

# Attestation with SGX

SGX also provides the attestation service.

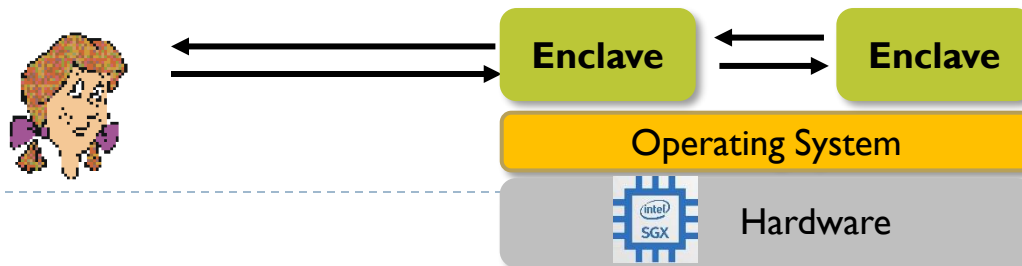
- ▶ Integrity measurement architecture: enclave measurement of the code, data, stack, heap, security flags, location of each page...
- ▶ Attestation protocol: attestation key and cryptographic protocol.

## Remote attestation

- ▶ A remote client attests the integrity of the code in the enclave.

## Local attestation

- ▶ In some scenarios, multiple enclaves collaborate on the same task, exchanging data at runtime.
- ▶ Collaborating enclaves have to prove to each other that they are trusted.



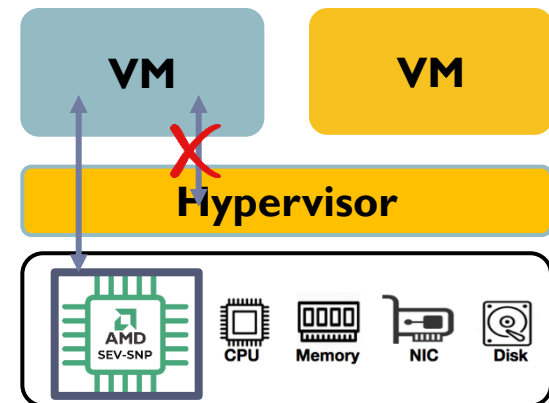
# AMD Secure Encrypted Virtualization (SEV)

## A hardware extension to protect VMs against untrusted hypervisor

- ▶ **SEV**: basic memory encryption for protecting VMs (release: 2016)
- ▶ **SEV-ES** (Encrypted State): encrypt CPU registers (release: 2018)
- ▶ **SEV-SNP** (Secure Nested Paging): adding integrity protection (release: 2020)

## Mechanism

- ▶ The processor encrypts the data (memory page, registers, configurations) of the guest VMs, so the hypervisor is not allowed to access the data.
- ▶ Uses an AMD Secure Processor to manage encryption keys.
- ▶ Transparent encryption with minimal modifications to the VM.



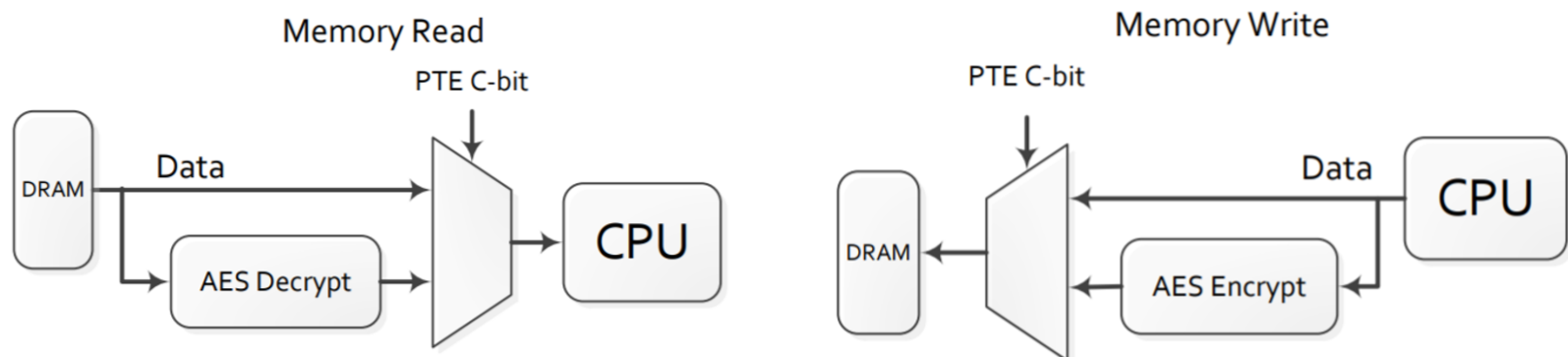
# AMD Secure Memory Encryption (SME)

## Virtual memory encryption is realized by SME

- ▶ An AMD architectural capability for main memory encryption
- ▶ Performed via dedicated hardware in the memory controllers
- ▶ Use AES engine to encrypt data and control with **C-bit** in Page Table Entry

## C-bit

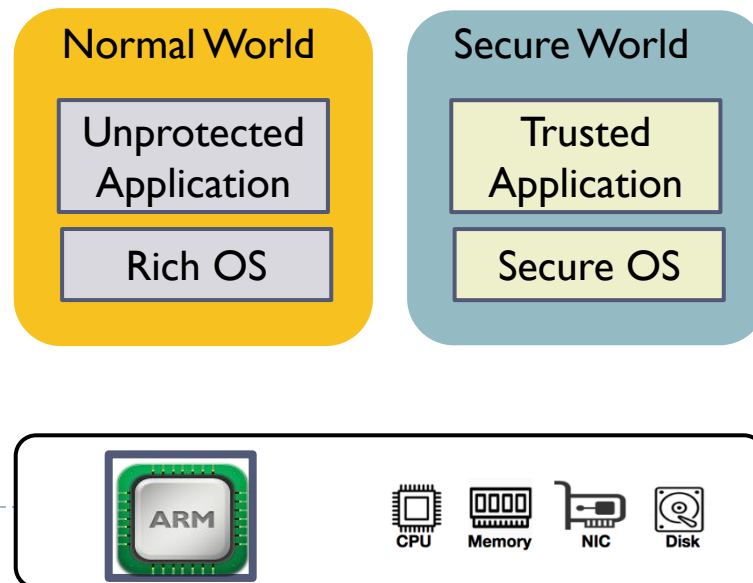
- ▶ Locate at physical address bit 47
- ▶ Set this bit to 1 to indicate this page is encrypted.
- ▶ Allow users to encrypt full memory of the VM, or selected memory pages



# ARM TrustZone

## The first commercial TEE processor (2003 in ARMv6 architecture)

- ▶ Create two environments that can run simultaneously on the same processor. Each world has an independent OS
- ▶ **Normal world:** runs the normal unprotected applications and a rich OS. They have restricted access to the hardware resources in the secure world
- ▶ **Secure world:** runs the sensitive protected applications and a smaller secure OS, isolating them from the untrusted world. They have full access to the hardware resources in the normal world.



# ARM TrustZone

## Context switch

- ▶ The **Non-secure** bit in the **Secure Configuration Register** is used to determine which world the processor is currently running.
- ▶ A third privilege mode: **secure monitor**, in addition to user and kernel.
- ▶ When the processor wants to switch the world, it first issues a special instruction **Secure Monitor Call** (SMC) to enter the secure monitor mode. Then it performs some cleaning works and enter the other world.

