Secured Component Verification

Dell Technologies

April 30, 2021 – Version 1.0

Prepared for
Dell Technologies

Prepared by
NCC Group

Executive Summary

Synopsis

During February 2021, Dell engaged NCC Group to conduct a security assessment of their supply chain security functionality and related and supportive foundational security functionality on 14th and 15th generation Dell servers. Documentation and source code was provided as well as access to a running lab server via network access, with access to both the Dell integrated remote access controller, iDRAC which is the BMC and server host network interfaces. The assessment was carried out by specialized consultants from NCC Group's Hardware and Embedded Systems practice who have expertise in areas of secure product manufacturing systems.

NCC Group is a global information assurance firm that specializes in application, mobile, network, host, and product security. Security conscious companies use NCC Group to verify product attributes in view of current security best practices, standard security functionality, and product protection. More information about the Group's processes and products can be found at https://nccgroup.com/us.

It is important to note that this document represents a point-in-time evaluation of security posture. Security threats and attacker techniques evolve rapidly, and the results of this assessment are not intended to represent an endorsement of the adequacy of current security measures against future threats. This document necessarily contains information in summary form and is therefore intended for general guidance only; it is not intended as a substitute for detailed research or the exercise of professional judgment. Any mention of effort or length of engagement is not intended to convey coverage; specifically, NCC Group makes no claim of complete coverage of the target(s) of this document. The information presented here should not be construed as professional advice or service.

Scope

The goal of this assessment was to determine the degree to which the Secured Component Verification (SCV) feature succeeds in providing assurance of a build-time component inventory and to highlight the threats it protects against. This assessment was performed by NCC Group under the guidelines provided in the statement of work for the engagement. The scope for attack scenarios we were commissioned to assess were supply chain interdiction attacks assuming temporary possession of the hardware during transport. This included a review of SCV provisioning processes in the factory through to product delivery and the use of SCV for system validation. Our approach included two phases:

1. Review of the SCV system design and implementation, and enumerations of dependencies
2. Review of various technologies that support SCV

Compromises of the factory infrastructure were not considered to be within scope for this assessment, however Dell does make additional information in this area available on their website.[1] Also out of scope for this engagement were possibly compromised component supply chains prior to the factory build process. However, we were provided with documentation and an interactive workshop with key engineers discussing technical details of internal processes for building and provisioning Dell servers, as well as generating, signing and installing the SCV inventory certificates on the server with follow up support for subsequent questions raised. Finally, the scope did not include a review of any logistical security controls that exist in the shipping process such as sealed containers, GPS tracking, trusted escorts, and other measures discussed in the Dell supply chain assurance whitepaper which may further frustrate an attacker.

Key Findings

It is NCC Group's opinion, that Dell has a mature product security program. They have a long history of engaging with external security partners like NCC Group to perform security reviews of their systems, and new features as they are developed. Their Secure Development Lifecycle continues to consider security throughout the product development process, where security can be built into the product from the earliest stages.

The SCV feature is a system identity framework. This framework is an ideal architecture for strong system identity attestation that puts Dell in position to effectively make use of several emerging standards for device attestation. During our background research it became clear that Dell is proactive and involved in the development of many of these emerging standards. As these standards mature they will enable third party component vendors to provide strong

[1] https://i.dell.com/sites/csdocuments/CorpComm_Docs/en/supply-chain-assurance.pdf

component attestation guarantees that many do not have today, and SCV is poised to leverage such improvements as they become available.

Intel BootGuard and AMD Platform Secure Boot are host processor features that provide strong firmware integrity guarantees, preventing firmware other than that authorized by the OEM from executing on the system. By enabling these as additional defense-in-depth measures, certain classes of physical attacks are mitigated, such as flash memory replacement or reprogramming, and Time-of-Check-Time-of-Use (TOCTOU) race conditions. All combined, the Root of Trust features in the system make compromise of the TCB difficult.

The SCV framework leverages well established cryptographic constructions throughout the implementation. In particular, the Proof of Possession and Remote Attestation processes provide strong cryptographic guarantees of system identity and certain vital components of the system build that tie them strongly to the platform Root of Trust in the iDRAC. Overall, we found that cryptographic measures such as device specific hardware root keys (HRK) are used in ways which will substantially increase the difficulty of extracting and cloning credentials. Sensitive key management functions are designed around a mature PKI that leverages HSMs, which is already in use in the Dell factories.

SCV verifies the security of the iDRAC subsystem early in its validation process using a strong attestation protocol before performing any other component validation. This ensures that inventory validation is happening only after the trust anchor is confirmed, ensuring that the report doesn't falsely report valid matches in the instance where the iDRAC is itself not verifiable. This is particularly important as the SCV inventory itself has no challenge response protocol intrinsic to it - SCV has a trust relationship with iDRAC, as it reports on the state of hardware components, and the attestation-testing first gives it a basis for this trust.

SCV represents a significant step from which to build a comprehensive, trusted and authenticated component inventory. As more third party component vendors implement strong attestation mechanisms, the assurance that SCV offers to customers will only increase. Dell is engaged with partners in the ecosystem to enable the ongoing improvements necessary to provide such component-level assurances, and the SCV framework easily supports such improvements.

Finally, several other opportunities for system improvement were reported to Dell along with recommendations, including improved DMA protections, and some recommendations for improved customer guidance when performing SCV validation.

Secured Component Verification is a Dell system intended to provide last-leg assurance of product integrity from order fulfillment at the Dell factory through to end-user delivery. To accomplish this, after a server has been built in the factory, applications are executed on the host which collect a manifest of installed components, and cryptographically sign them using Dell's PKI. This signed manifest is then stored securely within the iDRAC BMC subsystem. Later, upon delivery, the manifest data collection is repeated by the customer, and compared against the data stored in the signed certificate which will reveal system modifications.

High Level Process Flow

The SCV process begins when a customer places an order for a system:

1. Dell receives an order, and starts building the system to the specifications of that order
2. After this device is built, a collection script is executed on the *host* OS, gathering identifying characteristics of the various system components as described above.
3. This device hardware inventory is cryptographically signed using an intermediate certificate by Dell's PKI to produce an inventory certificate.
4. The inventory certificate is stored in the iDRAC, via the RACADM interface.
5. The inventory is validated again using the SCV process before being shipped for delivery.

After delivery of the product through some untrusted delivery agent, and before deployment, the customer performs the SCV verification. To accomplish this, they boot the system from a known-good OS image (using PXE boot), download the signed "iDRAC Tools" package from the Dell website[2,3](over HTTPS) and execute a collection application from this toolkit which:

1. Extracts and validates the signed manifest from the iDRAC.
2. Collects a manifest of the product's components as delivered.
3. Compares this collected manifest to the manifest retrieved from the iDRAC. Any mismatches are reported as failures.
4. For devices supporting cryptographic Proof of Possession (such as iDRAC), such validation of identity is also confirmed as discussed in Cryptographic Approach on page 6.

[2] https://www.dell.com/support/home/en-uk/drivers/driversdetails?driverid=gw4vd
[3] https://www.dell.com/support/home/en-us/drivers/driversdetails?driverid=ywr16

The primary class of threat that SCV is intended to address is known as "Supply Chain Interdiction". Here, a threat actor would intercept a shipment of products and install a malicious implant (such as malware or a backdoor) before forwarding the system to the intended recipient. A Supply Chain Interdiction attack could be leveraged to undermine the trusted computing base (TCB) or the hardware of a server during the period between when it leaves the factory and when it arrives at the customer premises. Such attacks are known to have been conducted by the NSA in the past,[4] however there is no reason to expect the NSA to hold a monopoly on such capabilities. Dell customers have begun requiring protections in this area, and Dell competitors have announced varying degrees of protections as well.

Plausible attackers may include nation states with various policy goals, organized crime with financial or extortion intents, and counterfeiters replacing components with lower quality parts and other grey-market profit aims. That is to say that the capability of such attackers may range from simple component or firmware swapping in transit, through to the installation of sophisticated hardware implants to interpose sensitive signals resulting in persistent transparent attacks on the system after delivery and installation in the customer environment.[5] A system without defenses like SCV is vulnerable to a number of attacks including simple firmware replacement (BIOS/UEFI) and PCIe device replacement. Multiple specific attack vectors are defended by SCV which are discussed in more detail below.

The following summarizes the specific attack avenues that were considered during NCC Group's review of the SCV system and its dependent technologies within the Dell server design.

1. **BMC Considerations:** Installed on every system, within the iDRAC, is a device-specific attestation key and certificate. This enables each Dell server to attest to its own identity. The iDRAC uses a hardware-backed encrypted storage mechanism and implements appropriate ROM-based firmware validation, and together these are an effective protection against direct attacks on the secure storage. Given the privileged position of the iDRAC within the server, the protections around the private attestation key and its use were explored in detail.
2. **Dependence on Data From Peripheral Devices:** While most component vendors in the industry have yet to provide mechanisms for strong attestation, looking forward, the SCV system is well-suited to take advantage of new specifications for standardized trusted device identification as discussed in Secured Component Verification on the previous page. Furthermore, we considered threats from peripheral devices (i.e. DMA attacks) and their communication channels (demonstrated by devices like *TPM Genie*[6]) to determine if such attacks might be feasible to compromise the SCV validation process.
3. **SCV Dependence on the iDRAC Root-of-Trust:** The core of SCV's trusted functionality exists inside of the iDRAC execution environment. Much of the manifest collection process depends on collecting data from device enumeration functionality offered by iDRAC. iDRAC provides a separate security domain which helps put large portions of the security guarantees provided by SCV out of harms way from potential exploits that affect the x86 host portion of the system.
4. **A compromise during SCV validation** is largely prevented by encouraging the customer to provide their own known-good system images on which the SCV validation tools will execute. The system by default is shipped in a state to PXE boot from the network, allowing the customer control over the system image. The SCV validation tools themselves are not shipped with the system, but are instead downloaded directly from a known-good source on Dell's website. This leaves only the system firmware and hardware available for the attacker to try to subvert, which is protected by the system root of trust.
5. **The SCV Inventory Signing Process** depends very little on external factory systems other than the Certificate Signing Request (CSR) to the Dell PKI system, which reduces the opportunity for compromised factory systems being used to subvert the SCV inventory process. The PKI itself makes use of Hardware Security Modules (HSM) for key management. By performing the SCV signing step late in the manufacturing process, this also provides additional opportunities for Dell to audit possible grey-market activities that may be occurring in their factories.[7]

[4] https://www.aclu.org/files/natsec/nsa/20140722/Stealthy%20Techniques%20Can%20Crack%20Some%20of%20SIGINT%27s%20Hardest%20Targets.pdf
[5] https://www.wired.com/story/plant-spy-chips-hardware-supermicro-cheap-proof-of-concept/
[6] https://github.com/nccgroup/TPMGenie
[7] https://research.nccgroup.com/wp-content/uploads/2020/07/secure-device-manufacturing-supply-chain-security-resilience-whitepaper.pdf

Cryptographic Approach

Robust systems use cryptography to provide strong guarantees of system integrity, and the SCV framework is no exception. Cryptographic protections are used in several key places within the SCV system, including:

1. Use of HTTPS for communication with factory signing servers and for customer SCV verification tool download
2. SCV certificate signing
3. Proof of Possession and Remote Attestation

SCV Certificate Signing Process

The SCV process gathers an inventory of currently installed hardware components, and compiles their identifiers into a certificate issued by a Dell certificate authority. This certificate (known as the SCV Certificate) also contains a public key associated with a private key stored in the iDRAC for proof-of-possession attestation purposes. The SCV certificate signing process is built on the Dell PKI and leverages the existing factory Hardware Security Modules (HSMs). HSMs are a common base for a strong key management system. During the SCV factory process, a certificate is built using the collected device inventory data, and a Certificate Signing Request (CSR) is issued to the PKI where it is signed using an intermediate certificate authority. This signed certificate is then stored within the iDRAC secure storage.

The fact that the SCV process occurs mostly on the host is beneficial in certain ways, as it reduces the opportunity for compromised factory systems being used to subvert it. The only external interaction during the SCV inventory is the CSR to sign the inventory and certificate information stored by the iDRAC. The subsequent customer validation process does not require any external interactions (beyond downloading and installing the SCV validation tools).

Proof of Possession and Remote Attestation

As part of this assessment, documentation and source was reviewed to assess the interaction of SCV with remote attestation of components. There are currently two remotely attestable components supported by the server (iDRAC and TPM), and more can be added in the future as peripheral devices support it. Remote attestation is made available as a service via the Redfish REST API. Of these, the iDRAC is the only component which currently has its identity certificate embedded within the SCV inventory.

The SCV process requires trusting the integrity of both the host system performing the verification and the iDRAC with which it communicates to retrieve component inventory information. This section examines mechanisms in place to protect the integrity of code running on the host processor and iDRAC.

Host

14th generation and newer Dell servers use hardware mechanisms to verify the integrity of platform firmware including UEFI BIOS before it is executed. The primary chain of trust begins with Intel Boot Guard or AMD Platform Secure Boot (AMD-PSB), depending on the choice of CPU in the customer's build order. Both of these mechanisms establish a silicon-based root of trust by using immutable ROM code (located within the PCH for Intel, and within the PSP for AMD) to validate the signature of the initial host code loaded from external SPI flash. The public key used for this validation is programmed into internal one-time-programmable memory. After signature validation, the initial code is then executed on the host, and it will in turn validate the next stage code before it is executed, which then validates subsequent stages, forming a secure boot chain up to the UEFI BIOS where traditional UEFI Secure Boot mechanisms continue the validation chain.

When validation of a boot stage fails, automatic BIOS Recovery is initiated by the iDRAC. Since Intel Boot Guard and AMD-PSB both validate code after it is copied into RAM from which it is executed, these mechanisms are resistant to Time of Check to Time of Use (TOCTOU) vulnerabilities.

Additionally, 15th generation Dell servers use the iDRAC to verify the integrity of firmware in SPI flash (Code ROM) before initiating power sequencing for the main system. iDRAC-based pre-boot firmware verification checks the integrity of not only the Initial Boot Block (IBB) or PSP firmware, but also later firmware stages loaded as part of the secure boot chain. This defense-in-depth measure protects against potential flaws in later stages of firmware validation in the chain of trust built upon Intel Boot Guard[8] or AMD's Root-of-Trust mechanisms.[9] iDRAC on 15th generation servers can also perform runtime integrity checking of the Code ROM through SPI multiplexing while the host system is running - a feature known as BIOS Live Scanning. This is possible because these servers use separate memories for Code ROM and Data NVRAM, and firmware code for the host is copied into and executed from RAM. This helps detect and mitigate against unexpected BIOS updates such as bootkits.

Since SCV validation is performed by an application running on the host operating system, it is necessary for the host OS environment to be trusted. While UEFI Secure Boot can theoretically be used to establish a chain of trust including the full OS environment, this is difficult to achieve with most stock operating systems when physical access by the attacker is assumed. Desktop/Server distributions of Linux and Windows have mutable filesystems that are not integrity protected. To defend against possible exploits, Dell pre-configures servers to PXE boot from the customer's network, allowing the customer to provide a known-good OS image. NCC Group further recommends that when a server is received, the boot drive should be wiped and the operating reinstalled from a known-good source to clear any potentially malicious modifications to the host operating system.

iDRAC

iDRAC 9 which is used on 14th and 15th generation Dell servers introduces a hardware root-of-trust for boot-time firmware verification. The iDRAC 9 boot ROM verifies the integrity of a first stage bootloader after it is loaded from flash memory. The public key for this validation is programmed in internal one-time-programmable memory. This first stage bootloader loads and verifies a second stage bootloader (U-Boot), which in turn loads and validates the iDRAC Linux kernel and filesystem. Thus, the entire iDRAC operating system is integrity protected, even against attacks which reprogram iDRAC flash memory through physical access.

On iDRAC 9 firmware version 4.40.00.00 and newer, dm-verity[10] is also used to verify filesystem integrity at runtime, defending against Time-of-Check to Time-of-Use (TOCTOU) attacks such as those using flash multiplexers.[11] The boot

[8] https://conference.hitb.org/hitbsecconf2019ams/materials/D1T1%20-%20Toctou%20Attacks%20Against%20Secure%20Boot%20-%20Trammell%20Hudson%20&%20Peter%20Bosch.pdf
[9] https://storage.googleapis.com/wzukusers/user-28822230/documents/5c5b3fd28b669cTWPzwo/AMDFlaws%20Lecture%20Slides.pdf
[10] https://www.kernel.org/doc/html/latest/admin-guide/device-mapper/verity.html
[11] CVE-2019-11098 is an example of a TOCTOU vulnerability: https://bugzilla.tianocore.org/show_bug.cgi?id=1614

ROM and subsequent bootloaders in the iDRAC 9 boot chain also implement anti-rollback functionality, to prevent attackers from reverting to older (but validly signed) firmware images to exploit known vulnerabilities that have been fixed in more recent images.

Since iDRAC configuration is stored on a separate partition, an iDRAC hard reset[12] should be performed upon receipt of a server from an untrusted supply chain prior to running SCV. This will restore factory default settings.

Each iDRAC 9 is provisioned with a unique private key stored within a hardware-backed key store, and a Dell-issued certificate with the associated public key. Within the SCV solution, this certificate and key pair is used for a proof-of-possession challenge/response handshake between the host and iDRAC to confirm the presence of the genuine iDRAC associated with the SCV certificate.

Version 3.21.21.21 and newer[13] of iDRAC 9 firmware limit the impact of potential software vulnerabilities in iDRAC by minimizing the privileges of most user-space processes. By running these processes as non-root users and further limiting their privileges by granting the minimum necessary access though SELinux and file permissions, the impact of vulnerabilities in these processes is limited to what these processes are able to access.

[12] https://www.dell.com/support/kbdoc/en-ca/000126703/how-to-reset-the-internal-dell-remote-access-controller-idrac-on-a-poweredge-server
[13] https://downloads.dell.com/manuals/all-products/esuprt_solutions_int/esuprt_solutions_int_solutions_resources/dell-management-solution-resources_white-papers20_en-us.pdf