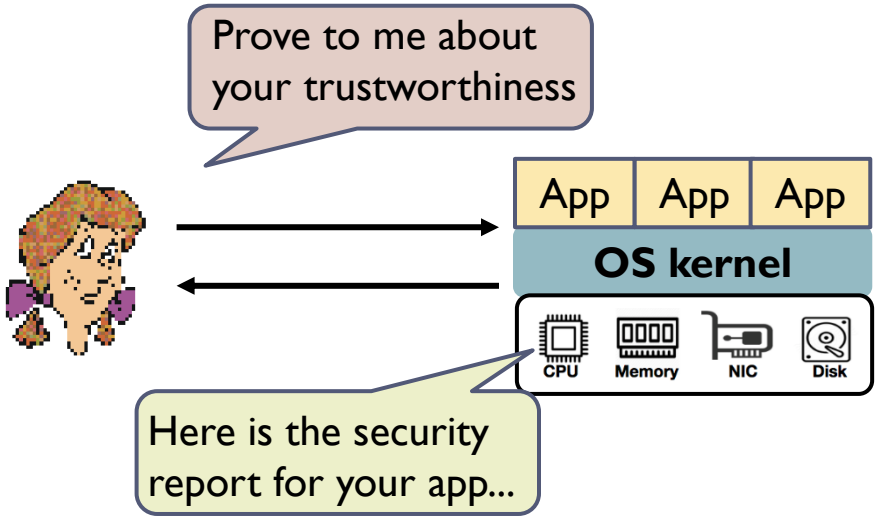
Basic Functionality: Remote Attestation

A mechanism that allows a user to know whether her app executes securely on a trusted platform.

- A remote platform provides unforgeable evidence about the security of its software to a client.
- A common strategy to prove the software running on the platform are intact and trustworthy.



Major components for remote attestation

- Integrity measurement architecture: provide reliable and trustworthy security report
- Remote attestation protocol: ensuring the attestation report is transmitted to the client without being modified by attackers in OS, apps or network

Outline

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

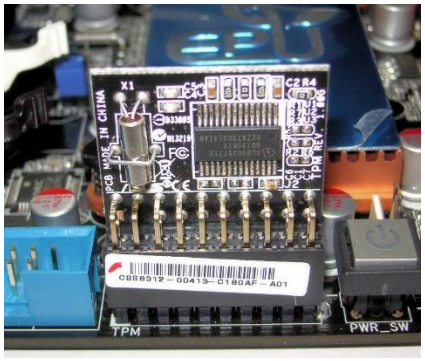
Trusted Platform Module (TPM)

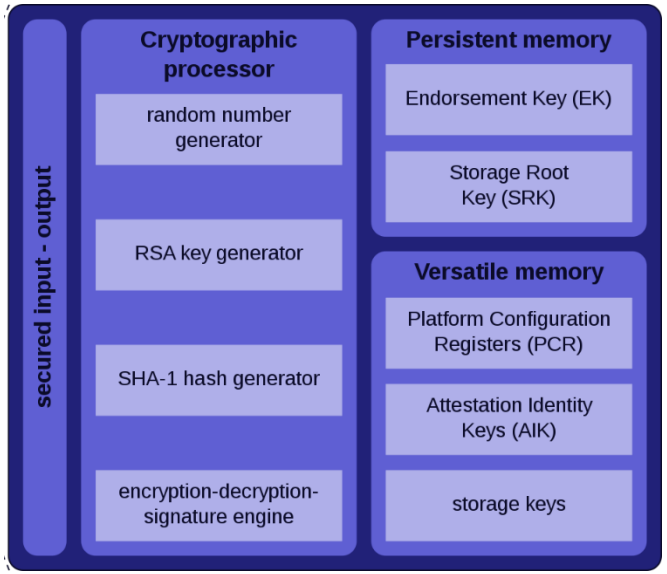
A chip integrated into the platform

- A separated co-processor
- Its state cannot be compromised by malicious host system software

Inside the chip

- Random number and key generators
- Crypto execution engine
- Different types of crypto keys.





Development and Implementation

Designed by Trusted Computing Group (TCG)

- First version: TPM 1.1b, released in 2003.
- An improved version: TPM 1.2, developed around 2005-2009
  - Equipped in PCs in 2006 and in servers in 2008
  - Standardized by ISO and IEC in 2009
- An upgraded version: TPM 2.0, released on 9 April 2014.

Application of TPM

- Intel Trusted Execution Technology (TXT)
- Microsoft Next-Generation Secure Computing Base (NGSCB)
- Windows 11 requires TPM 2.0 as a minimal system requirement
- Linux kernel starts to support TPM 2.0 since version 3.20
- Google includes TPMs in Chromebooks as part of their security model
- VMware, Xen, KVM all support virtualized TPM.

Building Chain of Trust with TPM

Chain of Trust: Establish verified systems from bottom to top

- From a hierarchic view, a computer system is a layered system.
  - Lower layers have higher privileges and can protect higher layers.
  - Each layer is vulnerable to attacks from below if the lower layer is not secured appropriately.
- TPM serves as the root of trust: establish a secure boot process from TPM, and continue until the OS has fully booted and apps are running.
  - The bottom layer validates the integrity of the top layer.
  - It is safe to launch the top layer only when the verification passes.

Potential applications

- Digital right management
- Enforcement of software license, e.g., Microsoft Office and Outlook
- Prevention of cheating in online games.