

Miscellaneous

AMD SEV (Secure Encrypted Virtualization):

Security Focus : AMD's SEV aims to protect virtual machines from both the hypervisor and other VMs by encrypting each VM's memory separately.

Attestation Method : AMD SEV uses a hardware-based attestation method to prove the integrity of a VM. A package, usually including a measurement of the VM's initial state and various certificates, is provided for verification.

AMD SEV has additional extensions like SEV-SNP (Secure Nested Paging) to provide stronger security features, including protection against replay and roll-back attacks.

ARM TrustZone:

Security Focus : ARM TrustZone technology offers an efficient, system-wide approach to security for a wide array of client and server computing platforms, including IoT devices.

Attestation Method : TrustZone employs both hardware and software-based attestation techniques. These methods typically involve verifying a chain of trust from the hardware to the running software.

ARM TrustZone is not limited to just CPUs; it is a part of the broader ARM security ecosystem, which extends to other hardware like GPUs and NPUs (Neural Processing Units).

[Previous AWS Nitro Enclaves Next Device Attestation](#) Last updated 5 hours ago On this page * [AMD SEV \(Secure Encrypted Virtualization\)](#): * [ARM TrustZone](#):

Was this helpful?