CYBER-RESILIENCY IN CHIPSET AND BIOS

Tech Note by:
Wei Liu
Seamus Jones

SUMMARY

New BIOS Features introduced in Dell EMC 14th generation of PowerEdge servers offer unique resiliency to malicious intent or user error.

Specific features outlined are:

- Intel Boot Guard Integration
- BIOS Recovery

These features enable customers to deploy routine BIOS updates without worry or risk of catastrophic corruption, ensuring the benefits of updated platforms for the full product lifecycle.

Basic Input Output System (BIOS) is implicitly a critical element of any solution stack and since the BIOS persists between power cycles it poses a potentially attractive target for malicious attacks. The CIH, also known as Chernobyl or Spacefiller virus was the first large scale industry wide virus that attacked a system BIOS.* First seen in 1998 it impacted over 60 million IT systems from multiple manufacturers and demonstrated how important it is to consider BIOS security and recovery.

Today, because of Dell EMC BIOS innovations and partnerships with chipset manufacturers, corruption incidents like this are extremely low. Due to the critical nature of the BIOS and the perceived risks of updating, some customers hesitate to perform scheduled updates during a server lifecycle. This can leave a platform or organization exposed to even further threat or performance issue. For this reason we have implemented multiple new features, the two outlined here are Boot Guard and BIOS Recovery. These ensure that the server is immune to compromise of OS, BIOS, System Management Mode (SMM), or Intel Management Engine (ME).

Protection at the Chipset

The Dell EMC 14th generation of PowerEdge servers support Intel Boot Guard verified boot feature. The Boot Guard extends the platform root of trust to the Platform Controller Hub (PCH). The PCH contains One-Time-Programmable (OTP) fuses that is burned by Dell EMC factory during the manufacturing process with selected Boot Guard policy and the hash of the Master Public Key.

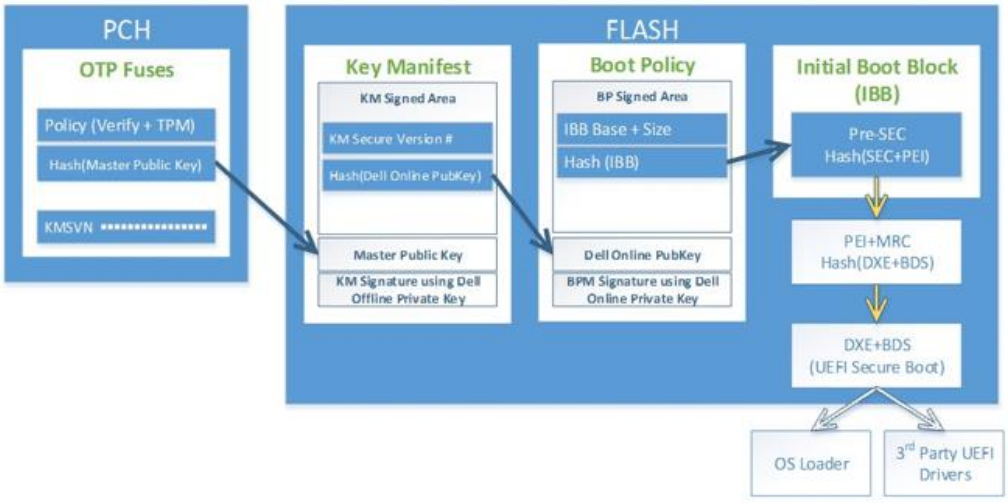


Figure 1: Intel Boot Guard process

*According to National Institute of Standards and Technology (NIST) document Special Publication 800-147

The Key Manifest on the BIOS SPI flash is signed by the Dell EMC Master OEM key, and delegates authority to the Boot Policy Manifest key. Then the Boot Policy Manifest authorizes the Initial Boot Block (IBB), which is the first BIOS code module to execute at reset vector. If the IBB fails authentication, Boot Guard will shut down the system and not allow it to boot. Each BIOS module contains a hash value of the next module in the chain, and uses the hash value to validate the next module. The IBB validates (SEC+PEI) before handing off control to it. The (SEC+PEI) then validates (PEI+MRC) and (PEI+MRC) further validates the (DXE+BDS) modules. After that point, the UEFI Secure Boot, if enabled, can extend the root of trust to the remaining BIOS, third-party UEFI drivers, and OS loader.

Cyber Resilient Redundant Recovery Options

The BIOS on Dell EMC PowerEdge Servers has industry-leading high security and quality standards, however, to further provide customers a peace of mind against potential cyber-attacks, Dell EMC has introduced an innovative BIOS Recovery feature found within PowerEdge 14G servers.

On each server there are two BIOS SPI ROMs, one is the primary ROM, another recovery ROM. The recovery ROM is offline in normal boot.

In case the primary ROM is corrupted, possibly due to an exploit from hackers or a power loss while updating the BIOS, a BIOS recovery process will be automatically triggered at system reset.

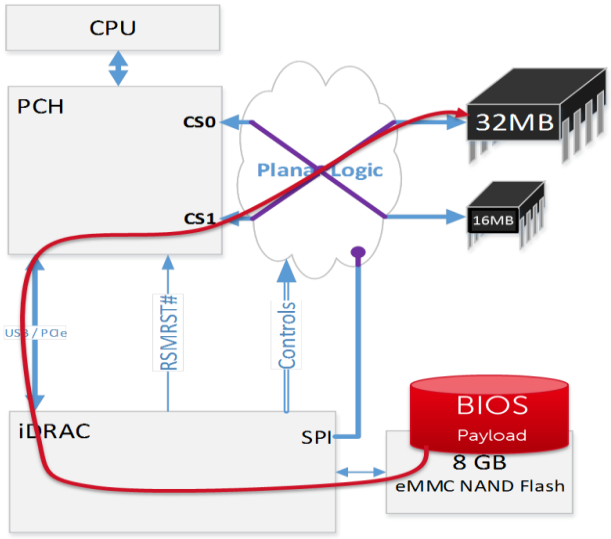
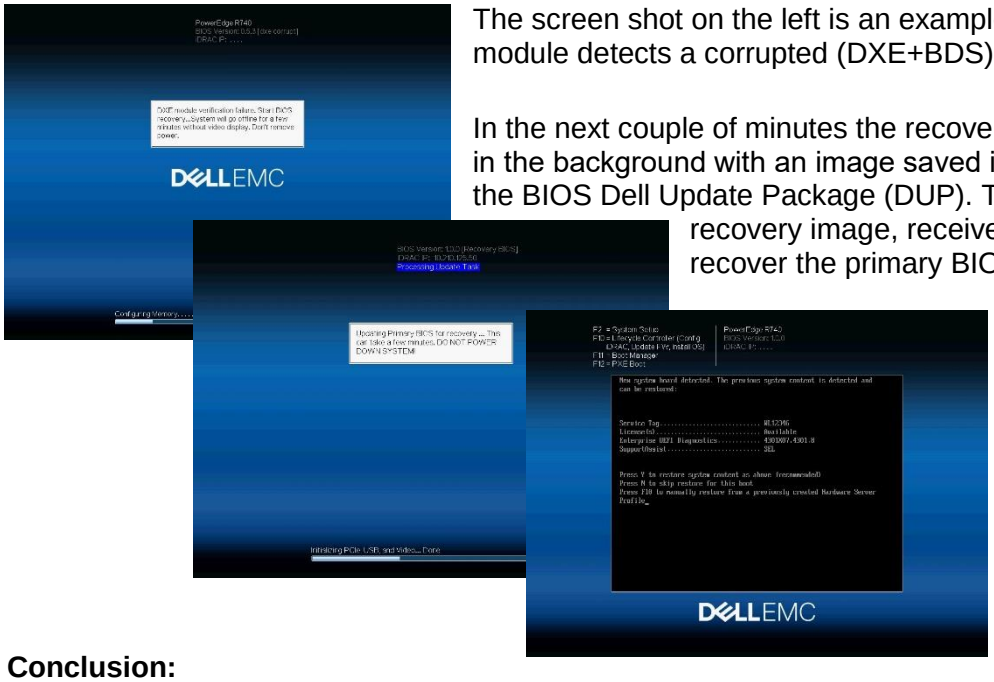


Figure 2: BIOS Recovery Process



The screen shot on the left is an example when the BIOS (PEI+MRC) module detects a corrupted (DXE+BDS) module in the chain.

In the next couple of minutes the recovery BIOS ROM will be programmed in the background with an image saved in iDRAC that's last updated via the BIOS Dell Update Package (DUP). The system will then boot from the recovery image, receive an update task from iDRAC and recover the primary BIOS ROM.

After the primary BIOS ROM is recovered, the recovery ROM will become offline again. The system will reset to boot from the primary BIOS and the system configuration settings such as Service Tag can be restored during POST.

The Lifecycle Log would contain the logs for BIOS recovery.

Conclusion:

The Dell EMC 14th generation of PowerEdge servers contain innovative features which offer new ways to protect and recover BIOS, ensuring platform integrity throughout the full server lifecycle. Intel Boot Guard and BIOS Recovery are just further demonstration of our engineering commitment ensuring the security and stability of your enterprise infrastructure.