Data Encryption with TPM

Full disk encryption

- Encrypt the data with the key in TPM.
- It is difficult for any attacker to steal the key, which never leaves TPM.
- TPM can also provide platform authentication before data encryption

Application: Windows BitLocker

- Disk data are encrypted with the encryption key FVEK.
- FVEK is further encrypted with the Storage Root Key (SRK) in TPM.
- When decrypting the data, BitLocker first asks TPM to verify the platform integrity. Then it asks TPM to decrypt FVEK with SRK. After that, BitLocker can use FVEK to decrypt the data
- With this process, data can only be decrypted on the correct platform with the correct software launched.

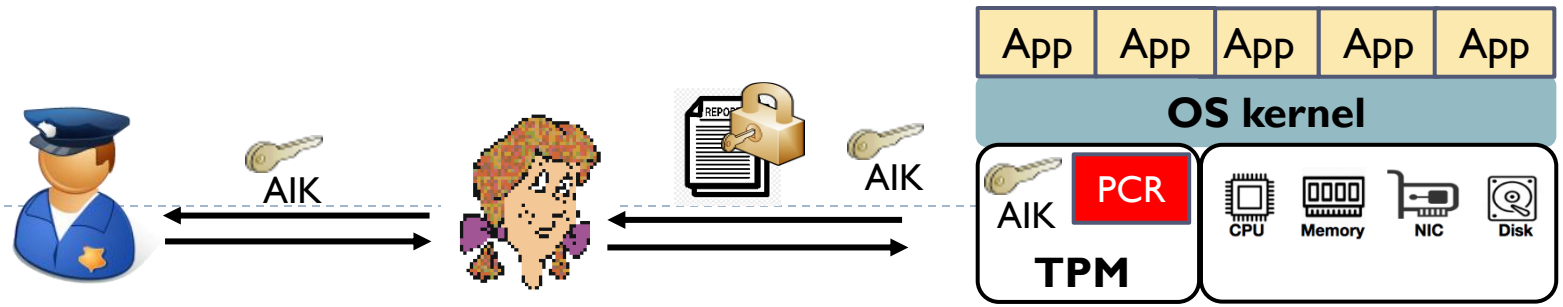
Remote Attestation with TPM

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

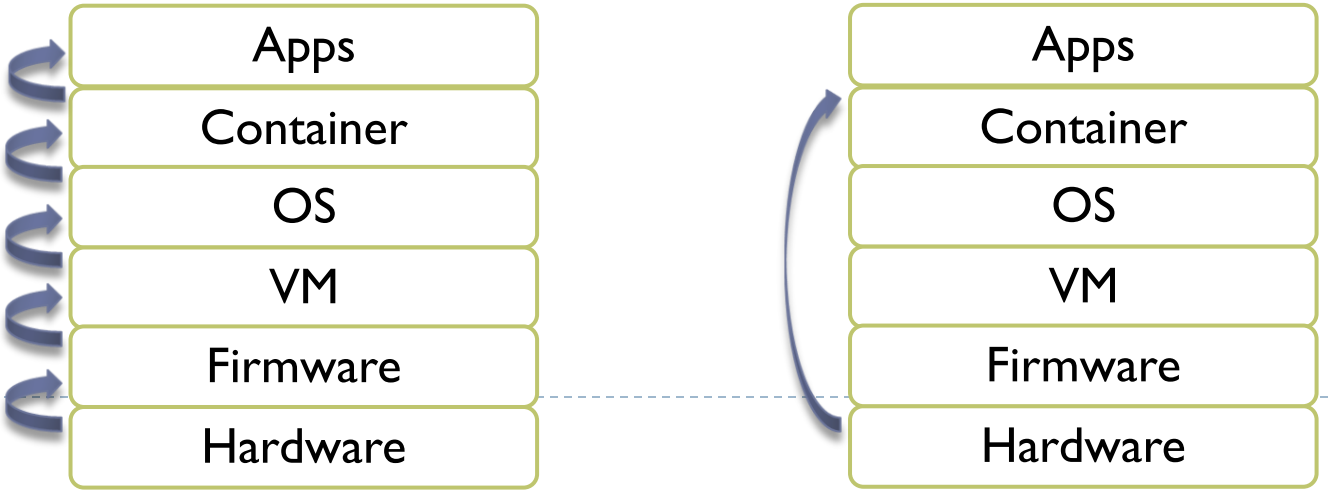
Untrusted Privileged Software

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