PowerEdge Product Group

Direct from Development

AMD CPU Security Features in PowerEdge 14G Servers

Tech Note by:

George Mathew

SUMMARY
PowerEdge 14G servers with AMD CPUs deliver several new security features, including the AMD Secure Processor and hardware memory encryption.

The AMD Secure Processor, upon power on or reset, provides a secure root-of-trust by authenticating the initial Dell EMC BIOS code.

Hardware memory encryption brings new capabilities for both virtualized and non-virtualized environments. Secure Memory Encryption enhances data encryption for non-virtualized environments. Secure Encrypted Virtualization prevents a given hypervisor from being able to access the contents of another virtual machine

.

AMD CPUs installed in Dell EMC PowerEdge 14G servers offer several new security features. Key among these are the AMD Secure Processor, and hardware memory encryption, respectively. This brief tech note describes these two new features and their capabilities.

AMD Secure Processor and Platform Secure Boot

The AMD Secure Processor is an independent processor core integrated in the CPU package alongside the main CPU cores. Upon system power-on or reset, the AMD Secure Processor executes its firmware while the main CPU cores are held in reset. One of the AMD Secure Processor's tasks is to provide a secure hardware root-of-trust by authenticating the initial PowerEdge BIOS firmware. If the initial PowerEdge BIOS is corrupted or compromised, the AMD Secure Processor will halt the system and prevent OS boot. If no corruption, the AMD Secure Processor starts the main CPU cores, and initial BIOS execution begins. The BIOS is capable of maintaining the chain-of-trust up to the OS boot loader.

The very first time a CPU is powered on (typically in the Dell EMC factory) the AMD Secure Processor permanently stores a unique Dell EMC ID inside the CPU. This is also the case when a new off-the-shelf CPU is installed in a Dell EMC server. The unique Dell EMC ID inside the CPU binds the CPU to the Dell EMC server.

Consequently, the AMD Secure Processor may not allow a PowerEdge server to boot if a CPU is transferred from a non-Dell EMC server. Similarly, a CPU transferred from a Dell EMC server to a non-Dell EMC server may not boot.

Main Memory Encryption

Another new CPU security feature is hardware memory encryption, specifically Secure Memory Encryption (SME) and Secure Encrypted Virtualization (SEV). Both features enable a dedicated encryption engine built into the integrated memory controllers to encrypt data written to main memory and decrypt it when read. The AMD Secure Processor manages the encryption keys.

SME is designed for non-virtualized environments in which a single encryption key is randomly generated on each system reset. The encryption key is not visible to software running on the main CPU cores. The OS manages encryption via page tables.

In today's virtualized environments, hypervisors have unrestricted access to the contents of a guest virtual machine, i.e. the operating system, applications and data inside. This creates the possibility for the hypervisor to access guest data, or inject code into a guest virtual machine. It is also possible for a guest virtual machine to access that data of other guests.

SEV directly addresses this situation. Each virtual machine has a unique encryption keys, so a rogue virtual machine cannot access the contents of other virtual machines or the hypervisor. The encryption keys are controlled by the AMD Security Processor. The administrator does not have access to encryption keys. This prevents the hypervisor from being able to access a virtual machine's contents.

Some OS and hypervisor modification is required for both SME and SEV. AMD is working with the leading OS and hypervisor vendors on the required modifications.