New Security Features in Integrated Dell Remote Access Controller 7

The new Dell Integrated Dell Remote Access Controller version 7 for Dell PowerEdge 12th generation servers delivers key security features with comprehensive management and enhanced functionality.

Dell │ OpenManage Systems Management

Contents

This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

April 2012| Rev 1.0

Introduction

The Integrated Dell Remote Access Controller version 7 (iDRAC7) provides comprehensive management, without relying on OS agents, for Dell™ PowerEdge™ 12th generation servers. In addition to many new functional and ease-of-use features, iDRAC7 includes the following new key security features. For more information, go to www.dell.com/idrac7.

- Firmware code signing and verification
- Built-in Hidden Root Key (provides a number of Trusted Platform Model (TPM)-like features to iDRAC)
- Credential Vault
- Field Service Debug Authorization Facility
- Lifecycle Controller wipe

iDRAC7 firmware signing

In response to a growing concern in the security industry and among security conscious customers about the threat of malicious firmware, iDRAC7 firmware updates are signed and verified. Updates are signed near the end of the firmware build process. The signatures are verified when firmware updates are later applied by customers. The signature generation and verification processes are as specified by the US Digital Signature Standard (FIPS-186-3). This verification results in a high level of assurance that iDRAC7 only runs firmware designed and delivered by Dell.

The threat landscape

In the last few years, the threat of “phlash attacks” has gone from a theoretical concern to a real phenomenon. From router rootkits, to hacked printers, to proofs of concepts of car hacks, to the many instances of “open source firmware,” the viability of changing or replacing the manufacturer’s firmware is well established.

While it would be both annoying and inconvenient to have a hacker ruin a home ink jet printer, a phlash attack against a server management solution, such as iDRAC7, could have much more serious consequences. Because iDRAC7 performs the important function of managing servers remotely, it can also provide a ready vehicle for attacking servers. Using iDRAC7, server operation can be disrupted in a large number of ways: from powering off the server all the way to erasing RAID configuration. Remote access solutions even provide a way to remotely boot a server with the OS image of an attacker’s choice.

Keeping pace

Dell server technology is keeping pace with the threat landscape by following a process of continuous security improvement and innovation. Our focus is on good security features and on secure development practices, while minimizing customer impact and providing high value. Firmware code signing and verification exemplifies this approach.

The build process: signing the firmware

IDRAC7 firmware signing and verification use industry standard cryptographic hashing and private/public key encryption technologies. The iDRAC7 firmware contains the public (verification) key.

The engineering team that designs and builds the iDRAC7 includes a group known as PG Release Engineering (PGRE). The PGRE team, while small, supports a wide variety of engineering activities. In particular, the team supports a single-purpose signing server. The signing server accepts unsigned firmware images, signs them with the private (signing) key, and returns the signed image. During this process, the private key never leaves the signing server. Because the signing server is maintained by a small group, the private key is only accessible to a handful of trusted individuals.

In addition to the actual iDRAC7 firmware, a number of other binary images that the iDRAC7 Lifecycle Controller technology manages are also signed. These other signed components are the driver pack (used during OS deployments), embedded diagnostics, and the iDRAC7 user interface that is accessible during boot (formerly known as the Unified Server Configurator).

Field update: verifying the firmware signature

As part of applying a field update of iDRAC7, the existing firmware performs the cryptographic inverse of the signing operation, using the public key that is built into the existing firmware's image. If the signature verification fails, the update process is aborted.

Firmware downgrades

The firmware signing scheme allows firmware downgrades as long as the downgraded version is signed with the same key that the existing firmware is verifying against. In the unlikely event of a compromised private key (see following section), firmware downgrades are not allowed.

At Dell, we realize that allowing firmware downgrades can be viewed as a security weakness. We have deliberately chosen to allow downgrades in order to maintain ease-of-use and supportability. If the threat landscape or customer demands require it, we may change this behavior in a future version.

In the unlikely event of a compromised private key

iDRAC7's signing scheme allows a new firmware signing key to be introduced if the existing key is compromised. A new signing key is introduced by creating a version of iDRAC7 that:

- Has the new signing key built into the image, and
- Is signed by the existing key

Because the new firmware is signed with the existing key, existing systems will determine that it is authentic; but subsequently, it will only allow firmware versions to be signed with the new key.

Built-in unique Hidden Root Key

Each iDRAC7 contains a unique binary value "burned" into the silicon. This 256-bit unique value cannot be read by the iDRAC7 firmware or any other software component. iDRAC7 also contains several cryptographic acceleration engines, one of which is a 128/256 bit AES engine. (The other cryptographic engines are: ECC 160/256, RSA 1024/2048, DES/TDES, random number generator, SHA1 and SHA-256.) The iDRAC7 firmware can program the AES 256 engine to use this unique value for encryption/decryption operations. iDRAC7 takes advantage of this capability to create a “root of trust” within iDRAC7’s early boot code.

Hidden Root Key: keeping secrets confidential

This 256-bit unique, hidden value is called the Hidden Root Key (HRK). The HRK is cryptographically composed from three sources: a 256-bit fused random value in iDRAC7’s CPU unit, a Public Key that is contained in iDRAC7’s boot block, and either the value True or the value False, depending on whether the code in the boot block was signed with the public key. (The boot block is a small amount of persistent memory that contains the initial portion of iDRAC7’s boot code).

Because of the way in which the HRK is calculated, a high degree of assurance is provided that the HRK for a particular iDRAC7 will take on a different value if code not signed by Dell is executed on that iDRAC7’s CPU than if the code is signed by Dell.

Therefore, data encrypted by the HRK when the iDRAC7 is running Dell signed firmware, won’t be decrypt-able by the HRK of firmware supplied by an attacker. It also means that if the flash storage chip iDRAC7 uses to store data were accessed directly (for example, by soldering wires to it), sensitive data is encrypted and therefore not accessible.

Hidden Root Key: uniquely identifying a particular server

Because the HRK is unique to every iDRAC it provides a means to uniquely identify an iDRAC in a cryptographically robust manner.

Uniquely identifying a server is important in a number of scenarios. Some scenarios are addressed by Dell PowerEdge 12th generation server features, while other scenarios will be addressed in future iDRAC versions. A few scenarios where strong server identification is important:

- In organizations where the threat of rogue servers is a possibility
- As a basis for building a chain of trust for:
    - Validating that hardware components of a system are authentic
    - Confirming that the firmware and firmware configuration of the various devices on the system is unchanged and is authentic
    - Clearing all aspects of customer data and customer-supplied configurations when a system is repurposed or decommissioned
- Combining servers in clusters or groups with high assurance against rogue or spoofed servers

Summary: best features of the TPM

The HRK allows the iDRAC7 to implement a number of features normally associated with the TPM, but does so in a way that doesn’t add additional cost to the system, while preserving all of the capabilities of the TPM for use by the customer.

Credential vault

Without too much trouble it is possible to find businesses that will de-solder industry standard flash memory devices from printed circuit boards and provide a copy of the contents of the device. IDRAC7 deals with this threat in a cost-effective and well accepted way. As the name suggests, the Credential Vault is a new feature in iDRAC7 to encrypt sensitive data before it is put into the iDRAC7 flash memory. Private keys are a good example of the kind of sensitive data that the Credential Vault holds and will expand to hold in future versions.

Protected storage

The cryptographic community uses the term "Protected Storage" to mean a storage facility that resists unauthorized attempts to read data contained within. A few well known examples of Protected Storage facilities are: smart cards, the "PStore" facility in Microsoft® Windows® 2003 and Windows XP, the BitLocker® facility in more recent Windows versions, and the TPM v1.2.

iDRAC7 uses the HRK mentioned previously, to encrypt sensitive information that iDRAC7 stores, such as the private keys associated with a user-generated SSL certificate. (iDRAC7, as well as previous iDRAC generations, supports generating Certificate Signing Requests (CSRs) that can be given to a certificate authority (CA). For a nominal fee a CA will generate an SSL certificate using the CSR. The resulting SSL certificate can then be uploaded to iDRAC7.)

Someone trying to steal a credential from iDRAC7, by either de-soldering the flash memory chip or by installing a rogue firmware on iDRAC7 (assuming the attacker figures out a way to get around the firmware verification feature in iDRAC7), would be thwarted trying to read the credentials, because they are encrypted.

Field Service Debug authorization facility

As with many devices that incorporate embedded firmware, iDRAC7 has a number of built-in debugging features. Generally, these debug capabilities are only turned on and used during product development. On rare occasions, it may be necessary to debug iDRAC7 once it is out of the development environment. The typical alternatives of:

- Not allowing substantive debugging after the product has shipped, or
- Having a mechanism where the manufacturer can access the debug features via an undocumented mechanism

are both problematic. iDRAC7 solves these problems by implementing a mechanism in which both the customer and Dell explicitly authorize debugging on a *particular* iDRAC7 and explicitly authorize debugging starting and ending at specific times.

Benefits

This innovation gives the customer control over their system. It protects the customer from having a back door into their system, which anyone with the right knowledge could exploit. By design, Field Service Debugging requires that each iDRAC7 is separately authorized. Consequently, if the token that enables debug on a particular system were stolen, other iDRAC7s are not vulnerable. Further, tokens expire so a stolen or lost token only remains a threat until its expiration date. (Additionally, placing a token on an iDRAC7 requires the "diagnose" privilege.)

This feature preserves the ability to thoroughly debug iDRAC7 in the field if necessary, helping to speed problem resolution and helping Dell to continuously improve our products.

Decommissioning and reprovisioning support

In the previous generation of Dell PowerEdge servers, iDRAC6 supported erasing all data stored since the iDRAC was deployed. This feature is typically used when a server is decommissioned or repurposed. iDRAC7 extends this feature by also wiping the non-volatile memory in which the server BIOS stores data.

The result is that customers can sell, reuse, or throw away their servers knowing that data stored by the BIOS and by iDRAC7 have been erased and can't be mined by anyone who later gains possession of the server.

Summary

The Dell product security philosophy is to design and engineer for security while maintaining a balance with usability and value. We believe that a process of continuous security improvements best serves our customers' needs. We delivered upon this philosophy in the Dell PowerEdge 12th generation of servers.