre-boot or Early-OS boot): Get a key to decrypt the VM image via FDE (Full Disk Encryption) tool in launch time
- **OS Runtime**: Get a key to decrypt AI model (as example) via a runtime attestation agent
Considerations for Disk Decryption in Launch Time

Remote Key Management Server
  - Key Management Service
  - Remote Attestation Service
  - Key Broker Service

Attestation for Disk Decryption

- GetQuote()
- GetKey()
- FDE

TLS (Transport Layer Security)
TCP/IP
vNIC/NIC

Quote Generation Service (on Host)

Pre-boot vs Early-boot
Host or Guest?
Pre-Boot Disk Decryption

Attestation Agent in pre-boot OVMF for FDE

1. TDG_VP_VMCALL_GET_QUOTE
2. KVM_SIGNAL_MSI
3. Restful API
   - HTTPS
   - TLS
4. VMCALL/vSock
5. TCP/IP

ACPI Table: Storage Volume Key

Decryption Agent

Initrd

Decrypt the Disk

Pros
- Simplify Tenant effort
- Flexible to support decryption in different stages like decryption agent in OVMF, grub or initrd

Cons
- Modifications involving multiple components
- Attack surface is bigger in OVMF

Pre-boot

Early-boot

Refer: Storage-Volume-Key is defined in GHCI specification chapter 4.4 or ACPI 6.5
**Early-Boot Disk Decryption**

**Pros**
- The attestation process of disk decryption is running in user space like a normal runtime-attestation
- Allow different type vBIOS/bootloader like OVMF, simplified td-shim, etc.

**Cons**
- Need modify customer’s VM image if put initrd in /boot partition instead of “-initrd” via launch command
Linux TDX MVP Stack

- TDX MVP Stack: github.com/intel/tdx-tools

- VM Orchestrator:
  - Launch TD VM via qemu & libvirt
  - Direct boot & Grub boot
  - Secure boot & measured boot
  - OS runtime attestation
  - Launch time attestation (WIP)

- Kubernetes Orchestrator (WIP):
  - Confidential Container (CNCF):
    - Launch/Manage confidential container in TDVM transparently
  - Kubevirt: Launch/Manage the TDVM explicitly