INSTITUTE of INFORMATION SECURITY

Lesson from Cloud Confidential Computing Remote Attestation Sample

FOSDEM 2026 Confidential Computing Devroom
Feb/1/2026 @Burussels
https://github.com/iisec-suzaki/cloud-ra-sample

Kuniyasu Suzaki
suzaki@iisec.ac.jp
IISEC: Institute of Information Security, Graduate School

This work is collaborated with Takuma Imamura @Acompany

Learned Lessons *at this moment*

INSTITUTE of INFORMATION SECURITY

- Each cloud has ***own security policy*** and ***affects its remote attestation***.
  - All attestation shows it runs on Confidential Computing Architecture (i.e., CC-CPU).
    - However,
      - vTPM is covered or not.
      - Secure boot is unknown.
      - The security of storage (i.e., encrypted or not) is unknown.
  - vTPM setting depends on Cloud
    - Some vTPM can keep Endorsement Key & Attestation Key, but we don't know their confidentiality on cloud.
  - Secure boot setting depends on Cloud
    - Some clouds are available, but others are not. Immutable or mutable.

Reference

- Mengyuan Li, et.al, SoK: Understanding Designs Choices and Pitfalls of Trusted Execution Environments [AsiaCCS 24]
- Gianluca Scopelliti et.al., Understanding Trust Relationships in Cloud-Based Confidential Computing [SysTex 24]
- Jana Eisoldt et.al., A cloudy view on trust relationships of CVMs: How Confidential Virtual Machines are falling short in Public Cloud [ACSAC 25]

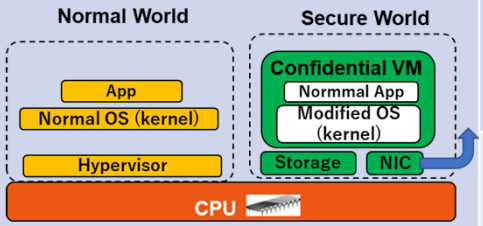
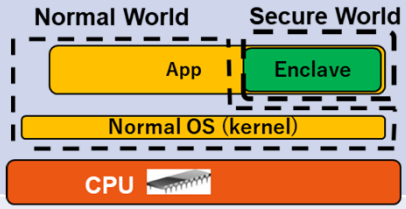
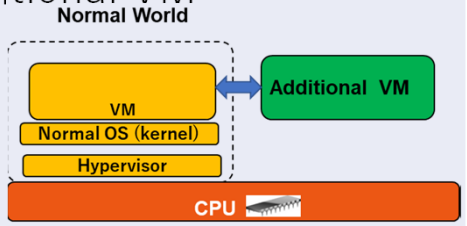
Contents

INSTITUTE of INFORMATION SECURITY

- Background of target Confidential Computing
  - AMD SEV-SNP, Intel TDX, Intel SGX, and AWS Nitro
- Implementation of the remote attestation sample on clouds
  - Confidential computing architecture and its attestation on Clouds
- Discussion and Conclusion

Target Confidential Computing

INSTITUTE of INFORMATION SECURITY

	CC Type	Target	Attestation Key Endorser	Measurement Target of Attestation	After VM Power-On
CPU	VM 	**SEV-SNP**	• AMD (VCEK) • AMD+Cloud Provider(VLEK)	UEFI + vTPM on VMPL	vTPM based attestation
		TDX	Intel	• UEFI (at TDMR) • shim,bootloader, kernel at (RTMR[0-3])	vTPM based attestation
	Lib 	**SGX**	Intel	• Lib image (at MRENCLAVE) • Binary signer (at MRSIGNER)	---
Hyp	Additional VM 	**Nitro**	AWS	Initial Docker image, kernel, apps (at PCR[0-3])	---

- **Generally, attestation evidence is based on the initial state of Confidential Computing.**
- VM type assumes 2-step attestations.
  - CPU based: Initial state of VM (UEFI, vTPM, etc) [Exception] TDX offers the runtime measurement.
  - vTPM based: After VM Power On. (Out of scope from current samples)

Target Clouds and used tools

INSTITUTE of INFORMATION SECURITY

	AWS	Azure	GCP	Sakura
SEV-SNP	☑	☑	☑	☑
TDX		☑	☑	
SGX		☑		
Nitro	☑			

- Tools used at Attester and Verifier

	Attestation Report tool	Verifier tool (service)
SEV-SNP	snpgust, go-snp-gust	snpgust, go-snp-gust, Microsoft Attestation Service (MAA)
TDX	go-tdx-guest	go-tdx-guest,tdx-quote-parser, Intel DCAP QVL, Microsoft Attestation Service (MAA)
SGX	DCAP Quote Generation Lib	DCAP QVL, Humane
Nitro	nitro-cli, Nitro Secure Module	Original

INSTITUTE of INFORMATION SECURITY

Implementation of remote attestation sample

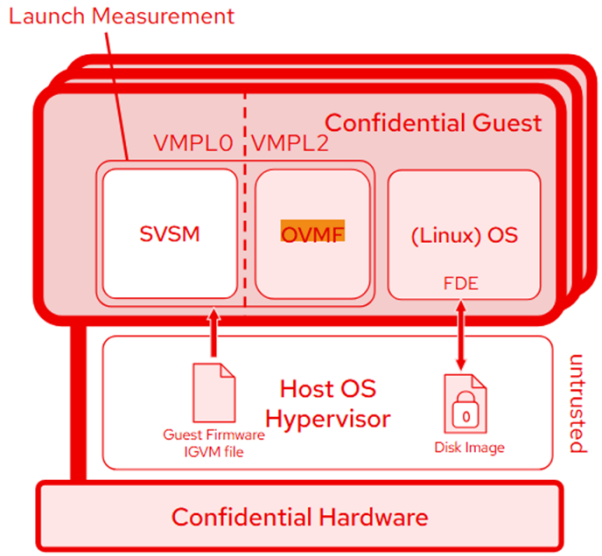
- AMD SEV-SNP
- Intel TDX
- Intel SGX
- AWS Nitro

Main target at this talk

AMD SEV-SNP features

INSTITUTE of INFORMATION SECURITY

1. Two types of Attestation Key
   - VCEK: Versioned Chip Endorsement Key
     - Based on Chip ID
   - VLEK: Versioned Loaded Endorsement Key
     - Based on Chip ID and CSP's seed.
2. Two types of Attestation method
   - Standard (Regular) Attestation
     - Without PKI certificate
   - Extended Attestation
     - With PKI certificate
3. VMPL (Virtual Machine Privilege Level) 0-3
   - Used by vTPM (Example: Coconuts SVSM)
   - VMPL is target of remote attestation and verified.



Updates on Coconut SVSM Secure Services and Stateful Devices for Confidential Virtual Machines [FOSDEM 25]
https://archive.fosdem.org/2025/events/attachments/fosdem-2025-5412-updates-on-coconut-svsm-secure-services-and-stateful-devices-for-confidential-virtual-machines/slides/237927/FOSDEM_20_X5nuOWj.pdf

Attestation tools for AMD SEV-SNP

INSTITUTE of INFORMATION SECURITY

- Combination of Attestation Keys, methods, and tools

CSP	Attestation Key	Method	Report Generation	Verification	Script
AWS	VLEK	Extended	snpguest	snpguest	AWS/aws-snp-xra-by-snpguest.sh
Azue	VCEK	Extended	tpm2-tools	MAA	Azure/azure-snp-ra-by-maa.sh
		Standard	snpguest	snpguest	Azure/azure-snp-sra-by-snpguest.sh
			tpm2-tools	snpguest	Azure/azure-snp-sra-by-tpm2-tools.sh
GCP	VCEK	Extended	snpguest	snpguest	GCP/gcp-snp-xra-by-snpguest.sh
		Standard	snpguest	snpguest	GCP/gcp-snp-sra-by-snpguest.sh
			go-sev-guest	go-sev-guest	GCP/gcp-snp-sra-by-go-sev-guest.sh
Sakura	VCEK	Standard	snpguest	snpguest	Sakura/sakura-snp-sra-by-snpguest.sh
			go-sev-guest	go-sev-guest	Sakura/sakura-snp-sra-by-go-sev-guest.sh

VLEK: committed by a cloud vendor

Extended: with PKI certificate

MAA: Microsoft Azure Attestation service

AMD SEV-SNP on Clouds

INSTITUTE of INFORMATION SECURITY

	AWS	Azure	GCP	Sakura
Attestation Interface	/dev/sevguest	**/dev/tpm0**	/sev/sevguest	/sev/sevguest
VMPL level for OS	0	0 **(True result 2?)**	0	**2**
vTPM	☑ **Immutable after VM creation**	☑**Immutable**	☑ **Immutable after VM creation**	☑ **Immutable** Ephemeral TPM
Secure Boot	Setting is difficult (require Key setting)	☑**Mutable**	☑ **Immutable after VM creation**	Cannot set on CVM

- Azure offers attestation evidence from vTPM. If the vTPM is limited by access (ex. property ***ownerAuthSet***), the attestation tools cannot get the evidence.
- vTPM, offered by VMPL, is a target of remote attestation. However, AWS, ~~**Azure**~~, and CGP offer other methods. They may be out of the scope of remote attestation.
- What is VMPL on Azure?

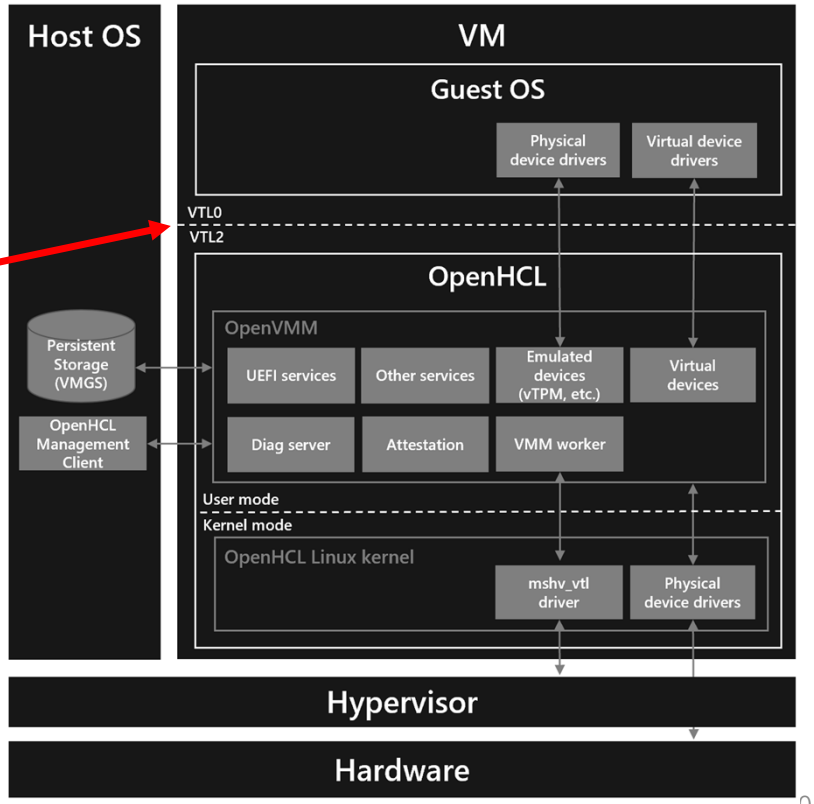
AMD SEV-SNP on Azure

INSTITUTE of INFORMATION SECURITY

- OpenHCL: the new, open source paravisor
  https://techcommunity.microsoft.com/blog/windowsosplatform/openhcl-the-new-open-source-paravisor/4273172

- This article says GuestOS runs on VMPL2 and vTPM runs on VMPL0.

The figure is wrong.



AMD SEV-SNP TPM Persistent Keys

INSTITUTE of INFORMATION SECURITY

(1) $ sudo tpm2_getcap handles-persistent

(2) $ sudo tpm2_createek -G rsa -u ek.pub -c ek.ctx

$ sudo tpm2_evictcontrol -C o -c ek.ctx 0x81010001

$ sudo tpm2_createak -C 0x81010001 -c ak.ctx -G rsa -g sha256 -s rsassa -u ak.pub -n ak.name

$ sudo tpm2_evictcontrol -C o -c ak.ctx 0x81000002

(3) $ sudo tpm2_getcap handles-persistent

(4) $ reboot

(5) $ sudo tpm2_getcap handles-persistent

EK and AK are stored in NV of TPM.
Are they saved safely after power-off?

	AWS	Azure	GCP	Sakura
(1) Initial State	- 0x81010001 (EK-RSA) - 0x81010016 (EK-ECC)	- 0x81000001 (EK-RSA) - 0x81000003 (??-RSA)	None	None
(2) Setup EK and AK	EK exists and is used. Create & register AK	EK exists but cannot be used. Create EK & AK Can register	Create EK & AK Can register	Create EK & AK Can register
(3) After register	- 0x81000002 (AK-RSA) - 0x81010001 (EK-RSA) - 0x81010016 (EK-ECC)	- 0x81000001 (EK-RSA) - 0x81000002 (AK-RSA) - 0x81000003 (??-RSA) - 0x81010001 (EK-RSA)	- 0x81000002(AK-RSA) - 0x81010001(EK-RSA)	- 0x81000002(AK-RSA) - 0x81010001(EK-RSA)
(4) Reboot	Can	Can	Can	Can not (Reset form Dashboard)
(5) After Reboot	- 0x81000002(AK-RSA) - 0x81010001(EK-RSA) - 0x81010016(EK-ECC)	- 0x81000001 (EK-RSA) - 0x81000002 (AK-RSA) - 0x81000003 (??-RSA) - 0x81010001 (EK-RSA)	- 0x81000002(AK-RSA) - 0x81010001(EK-RSA)	**None**

Intel TDX features

INSTITUTE of INFORMATION SECURITY

- TDX offers two types of measurement.
  - MRTD (Measurement of Trust Domain Register)
    - TheTDVF(Trust Domain Virtual Firmware) is measured.
  - RTMR[0-3] (Runtime Measurement Registers)
    - Some components are measured after VM power-on. (works as TPM).
    - RTMR[i] = SHA384(RTMR[i] || x);

Sample of Measurements and Measurer software

	Measurements	Measurer software
RTMT[0]	TDX configuration, ACPI tables	TDMF
RTMT[1]	OS kernel, boot parameters	shim,grub
RTMT[2]	cmdline, initrd	Linux
RTMT[3]	reserved	

Attestation tools for Intel TDX

INSTITUTE of INFORMATION SECURITY

CSP	Report Generation	Verification	Script
Azure	● trustauthority-cli ● (tpm2_tools “for MAA”)	MAA	azure/azure-tdx-ra-by-maa.sh
		• go-tdx-guest • tdx-quote-parser	azure/azure-tdx-ra-by-go-tdx-guest.sh
		• DCAP-QVL • tdx-quote-parser	azure/azure-tdx-ra-by-dcap-qvl.sh
GCP	go-tdx-guest	• go-tdx-guest • tdx-quote-parser	gcp/gcp-tdx-ra-by-go-tdx-guest.sh
		• DCAP-QVL • tdx-quote-parser	gcp/gcp-tdx-ra-by-sgx-dcap-qvl.sh

MAA: Microsoft Azure Attestation service

Intel TDX Attestation Results

INSTITUTE of INFORMATION SECURITY

Cloud	Verifier	Results
Azure	MAA	"tdx_mrtd": "**fe27b2aa3a05ec56864c308aff03dd13c189a6112d21e417ec1afe626a8cb9d91482d1379ec02fe6308972950a930d0a**",
		"tdx_rtmr0":"000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000“ "tdx_rtmr1": "000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000“ "tdx_rtmr2": "000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000“ "tdx_rtmr3": "000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000“
	tdx-quote-parser	MRTD: **0a0d930a95728930e62fc09e37d18214d9b98c6a62fe1aec17e4212d11a689c113dd03ff8a304c8656ec053aaab227fe**
		RTMR0: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 RTMR1: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 RTMR2: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 RTMR3: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
GCP	tdx-quote-parser	MRTD: 94862837c0319a50122ae40e1170ab5bebf3ecccfdf03291f3c3c94b2cc504736cfd4def29f9be18c3707b89884e84a5
		RTMR0: 100b5f09997bbdad1c96605d7abe9473e3b57ccaf4e04a75a34f8c08ae7ed7c26905460397cffa38e9a6981669899413 RTMR1: b3e784922890627f28ea4dc74a834f754e5337e632450a02ac3c490ffb19d318a705d3d4773443e14fc382e302e8b910 RTMR2: fd9c54915336f262e1aba0e0ecb40c39ba58de6df230e752058c222476cada58db0d3743e714190ac4a4184a6e5f6f96 RTMR3: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

- Red characters are in reverse order.
  - Caused by the version difference of TDX verification? TDX v4 or v5 quote?
- On Azure, RTMR [0-3] are all Zero.
- The RTMR's event logs can get by **"tdeventlog"** tool from /sys/firmware/acpi/tables/data/CCEL.
  - Unfortunately, Azure does not offer it.

Intel TDX on Clouds

INSTITUTE of INFORMATION SECURITY

	Azure	GCP
Attestation Interface	**/dev/tpm0**	/dev/tdx_guest
vTPM	☑ **Immutable**	☑ **Immutable after VM creation**
Secure Boot	☑ **Mutable**	☑ **Immutable after VM creation**

- Azure offers attestation evidence from vTPM. If the vTPM is limited by access (ex. property ***ownerAuthSet***), the attestation tools cannot get the evidence.

- The situation of vTPM and Secure boot are same as the SEV-SNP.
- We guess it is caused by the Cloud security policy.

Intel TDX TPM Persistent Keys

INSTITUTE of INFORMATION SECURITY

EK and AK are stored in NV of TPM.
Are they saved safely after power-off?

(1) $ sudo tpm2_getcap handles-persistent

(2) $ sudo tpm2_createek -G rsa -u ek.pub -c ek.ctx

$ sudo tpm2_evictcontrol -C o -c ek.ctx 0x81010001

$ sudo tpm2_createak -C 0x81010001 -c ak.ctx -G rsa -g sha256 -s rsassa -u ak.pub -n ak.name

$ sudo tpm2_evictcontrol -C o -c ak.ctx 0x81000002

(3) $ sudo tpm2_getcap handles-persistent

(4) $ reboot

(5) $ sudo tpm2_getcap handles-persistent

	Azure	GCP
(1) Initial State	- 0x81000001 (EK-RSA) - 0x81000003 (??-RSA)	None
(2) Setup EK and AK	EK exists but cannot be used. Create EK & AK Can register	Create EK & AK Can register
(3) After register	- 0x81000001 (EK-RSA) - 0x81000002 (AK-RSA) - 0x81000003 (??-RSA) - 0x81010001 (EK-RSA)	- 0x81000002(AK-RSA) - 0x81010001(EK-RSA)
(4) Reboot	Can	Can
(5) After Reboot	- 0x81000001 (EK-RSA) - 0x81000002 (AK-RSA) - 0x81000003 (??-RSA) - 0x81010001 (EK-RSA)	- 0x81000002(AK-RSA) - 0x81010001(EK-RSA)

Intel SGX features

INSTITUTE of INFORMATION SECURITY

- The binary (signed shared library “***signed.so”) for SGX has two types of hashes.
  - **MRENCLAVE:** A cryptographic hash (measurement) of the enclave’s initial code and data.
  - **MRSIGNER:** A hash of the public key that signed the enclave (the signer’s identity).
- The remote attestation verifies the two hashes.

Attestation tools for Intel SGX

INSTITUTE of INFORMATION SECURITY

CSP	Report Generation	Verification	Script
Azure	• DCAP-Quote Generation Library (QGL) • Linux SGX SDK and Platform Software (PSW)	• DCAP QVL • Humane-RAFW-MAA (Humane Intel SGX Remote Attestation Framework for Microsoft Azure Attestation)	• update_keys.py • generate_settings.py

Attestation results on Intel SGX

INSTITUTE of INFORMATION SECURITY

DEBUG: Required MRENCLAVE ->

DEBUG: 06542c732b6fc5df0a9b065f60d494e426de57be9d9f5b95a3b730f8dda3bbc9

DEBUG: MRENCLAVE from Quote ->

DEBUG: 06542c732b6fc5df0a9b065f60d494e426de57be9d9f5b95a3b730f8dda3bbc9

DEBUG: MRENCLAVE from MAA RA report ->

DEBUG: 06542c732b6fc5df0a9b065f60d494e426de57be9d9f5b95a3b730f8dda3bbc9

INFO: MRENCLAVE matched.

DEBUG: Required MRSIGNER ->

DEBUG: 5ad6ce21e2a3b3855c69a956bf8d2f8e56ec33064e0f09007d78ed43a04627e8

DEBUG: MRSIGNER from Quote ->

DEBUG: 5ad6ce21e2a3b3855c69a956bf8d2f8e56ec33064e0f09007d78ed43a04627e8

DEBUG: MRSIGNER from MAA RA report ->

DEBUG: 5ad6ce21e2a3b3855c69a956bf8d2f8e56ec33064e0f09007d78ed43a04627e8

DEBUG:

INFO: MRSIGNER matched

AWS Nitro Enclave features

INSTITUTE of INFORMATION SECURITY

- Hypervisor-based CC
  - CPU independent and runs on X86_64 and Cortex-A architecture.
  - supported by security hardware “Nitro Security Chip”.
- Attestation
  - Measure the additional guest OS at boot time.

PCR	Hash of …	Description
PCR0	Enclave image file	A contiguous measure of the contents of the image file, without the section data.
PCR1	Linux kernel and bootstrap	A contiguous measurement of the kernel and boot ramfs data.
PCR2	Application	A contiguous, in-order measurement of the user applications, without the boot ramfs.
PCR3	IAM role assigned to the parent instance	A contiguous measurement of the IAM role assigned to the parent instance. Ensures that the attestation process succeeds only when the parent instance has the correct IAM role.
PCR4	Instance ID of the parent instance	A contiguous measurement of the ID of the parent instance. Ensures that the attestation process succeeds only when the parent instance has a specific instance ID.
PCR8	Enclave image file signing certificate	A measure of the signing certificate specified for the enclave image file. Ensures that the attestation process succeeds only when the enclave was booted from an enclave image file signed by a specific certificate.

- https://docs.aws.amazon.com/enclaves/latest/user/set-up-attestation.html

Attestation tools for AWS Nitro

INSTITUTE of INFORMATION SECURITY

CSP	Report Generation	Verification	Script
Azure	• nitro-cli • AWS Nitro Secure Module (NSM) library	original	• run.sh # Start the Nitro Enclave • get-ca.sh # Download AWS Nitro Enclaves root certificate • attest.sh # Execute attestation verification

Attestation Results on AWS Nitro

INSTITUTE of INFORMATION SECURITY

./build.sh

" "PCR0": "be444cb51e05ef175de00b19921ea2a2c13a8626700c18bd2998048206eeb69e476ce2a4a3ffe809dd3af6a3c6e0c6a9",

"PCR1": "0343b056cd8485ca7890ddd833476d78460aed2aa161548e4e26bedf321726696257d623e8805f3f605946b3d8b0c6aa",

"PCR2": "102befdefa035ae9b5cf89d17e916c8e06c1b1a7c9da33ea6419ae63d84d8411d7c72eff4b6176b4992d065ff55042c4"

./attest.sh

Step 4: Verifying PCR values, user data, and nonce...

Expected PCR values loaded from expected-measurements.json

☑ PCR0: MATCH

Expected: be444cb51e05ef175de00b19921ea2a2c13a8626700c18bd2998048206eeb69e476ce2a4a3ffe809dd3af6a3c6e0c6a9

Actual: be444cb51e05ef175de00b19921ea2a2c13a8626700c18bd2998048206eeb69e476ce2a4a3ffe809dd3af6a3c6e0c6a9

☑ PCR1: MATCH

Expected: 0343b056cd8485ca7890ddd833476d78460aed2aa161548e4e26bedf321726696257d623e8805f3f605946b3d8b0c6aa

Actual: 0343b056cd8485ca7890ddd833476d78460aed2aa161548e4e26bedf321726696257d623e8805f3f605946b3d8b0c6aa

☑ PCR2: MATCH

Expected: 102befdefa035ae9b5cf89d17e916c8e06c1b1a7c9da33ea6419ae63d84d8411d7c72eff4b6176b4992d065ff55042c4

Actual: 102befdefa035ae9b5cf89d17e916c8e06c1b1a7c9da33ea6419ae63d84d8411d7c72eff4b6176b4992d065ff55042c4

☑ User data: MATCH

Expected: b'hello'

Actual: b'hello'

☑ Nonce: MATCH

Expected: 8c9e628b9add4b92687f703d60c6181110be14ab1a500cb744171a4cf7eb1d751f0b150bbb9f149793a69dcbece2c96fe98a1c616eb2827dfd52122b2cf3744e

Actual: 8c9e628b9add4b92687f703d60c6181110be14ab1a500cb744171a4cf7eb1d751f0b150bbb9f149793a69dcbece2c96fe98a1c616eb2827dfd52122b2cf3744e

☑ Report contents are valid

Discussion

INSTITUTE of INFORMATION SECURITY

- vTPM and Secure Boot
  - Their implementations depend on cloud vendors based on their security policy.
  - vTPM is a target of remote attestation when it is implemented in VMPL of SEV-SNP. However, other implementations are not a target.
  - Secure Boot is not measured by CPU based remote attestation.
    - TPM can measure. However, vTPM on cVM is not trustful.

- Interoperability
  - Cloud vendors offer a modified attestation interface and results even if the CPUs are the same.
  - The difference may cause an interoperability problem (i.e., migration).

Conclusion

INSTITUTE of INFORMATION SECURITY

- Each cloud has ***own security policy*** and ***affects its remote attestation***.

- We need to understand the situation when we use confidential computing on clouds.
- Our remote attestation samples will help to understand.

https://github.com/iisec-suzaki/cloud-ra-sample

Contact: suzaki@iisec.ac.jp

Acknowledgment: This work was supported by JST K Program Grant Number JPMJKP24U4, Japan.

My guess

INSTITUTE of INFORMATION SECURITY

- Azure's Arm CCA (Cobalt 200) will offer attestation information from **"/dev/tpm0".**
  - Current Interface is "/sys/kernel/config/tsm/report/report0"