20171019_Secure Boot feature Study and practice

2017年10月19日 10:52

What's UEFI secure boot?

A UEFI firmware feature, which can secure the boot process by preventing the loading of drivers or OS loaders that are not <u>signed</u> with an acceptable <u>digital signature</u>.

Secure boot is supported by <u>Windows 8</u> and 8.1, <u>Windows Server 2012</u>, and 2012 R2, and Windows 10, VMware vSphere 6.5 and a number of <u>Linux distributions</u> including <u>Fedora</u> (since version 18), <u>openSUSE</u> (since version 12.3), RHEL (since RHEL 7), CentOS (since CentOS 7) and <u>Ubuntu</u> (since version 12.04.2).As of January 2017, <u>FreeBSD</u> support is in a planning stage.

What secure boot looks like if enabled?

Invalid signature detected. Check Se Boot Policy in Setup	ecure
--	-------

How to disable secure boot in BIOS?

Trusted Platform Hodula (TPH)	(Enabled)
Basuro Beet Centrol	-
Dostali Default Bacure Boot Keys	
Delete All Becure Boot Koya Exit Betup	
Version 2.15.1236. Copyright (C) 2013 A	Wwwricen Hegetrends, Inc.

UEFI Secure Boot on Dell C6320 (in BIOS setup)

• if Boot Mode = BIOS, then Secure Boot feature is not available (become grey)

System Setup	Help About Exit	System Setup	٢	lelp About Exit
System BIOS	System B	NOS		
System BIOS Settings Boot Settings	System Bl	OS Settings • System Security		
Boot Mode	AC Power User Defin UEFI Varial SECURE BO NOTE: Secur Secure Boo Secure Boo	ton	Enabled Olisabled Last On Off mmediate Random Oliser Defined Standard Ocontrolled	
Select this menu to configure the Boot Sequence and enable or disable individual boot options.	to and	ystem password is the password that must be ente operating system. (Press <f1> for more help)</f1>	red to allow the system to boot	
PowerEdge Co320 Service Tag : 27LJBD2	Back PowerEdge Service Tag			Back

• if Boot Mode = UEFI, then Secure Boot feature is able to be configured.

System Setup Help About Exit	System Setup Help About Exit
System BIOS	System BIOS
System BIOS Settings • Boot Settings	System BIOS Settings • System Security
Boot Mode O BIOS UEF Boot Sequence Retry Enabled O Disabled Hard-Disk Failover O Enabled Disabled BIOS Boot Settings O Enabled Disabled NOTE: A new boot mode is selected. Boot option settings for the selected boot mode will be available after the boot mode is saved and the system is reset.	Intel(R) TXT
This field determines the boot mode of the system. (Press <f i=""> for more help) PowerEdge C6320 Service Tag : 27LJBD2 Back</f>	Allows selecting the Secure Boot Policy. (Press <-> for more help) PowerEdge C6320 Service Tag: 27LUED2 Back
System Setup About Exit	
System BIOS	
System BIOS Settings • System Security • Secure Boot Policy Summary	
Platform Key (PK) x.509 Certificate Type X.509 Certificate Issuer Dell Inc. Issuing CA 1 Subject Dell UEFI PK PowerEdge Signature Owner GUD A65F1588-A90B-4C2E-9633-A4DA468C66E7 Key Exchange Key (KEK) Database Entries	
Type X.509 Certificate Issuer Microsoft Corporation Third Party Marketplace Root Subject Microsoft Corporation KEK CA 2011 Signature Owner GUD 77FA9ABD-0359-4D32-BD60-28F4E78F784B Authorized Signature Database (db) Entries -	
PowerEdge C6320 Service Tag : 27LJBD2 Back	

UEFI Secure Boot In-Depth

UEFI Secure Boot

Secure boot is designed to protect a system against malicious code being loaded and executed early in the boot process, before the operating system has been loaded. This is to prevent malicious software from installing a "bootkit" and maintaining control over a computer to mask its presence. If an invalid binary is loaded while secure boot is enabled, the user is alerted, and the system will refuse to boot the tampered binary.

On each boot-up, the UEFI firmware inspects each EFI binary that is loaded and ensures that it has either a valid signature (backed by a locally trusted certificate) or that the binary's checksum is present on an allowed list. It also verifies that the signature or checksum does not appear in the deny list. Lists of trusted certificates or checksums are stored as EFI variables within the non-volatile memory used by the UEFI firmware environment to store settings and configuration data.

UEFI Key Overview

The four main EFI variables used for secure boot are shown in Figure a. The Platform Key (often abbreviated to PK) offers full control of the secure boot key hierarchy. The holder of the PK can install a new PK and update the KEK (Key Exchange Key). This is a second key, which either can sign executable EFI binaries directly or be used to sign the db and dbx databases. The db (signature database) variable contains a list of allowed signing certificates or the cryptographic hashes of allowed binaries. The dbx is the inverse of db, and it is used as a blacklist of specific certificates or hashes, which otherwise would have been accepted, but which should not be able to run. Only the KEK and db (shown in green) keys can sign binaries that may boot the system.

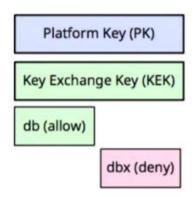


Figure a. Secure Boot Keys

From <<u>http://www.linuxjournal.com/content/take-control-your-pc-uefi-secure-boot?page=0,0</u>>

Reference

- Take Control of Your PC with UEFI Secure Boot
- How to Boot and Install Linux on a UEFI PC With Secure Boot
- <u>RAC-4902</u> UEFI Secure Boot Redfish API As a RackHD user, I want to be able to manage UEFI Secure Boot functionality on a dell node using the Redfish API.

. Develop Redfish APIs for: Add secure boot resource to a node. Enable or disable secure boot on a node. Get current secure boot state.

https://github.com/RackHD/on-http/pull/648