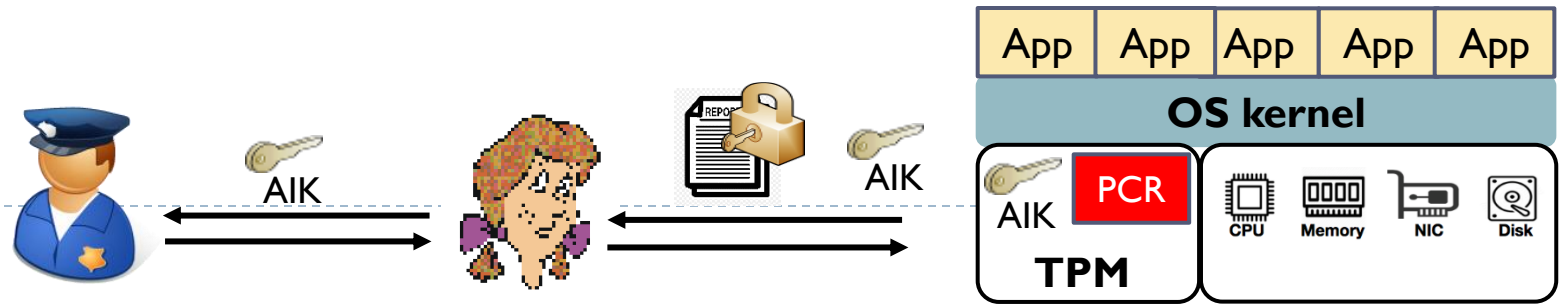
Remote Attestation with TPM

Integrity measurement architecture:

- TPM measures hash values of each loaded software, as integrity report.
- The hash values are stored in the Platform Configuration Registers (PCR) in TPM and could not be compromised by OS or any apps.

Remote attestation protocol

- TPM generates an Attestation Identity Key (AIK), to sign the hash values.
- The hash values together with AIK will be sent to client.
- A trusted third party, Privacy Certification Authority (PCA) is called to verify this AIK is indeed from the correct platform.
- Client uses this AIK to verify that received hash values are authentic.
- By checking the hash values, client knows if the loaded software is correct



Outline

- **Protection Strategies**
  - Confinement
  - Reference Monitor
- **Hardware-assisted Protection**
  - Basic Functionalities
  - Trusted Platform Module
  - Trusted Execution Environment

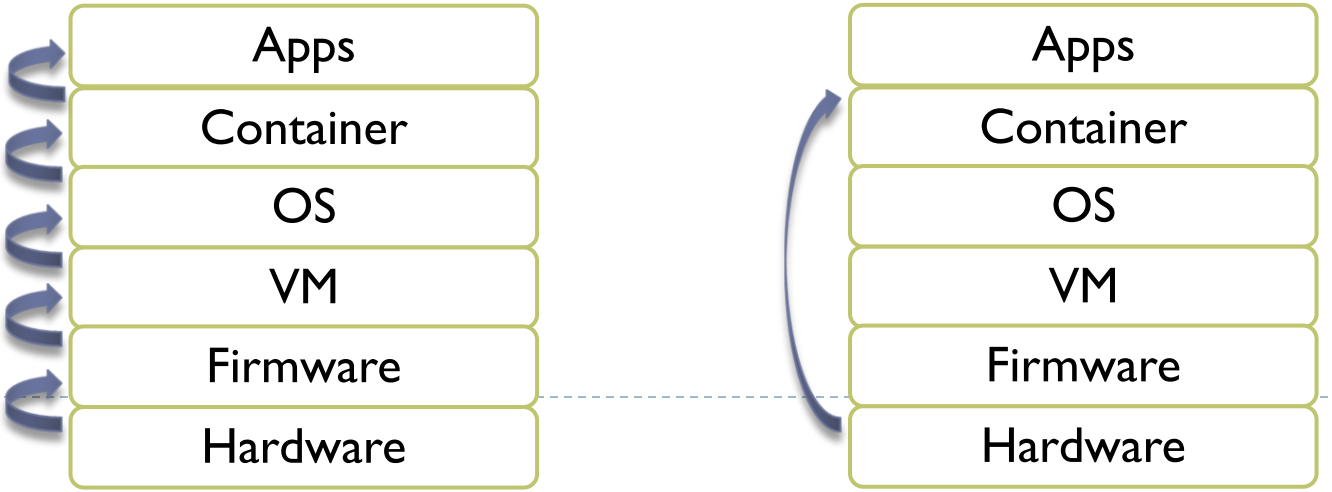
Untrusted Privileged Software

Chains of Trust can guarantee the integrity of secure booting, but not runtime security

- Even the privileged software (OS, hypervisor) is booted with integrity verification, it may still be compromised at runtime.
- How to protect applications with untrusted privileged OS or hypervisor?

Trusted Execution Environment (TEE)

- New hardware to protect the apps from untrusted OS or hypervisor.
- OS or hypervisor can support execution of apps, but not access their data



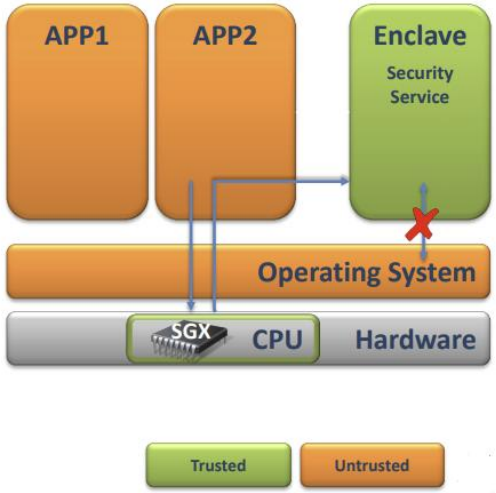
Intel Software Guard Extensions (SGX)

A security technology that safeguards application's data and code

- 2013: Intel introduced SGX in research papers
- 2015: officially launched with Intel's Skylake processor family
- 2016-2019: Improvements in SGX capabilities, expanding memory enclave sizes and strengthening security.
- 2021: SGX support removed from consumer desktop but retained in server.

Enclave

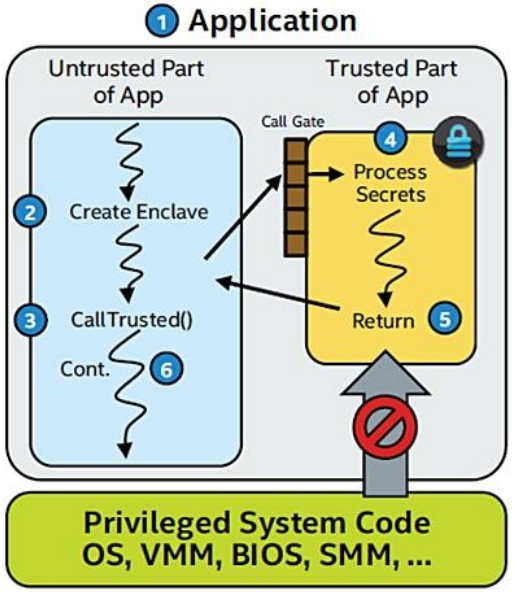
- An isolated and protected region for the code and data of an application
- Data in the enclave are encrypted by the processor when they are stored in the memory
  - Only the processor can access the data.
  - Attempts from other apps or OS will be forbidden and invoke exception



Application Execution in Enclave

The lifecycle of an application in enclave

1. An application is divided into a trusted part and an untrusted part.
2. The untrusted part creates an enclave and puts the trusted part into it.
3. When trusted code needs execution, the processor enters the enclave.
4. In the enclave, only trusted code can be executed and access the data.
5. After the code is completed, the processor exits from the enclave.
6. The untrusted part continues its execution.



Attestation with SGX

SGX also provides the attestation service.

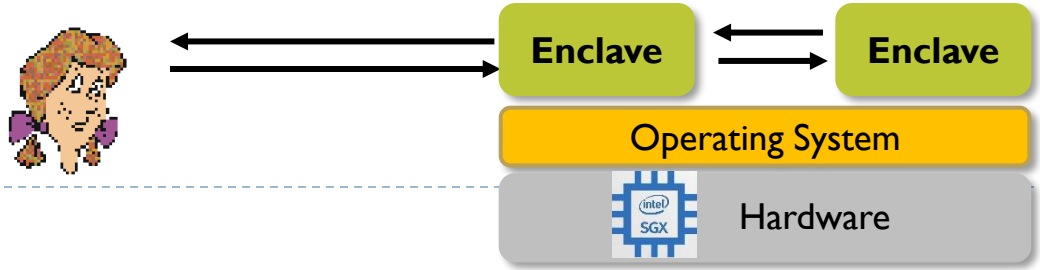
- Integrity measurement architecture: enclave measurement of the code, data, stack, heap, security flags, location of each page…
- Attestation protocol: attestation key and cryptographic protocol.

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.