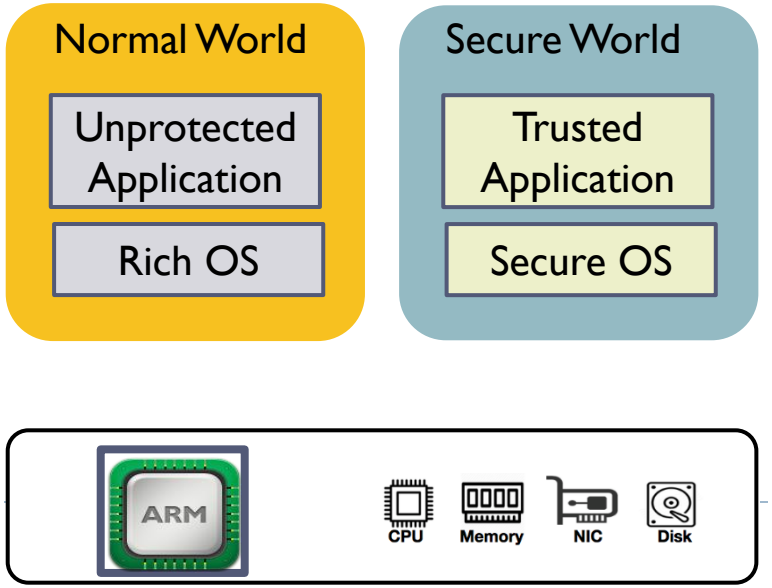
ARM TrustZone

The first commercial TEE processor (2003 in ARMv6 architecture)

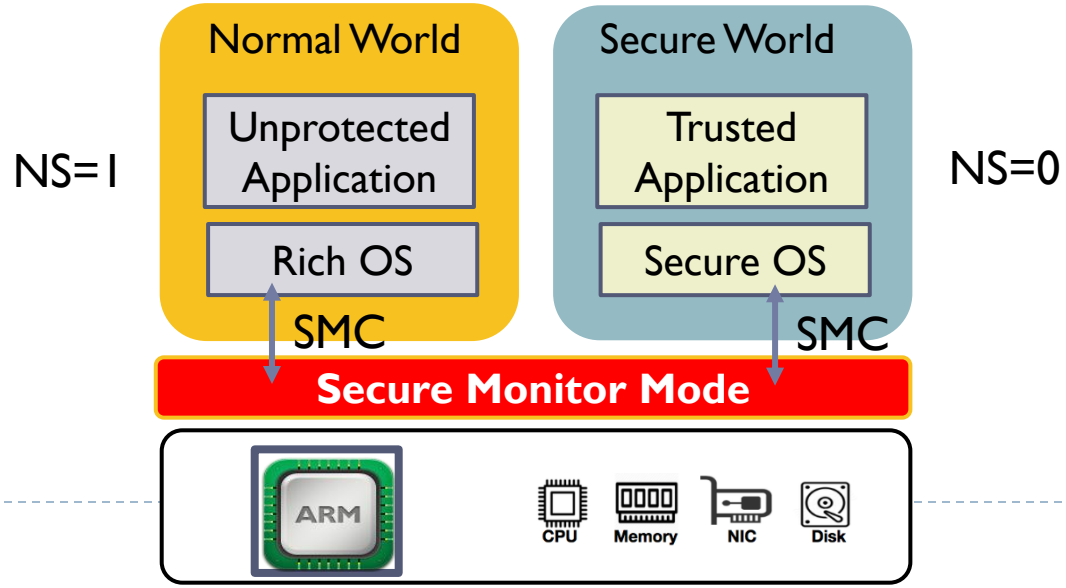
- Create two environments that can run simultaneously on the same processor. Each world has an independent OS
- Normal world: runs the normal unprotected applications and a rich OS. They have restricted access to the hardware resources in the secure world
- Secure world: runs the sensitive protected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



Application of TEE: Double-edged Sword

Positive usage

- Cloud computing: you do not need to trust the cloud provider
- Digital right management
- Cryptocurrency and blockchain

Negative usage

- Adversaries leverage TEE to hide malicious activities for stealthier attacks (conflicting with malware analysis)