PowerEdge Product Group

Direct from Development

Secure Boot and Secure Operation for VDI Environments with PowerEdge R6415, R7415, R7425 Servers

Tech Note by:
Sonja Hickey

SUMMARY

While there are many aspects of VDI deployments to consider, security risks should be considered and addressed.

Adequately securing a VDI environment goes beyond implementing just end-point and software-based security solutions.

Implementing Secure Boot and Secure Operation in infrastructure supporting VDI environments is critical.

Securing VDI environments goes beyond implementing end-point security. Other security-related issues need to be considered, especially risks associated with infrastructure supporting those environments. One such example regards security controls for the virtualized OS, which need to provide the same level of security as those used for operating systems running directly on hardware. IT professionals should also determine whether other pre-hypervisor (BIOS, boot loader, etc.) steps and configurations are invoked according to the enterprise's security standards. Physical security may not be the newest of risk mitigation techniques, but the IT professional's assessment of the VDI environment should include assurance that all related hardware is appropriately restricted relative to physical access, thereby reducing the chance that CPU boot processes could be altered. That being said, Secure Boot and Secure Operation are two critical security measures that should be considered for implementation in VDI environments.

Secure Boot

The main objective of malware writers is to make malicious code start as early as possible, enabling it to make modifications to the operating system's code and system drivers. Rootkits/bootkits are one of the most advanced tools available to cybercriminals since it enables malicious code to start before the operating system loads. 'Secure Boot' mitigates these threats by checking the cryptographic signatures for drivers and other code loaded prior to the OS running and preventing unsigned (untrusted) device drivers from being loaded.

Secure Operation

As many people know, systems provide encryption solutions for Data at Rest (on a HDD or SSD) and for Data in Motion (on a network), but data running in main system memory is not encrypted, leaving it vulnerable to attacks such as memory scrapes and cold boot attacks. 'Secure Memory Encryption' or SME mitigates this challenge by providing a solution that encrypts system memory and protects data at rest.

Implementing Secure Boot and Secure Operation

The combination of both hardware- and software-based security measures provide a far superior solution than implementing one or the other. Dell PowerEdge R6415, R7415 and R7425 servers, which are based on AMD EPYC processors, complete the second half of the equation by providing provide hardware-based security measures. These measures are implemented through what is called 'System-on-a-Chip' or SOC. This feature provides a dedicated 32-bit microcontroller located on the physical die of the chip.

SOC addresses the Secure Boot concern by prohibiting modifications to an operating system's code and system drivers. It does this by providing a hardware root of trust that is designed to ensure only known and trusted software is loaded and run from the initial boot load through the BIOS load. It does this through 4 steps, as follows (see Figure 1):

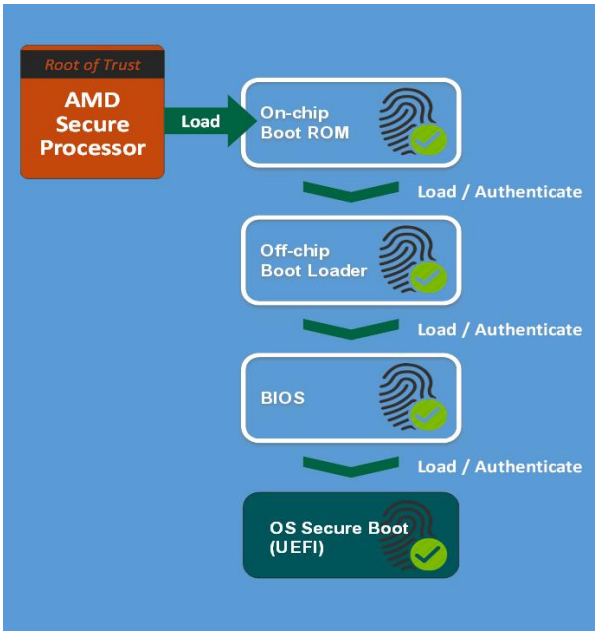

Figure 1: AMD EPYC Secure Boot Process

- An AMD 'Secure Processor' loads an on-chip, Boot ROM which includes a signing key (a key that is embedded in the AMD Secure Processor).
- The Boot ROM then loads and authenticates, via the signing key, an off-chip "OS Boot Loader'.
- This OS Boot Loader then authenticates the BIOS before the x86 cores start executing the BIOS code.
- Once the BIOS is authenticated, the OS Boot Loader loads the OS or Hypervisor.

The OS Boot Loader also authenticates/loads code for the AMD Secure Processor to perform secure key management.

Leveraging capabilities of the AMD EPYC processor, the PowerEdge R6415, R7415 and R7425 servers also ensure that "data at work" (data that is in main system memory) stays safe via AMD's 'Secure Memory Encryption' or SME. Like Secure Boot, the AMD Secure Processor enables this by generating a single key that is used to encrypt everything in system memory. An added benefit is that this can be enabled with no changes to applications or the OS/hypervisor.

In-depth technical explanations of the above can be found in the *Direct from Development* tech note, 'AMD CPU Security Features in PowerEdge Servers.'

Conclusion

There are many security aspects to address when implementing a VDI environment. While it may seem sufficient to implement end-point and/or software-based security solutions, security concerns associated with the underlying hardware must also be addressed. The Dell PowerEdge R6415, R7415, and R7425 servers, based on AMD EPYC processors, provide Secure Boot and Secure Operation security capabilities that prevent accidental or malicious alteration or corruption of BIOS, firmware and data in memory. In doing so, these features implement security at the hardware level, and should be seriously considered for implementation in servers that support VDI environments.