Remote attestation is necessary for CVM

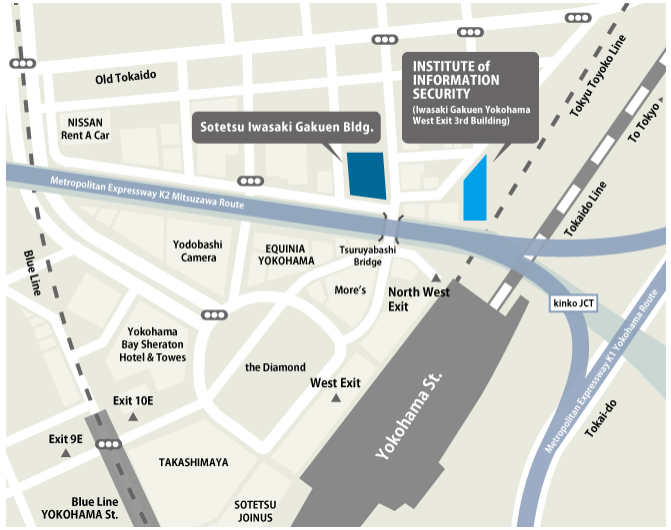
IIJ Seminar 2025/05/19 (Mon)

Institute of Information Security (情報セキュリティ大学院大学)
Kuniyasu Suzaki (須崎 有康)

Who am I ? (Kuniyasu Suzaki)

INSTITUTE of INFORMATION SECURITY

- Professor, IISEC: Institute of Information Security from 2022/9/1
  - 情報セキュリティ大学院大学 Graduate School @ Yokohama
    - ◆https://www.iisec.ac.jp/
  - Former : AIST (National Institute of Advanced Industrial Science and Technology)
  - TGC (Trusted Computing Group) Invited Expert 2019 -
  - Privacy-Tech Association Advisor 2024 -
  - 1CD Linux KNOPPIX Japanese Edition (2003-2013)



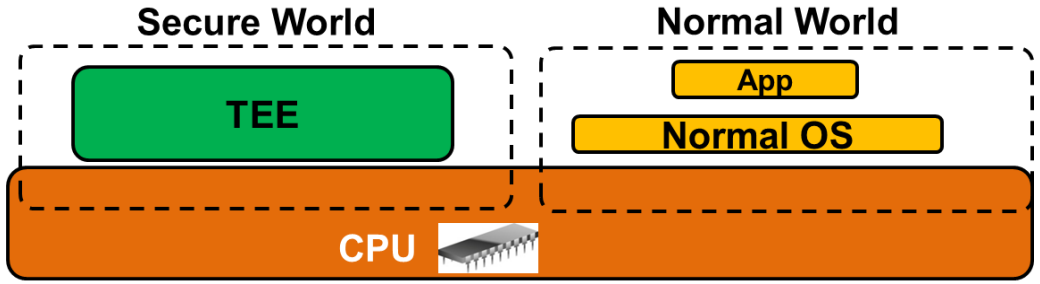
Contents

What is Confidential VM?

- Confidential VM is a special VM protected by TEE (Trusted Execution Environment).
  - Because we cannot trust cloud vendors (administrators)!

https://www.cpomagazine.com/cyber-security/leaked-documents-indicate-google-fired-dozens-for-data-misuse-unauthorized-access-of-user-data-modification-deletion-of-employee-data-among-complaints/?utm_source=chatgpt.com

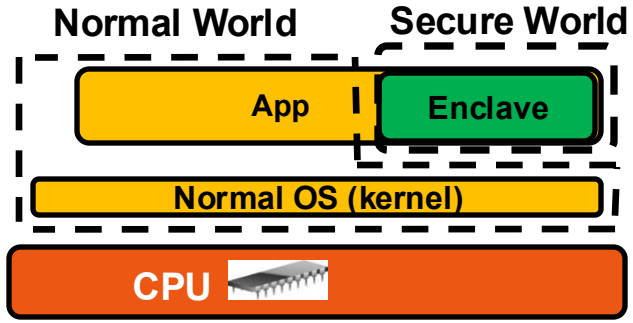
- TEE offers an isolated execution environment on the same CPU.
- We can run a confidential application in secure world.
- There are several types of TEE implementations.



Type of Confidential Computing

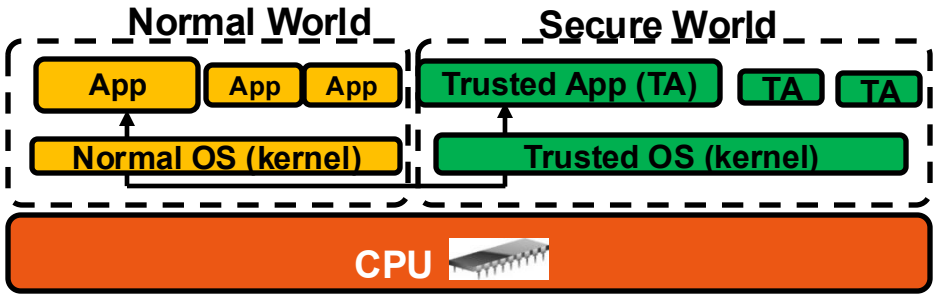
Library Type

- A part of process (library) is executed in TEE.
- CPU: Arm Cortex-M, Intel SGX



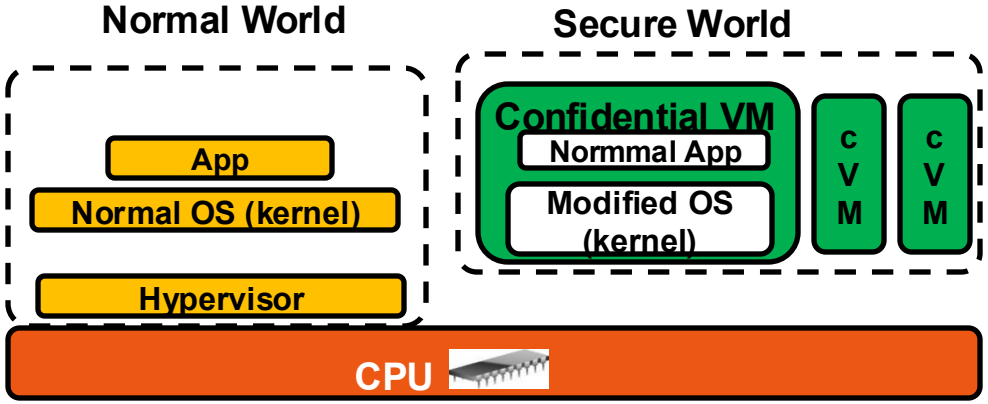
Process Type

- Secure World has an own OS and TA (Trusted Application) runs on it. Normal App calls TA.
- CPU: Arm Cortex-A, AMD PSP, Apple Secure Enclave



VM Type

- Secure World has VMs, namely confidential VM.
- The OS modified for secure world.
- CPU: Intel TDX, AMD SEV, Arm CCA



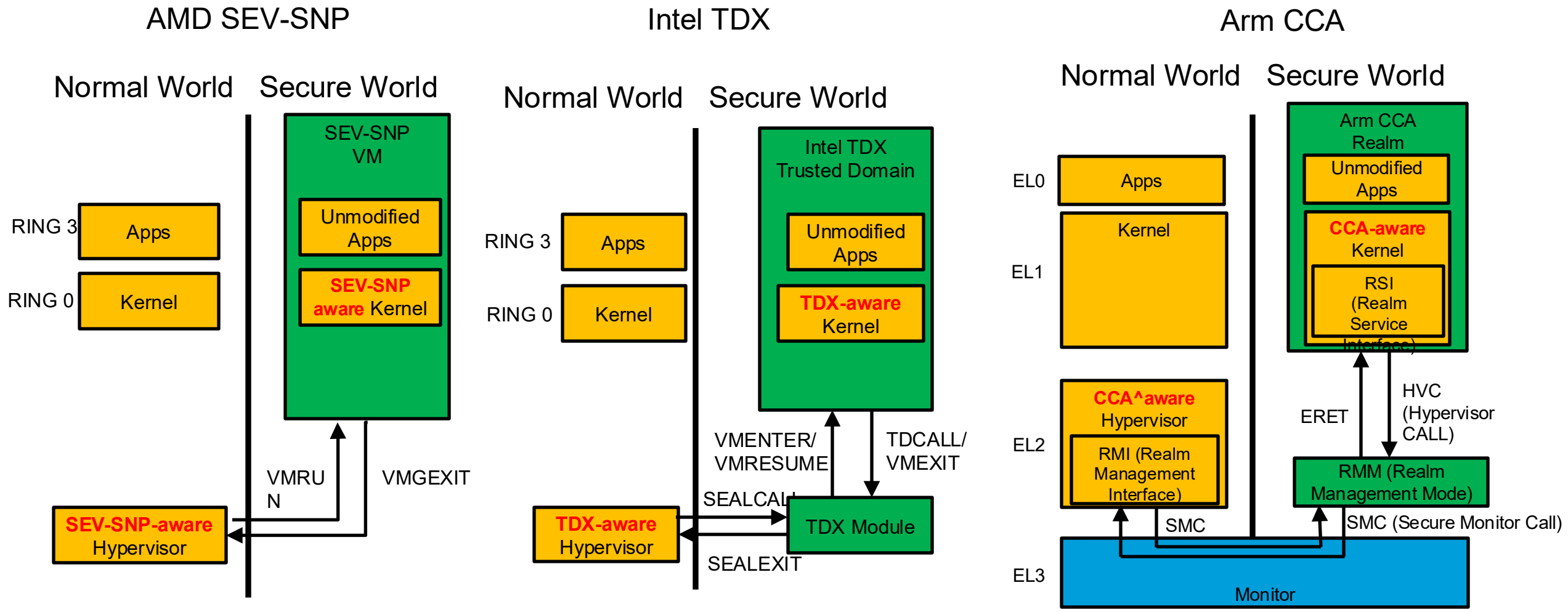
Current TEE-enabled CPUs and targets

INSTITUTE of INFORMATION SECURITY

	Embedded	Smartphone	Game	PC	Server/Cloud
Arm TrustZone (Cortex-M)	Raspberry Pi Poco				
Arm TrustZone (Cortex-A)	Raspberry Pi 3B+	Many	Nintendo Switch		
Arm CCA upcoming		?		?	?
Intel SGX (Core) deprecated				deprecated	
Intel SGX (Xeon Scalable)					Azure, GCP, etc
Intel TDX (Xeon)					Azure, GCP, etc
AMD PSP			Playstation5		
AMD SEV (EPYC)					Azure, GCP, etc
Apple Secure Enclave		iPhone		Mac	

Confidential VM

- Green parts run on encrypted memory, namely Secure World.



Who you are (authentication)? What is it (attestation)?

- **"On the Internet, nobody knows you're a dog"**
  - User authentication is important.

- Remote attestation is a mechanism to confirm ***intended hardware and software (device and software authentication)***
  - ***is not user authentication. Another technology.***

- Applied on
  - Smartphone
  - TPM (Trusted Platform Module) on PC
  - FIDO (Fast IDentity Online)
  - Smart home protocol "Matter"
  - TEE
    - ◆Because TEE is isolated execution environment and hides the behavior.

Drawn by Peter Steiner, published in the July 5, 1993 issue of the American magazine The New Yorker.

Remote Attestation

INSTITUTE of INFORMATION SECURITY

■ IETF RFC 9334 RATS(Remote Attestation ProcedureS)

RATS Logo

- **Attester**

  wants to get data or service form Relying Party. The device offers the evidence which shows the soundness of devices, systems, applications, configurations, etc.

- **Relying Party**

  wants to confirm the Attester's soundness to provide data or service.

- **Verifier**

  judges the Attester's evidence based on registered endorsement (ex: attestation public key), reference values, and policies.

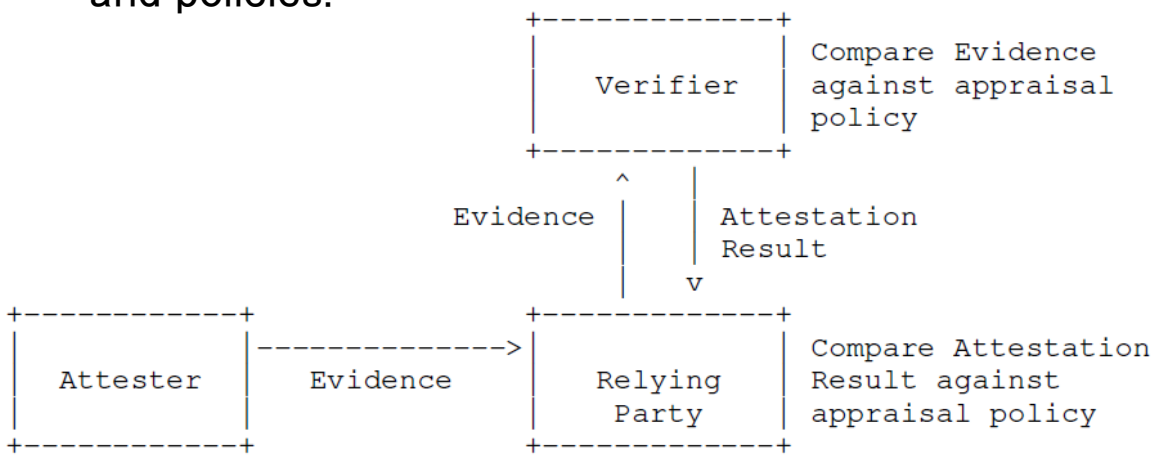


Figure 6: Background-Check Model

① Make "Attestation Evidence (Ex:hash values of applicatoins)" and sign it with Attestation Private Key.

③ Verifier has the certificate of Attestation Public Key and reference values (ex: hashes of applications).
Verifier judges the Evidence with them and send the result.

Evidence ⇑ ⇓ Result

② Relying Parity cannot verify and ask Verifier with the evidence.

Evidence ⇑

Remote Attestation Requirements

Requirement ① : Attestation Secret Key must be protected securely.

- Anti-pamper device (hardware Root of Trust) protects the key.
  - Some devices are gets the FIPS(Federal Information Processing Standards) 140-3 validation certificate.
  - https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search

Certificate Number	Vendor Name	Module Name	Module Type	Validation Date	Status
4749	Intel Corporation	Crypto Module for Intel® Alder Point PCH Converged Security and Manageability Engine (CSME)	Firmware-hybrid	08/02/2024	Active
4941	Advanced Micro Devices (AMD)	AMD ASP Cryptographic CoProcessor ("Genoa")	Firmware-hybrid	01/15/2025	Active
4915	Advanced Micro Devices (AMD)	AMD ASP Cryptographic CoProcessor ("Raphael")	Firmware-hybrid	12/12/2024	Active
4914	Advanced Micro Devices (AMD)	AMD ASP Cryptographic CoProcessor ("Storm Peak")	Firmware-hybrid	12/12/2024	Active

Requirement ② : Only trusted software uses the keys and measures hash values, etc.

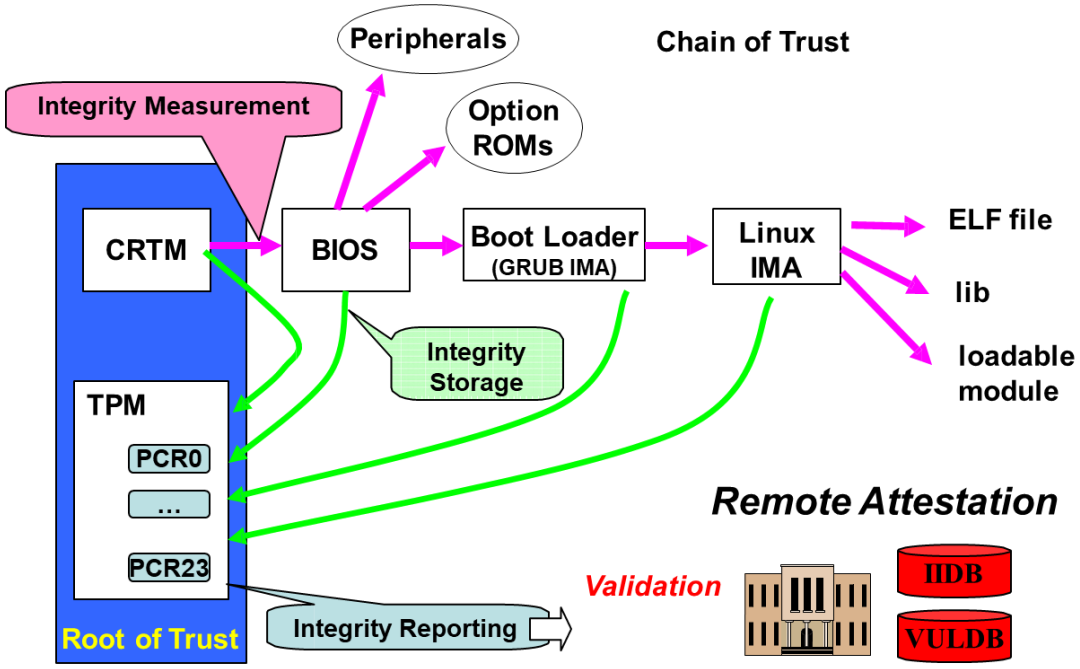
Remote Attestation on TPM (measured boot)

INSTITUTE of INFORMATION SECURITY

- TPM (Trusted Platform Module) is anti-tamper device.
  - TPM is a passive device and does not offer active security. (*** TPM does not secure boot.)
  - TPM has PCR (Platform Configuration Register) and trusted software records a measured hash value.
  - Chain of Trust starts from CRTM: Chain of Root of Trust Management.
  - TPM has AK: Attestation Key sec-key and signs the PCR values with it.

Remote Attestation

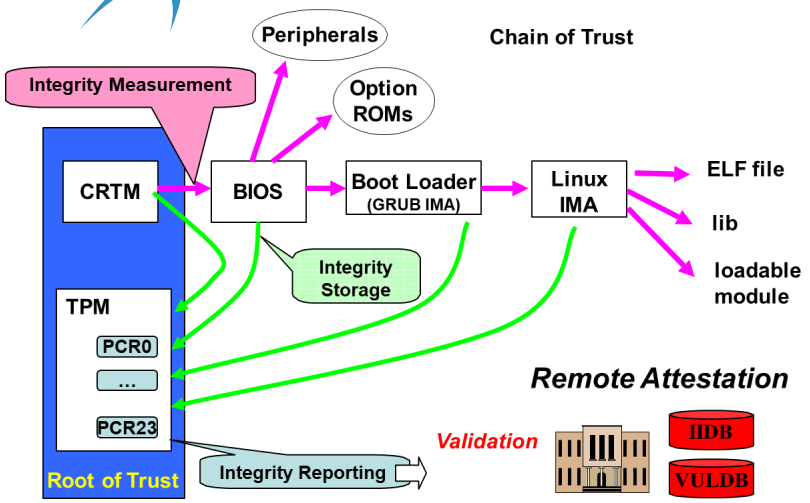
- Attester sends evidence
  - ① Signs the PCR values with AK sec-key
  - ② List of measurements
- Verifier has
  - AK pub-key (or certificate)
    - PCR values are guaranteed by AK.
    - The hashes of measurements are recalculated and verified with the PCR value.
  - Validation is success or not.



TPM Remote Attestation

- Measured Hash values are recorded in TPM PCR with “Extend”.
  - **Extend**
    - **PCR(i) = SHA1(PCR(i) +Digest)**

The method is standardized by TCG (Trusted Computing Group).



TPM 2.0

PCR Index	PCR Usage
0	SRTM, BIOS, Host Platform Extensions, Embedded Option ROMs and PI Drivers
1	Host Platform Configuration
2	UEFI driver and application Code
3	UEFI driver and application Configuration and Data
4	UEFI Boot Manager Code (usually the MBR) and Boot Attempts
5	Boot Manager Code Configuration and Data (for use by the Boot Manager Code) and GPT/Partition Table
6	Host Platform Manufacturer Specific
7	Secure Boot Policy
8-15	Defined for use by the Static OS
16	Debug
23	Application Support

– **/sys/kernel/security/tmp0/ascii_bios_mesurements**

PCR SHA1 Event

```
3 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
4 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
5 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
6 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
7 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
4 c1e25c3f6b0dc78d57296aa2870ca6f782ccf80f 05 [Calling INT 19h]
4 38f30a0a967fcf2bfee1e3b2971de540115048c8 05 [Returned INT 19h]
4 7ca42b22324927c400263bae94e1e7cc28655532 05 [Booting CD ROM]
4 5c3eb80066420002bc3dcc7ca4ab6efad7ed4ae5 01 [POST CODE]
4 1cdac212c5342627905cfcc4931972a8b4a09996 0d [IPL]/boot/grub/stage2_eltorito
4 2cedbf54913d69d027c5b97e02763f921b16e345 06 []
4 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 f1f74d078d57197ee9cd9205995a6ba5e6a68cbf0e [IPL Partition Data] /boot/grub/grub.conf
5 aed235d4ddb5fed00156f4991f2c1d1330c97694 1105 []
8 94c417906f8d383b811d918dce6bafdbc650ed42 1205 [] /boot/isolinux/linnux-ima
8 793eb4a591229afe35d60d5c2b66cee9dc33225c 1405 [] /boot/isolinux/minirt-ima.gz
5 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]
8 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]
8 fac33a1fc0ad42c07d00322d64c23f67567f334a 1005 []
```

Measured files

Remote Attestation on TEE

■ Type of Remote Attestation for TEE

① On VM Type TEE

◆Remote attestation is used to know the booting processes (BIOS, bootloader, kernel, and kernel arguments) for mounting a root FS.

- ➢ Inside TEE is open.

② On other TEEs (library type and process type)

◆Remote attestation is used to know TA

- ➢ Inside TEE is hidden.

Remote Attestation for cVM

INSTITUTE of INFORMATION SECURITY

- CPU rooted Attestation
  - CPU Vendor offers
    - ① Signing Secret Key is embedded in CPU securely.
      - The certificate information is also offered.
        - » Intel TDX https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_TDX_DCAP_Quoting_Library_API.pdf
        - » AMD SEV https://www.amd.com/ja/developer/sev.html
    - ② Mechanism to measure the initial VM memory only (BIOS, kernel, etc).
      - CAUTION: Disk image is not measured.
      - After booting, there is no mechanism to measure the applications.

To solve this problem

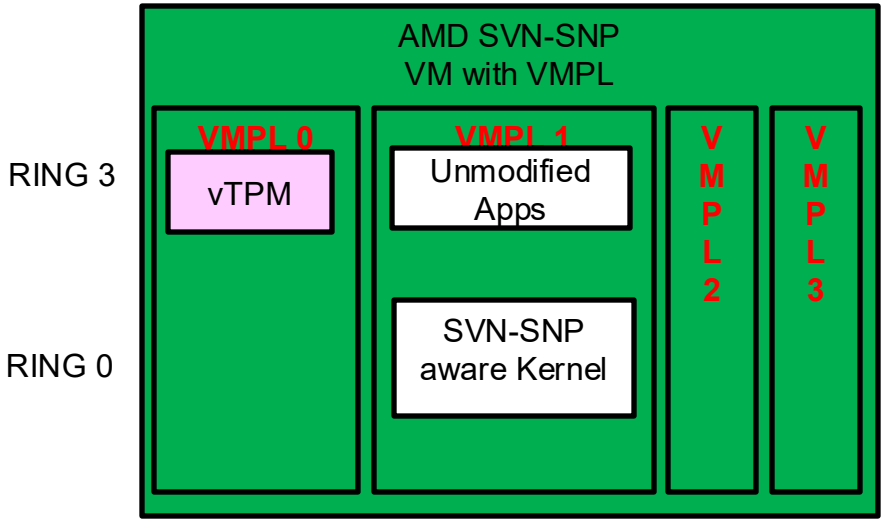
TPM's remote attestation is used.

- CPU Vendor offers
  - The mechanism to implement virtual TPM for cVM.

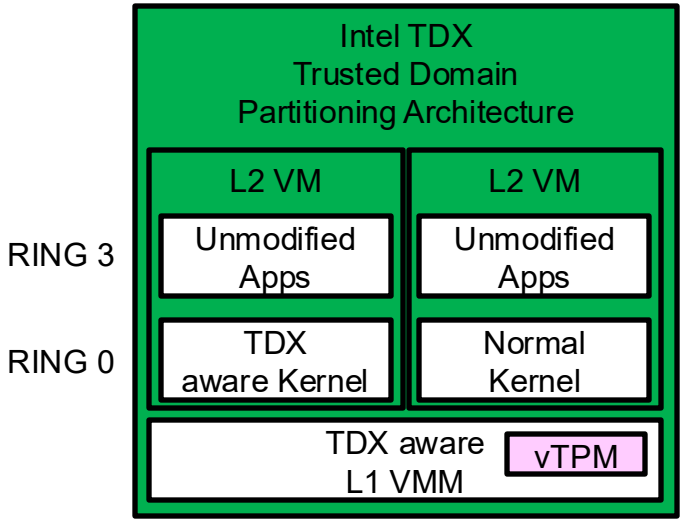
vTPM on cVM

- Privilege mode in VM
  - Used to implement virtual TPM

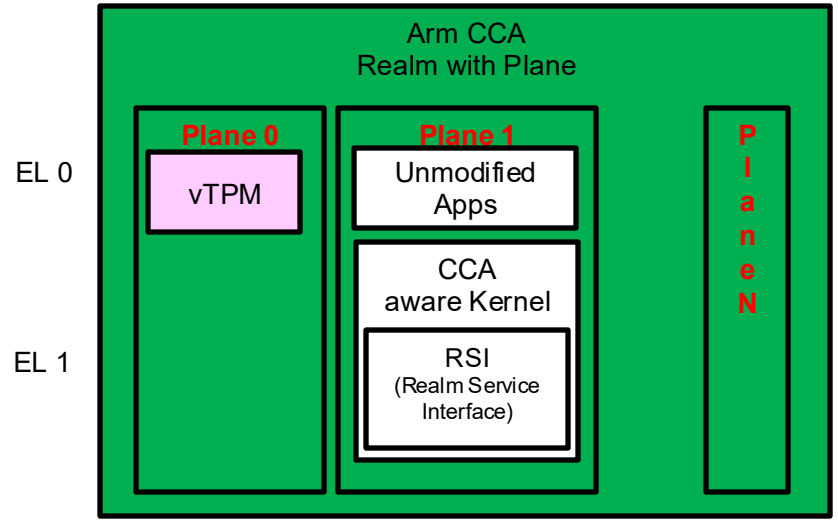
AMD SEV-SNP
VMPL (VM Privilege Level)



Intel TDX
TD Partitioning Architecture



Arm CCA
Plane



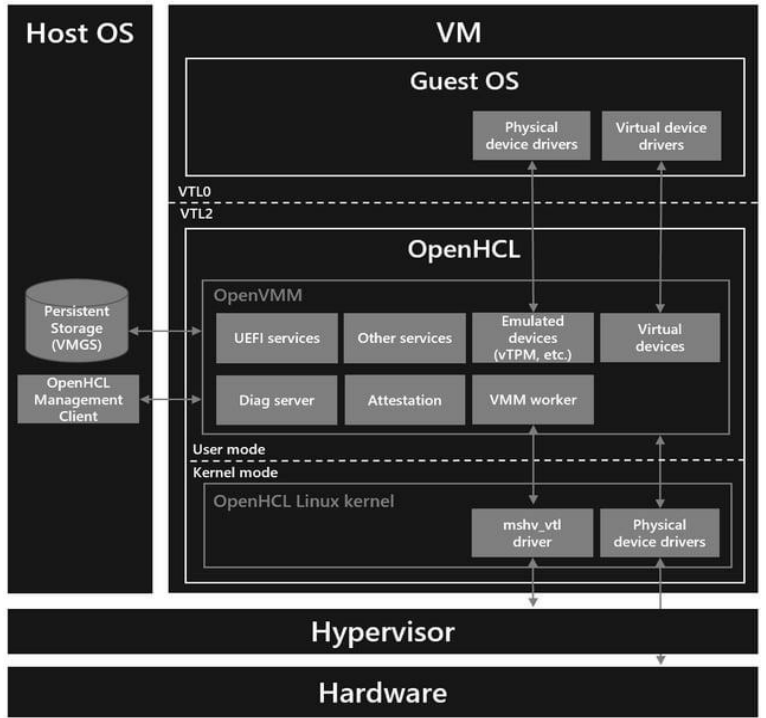
Intel TDX Partitioning Architecture Linux Plumber Conf 24
https://lpc.events/event/18/contributions/1918/attachments/1632/3406/02-lpc2024_mc_tdp_vtpm.pdf

Arm CCA Plane OC3 2024
https://assets-global.website-files.com/63c54a346e01f30e726f97cf/660e6e6124fce8fe497b508d_Arm_CCA%20Evolution%20And%20Ecosystem%20Support%20-%20Gareth%20Stickwell%20Nick%20Sample%20Paul%20Howard.pdf#page=20.00

vTPM implementation

- COCONUT Secure VM Service Module (SVSM)
  - https://github.com/coconut-svsm/svsm
  - https://coconut-svsm.github.io/svsm/

- Microsoft OpenHCL
  - https://techcommunity.microsoft.com/blog/windowsosplatform/openhcl-the-new-open-source-paravisor/4273172
  - Unify the CPU differences.



Remote Attestation for cVM

■ 2 step attestation

① CPU rooted Attestation

- ◆ Attest the initial memory image on cVM

Requirement ① The key is offered by CPU vendors and protected by hardware Root of Trust.

- ◆ Intel TDX: uses SGX remote attestation based on CSME (Converged Security and Manageability Engine, 32 bit Intel x86 CPU) .
- ◆ AMD SEV: ASP: AMD Secure Processor (Arm Cortex-A Architecture CPU)

Requirement ② The measurement is guaranteed by CPU instructions. The signing is also guaranteed by CPU.

② Virtual TPM Attestation

- ◆ Attest after booting

Requirement ① ???

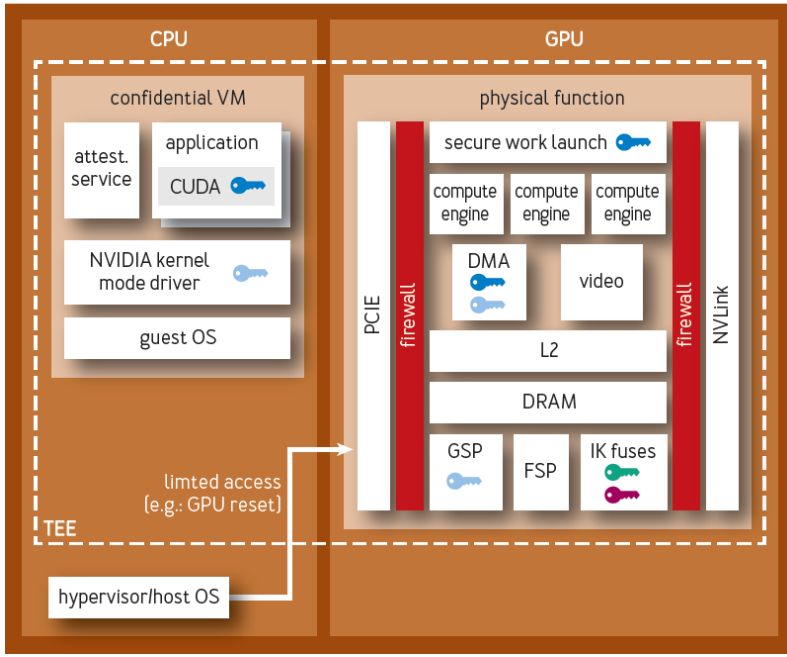
Requirement ② ???

■ Remaining Issue: Migration

cVM with GPU and other

- Current cloud VM offers GPU services.
- cVM also wants to use GPU. Does the GPU turst?
- nVIDIA H100 (or later) offers remote attestation mechanism from AMD SEV and Intel TDX.
  - ACM Qeue “Creating the First Confidential GPUs”, 2023/Sep
    - https://queue.acm.org/detail.cfm?id=3623391

FIGURE 1: A TRUSTED EXECUTION ENVIRONMENT



- PCI-Sig Proposes TEE Device Interface Security Protocol (TDISP)
  - https://pcisig.com/tee-device-interface-security-protocol-tdisp

Conclusions

- Remote attestation is a mechanism to confirm intended hardware and software (device and software authentication)

  Requirement ① : Attestation Secret Key must be protected securely.

  Requirement ② : Only trusted software uses the keys and measures hash values, etc

- Current CVM Remote Attestation
  - ① CPU rooted Attestation
  - ② Virtual TPM Attestation
- Next IPSJ (Information Processing Society of Japan) Magazine 2025/07 has article “Technical new points on Confidential Computing （機密コンピューティングの技術的特徴)”
- OpenSSF Community Day Japan 2025, June/18 @Odaiba Hilton
  - https://openssf.org/event/openssf-community-day-japan/
  - Current Remote Attestation on IoT --- Arm TrustZone OP-TEE with VERAISON Verifier –

Contents

- Background
  - What is cVM? What is TEE？
  - What is Remote Attestation？
- Remote Attestation for cVM
  - CPU rooted Attestation
  - Virtual TPM Attestation
- Remote Attestation Extension
  - GPU on cVM (nVidia H100)
  - Serverless Computing
- Current Status
  - Microsoft Azure Attestation
  - Intel Trust Authority

TPMの鍵管理（Provisioningが重要）

- Remote Attestationで使う署名鍵AK(Attestation Key)は事前に作る必要がある。
  - AKはTPMベンダーが設定するものではない。TPMベンダーが設定するのはEK (Endorsement Key)のみ。
  - AKはEKから鍵導出関数 KDF (Key Derivation Function) で作成され、その際に作成されるnameと合わせて、TPM由来であることが検証できる。
  - AKもEKの秘密鍵はTPMが出ないで安全
- 作成したAKはVerifierに事前登録する。