(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105160258 A
(43)申请公布日 2015.12.16

(21)申请号 201510604438.5

(22)申请日 2015.09.21

(71)申请人 无锡中太服务器有限公司
地址 518057 广东省深圳市高新区北区清华信息港A座302号

(72)发明人 王雪松

(74)专利代理机构 深圳市科进知识产权代理事务所（普通合伙） 44316
代理人 宋鹰武

(51)Int.Cl.
G06F 21/57(2013.01)

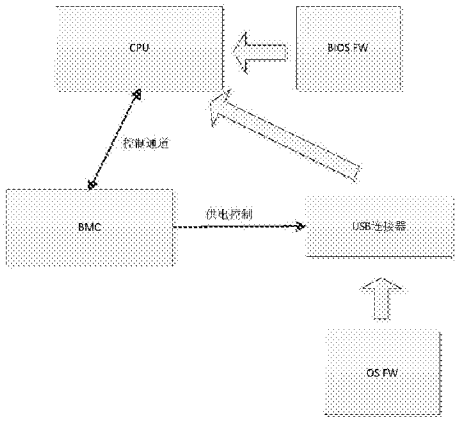
权利要求书1页 说明书2页 附图1页

(54)发明名称

一种防止用户非法修改OS的方法

(57)摘要

本发明公开了一种防止用户非法修改OS的方法，包括下述步骤：(1)当BIOS启动完毕后，CPU向BMC发出请求给连接OS FW的USB连接器供电的指令；(2)BMC接收所述指令并给连接OS FW的USB连接器供电；(3)CPU读取OS FW在内存中解压，并启动解压后的OS，同时CPU向BMC发出终止给连接OS FW的USB连接器供电的指令；(4)BMC收到该指令后终止给所述USB连接器供电。本发明通过在服务器的BIOS中内置OS，使得用户只能使用内置的OS，不能使用其他的OS，从而防止用户非法修改OS；有效的阻止了非授权操作对OS FW的访问和篡改。



CN 105160258 A

1.一种防止用户非法修改OS的方法,其特征在于,包括下述步骤:

(1)当BIOS启动完毕后,CPU向BMC发出请求给连接OS FW的USB连接器供电的指令;

(2)BMC接收所述指令并给连接OS FW的USB连接器供电;

(3)CPU读取OS FW在内存中解压,并启动解压后的OS,同时CPU向BMC发出终止给连接OS FW的USB连接器供电的指令;

(4)BMC收到该指令后终止给所述USB连接器供电。

2.如权利要求1所述的方法,其特征在于,所述CPU与OS FW之间的数据通道不限于USB链路,也可以是其他快速链路。

3.如权利要求1所述的方法,其特征在于,通过将OS FW挂载在USB连接器下,并在不使用时进行下电,从而阻止了非授权操作对OS FW的访问和篡改。

一种防止用户非法修改 OS 的方法

技术领域

[0001] 本发明属于服务器产品技术领域，更具体地，涉及一种防止用户非法修改 OS 的方法。

背景技术

[0002] 现有技术的做法是 BIOS(Basic Input Output System，基本输入输出系统）中并不内置 OS(Operating System，操作系统），BIOS FW(Firmware，固件）存放在 Flash 中，OS FW 存放在外部存储设备（如硬盘、U 盘等）中，BIOS 启动完毕后扫描外部存储设备，列举所有已安装的 OS 供用户选择，然后启动用户选定的 OS 或者在等待超时后启动默认的 OS。

[0003] 现有技术的缺点是 OS 存放在外部存储设备中，用户可以任意安装、修改。现有技术无法满足云服务器厂商等的需求，后者希望可以在服务器中部署安全可靠的 OS，且该 OS 不会被非法修改。

发明内容

[0004] 针对现有技术的缺陷，本发明的目的在于提供一种防止用户非法修改 OS 的方法，旨在解决现有技术中由于将 OS 存放在外部存储设备中导致用户可以任意安装或修改的技术问题。

[0005] 本发明提供了一种防止用户非法修改 OS 的方法，包括下述步骤：

[0006] (1) 当 BIOS 启动完毕后，CPU 向 BMC 发出请求给连接 OS FW 的 USB 连接器供电的指令；

[0007] (2)BMC 接收所述指令并给连接 OS FW 的 USB 连接器供电；

[0008] (3)CPU 读取 OS FW 在内存中解压，并启动解压后的 OS，同时 CPU 向 BMC 发出终止给连接 OS FW 的 USB 连接器供电的指令；

[0009] (4)BMC 收到该指令后终止给所述 USB 连接器供电。

[0010] 更进一步地，所述 CPU 与 OS FW 之间的数据通道不限于 USB 链路，也可以是其他快速链路。

[0011] 更进一步地，通过将 OS FW 挂载在 USB 连接器下，并在不使用时进行下电，从而阻止了非授权操作对 OS FW 的访问和篡改。

[0012] 本发明通过在服务器的 BIOS 中内置 OS，使得用户只能使用内置的 OS，不能使用其他的 OS，从而防止用户非法修改 OS；有效的阻止了非授权操作对 OS FW 的访问和篡改。

附图说明

[0013] 图 1 是本发明实施例提供的防止用户非法修改 OS 的方法所基于的系统原理框图。

具体实施方式

[0014] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对

本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0015] 本发明提供的一种防止用户非法修改 OS 的方法主要应用领域为服务器产品；具体地，通过在服务器的 BIOS 中内置 OS，使得用户只能使用内置的 OS，不能使用其他的 OS，从而防止用户非法修改 OS。

[0016] BIOS FW 一般存储在 SPI Flash 中，这个 Flash 的大小一般是有限制的，如不能超过 256M。而 OS FW 一般比较大，比如可能达到 1-2G。因此 BIOS FW 和 OS FW 需要分开存储。为了防止 OS FW 被非法的替换或修改，需要将 OS FW 存储在一个比较隐蔽的位置，以保证既可以被 BIOS 访问到，又很难被非授权的操作访问到。为了做到这一点，OS FW 存储在 USB 连接器下挂的 USB 存储设备中（即 OS FW 与 USB 连接器连接），而该 USB 连接器挂在 CPU 下（即 USB 连接器与 CPU 连接）。

[0017] 如图 1 所示，当 BIOS 启动完毕后，CPU 向 BMC 发出请求给连接 OS FW 的 USB 连接器供电的指令；BMC 收到该指令后给连接 OS FW 的 USB 连接器供电；CPU 读取 OS FW 在内存中（内存就是 CPU 使用的内存，相对而言，USB 存储设备是外存）解压并启动解压后的 OS（计算机系统要工作必须有 OS，一般的系统 OS 都放在外存上，这里是将压缩打包后的 OS 作为一个文件放在外存，使用时解压到内存），同时 CPU 向 BMC 发出终止给连接 OS FW 的 USB 连接器供电的指令，BMC 收到该指令后终止给所述 USB 连接器供电。

[0018] BMC 与 OS FW 之间的数据通道不限于 USB 链路，也可以是其他快速链路。

[0019] 通过将 OS FW 挂载在 USB 连接器下，并在不使用时进行下电，有效的阻止了非授权操作对 OS FW 的访问和篡改。

[0020] 在本发明实施例中，BIOS 只能启动其内置的 OS，不能启动其他外部存储设备上的 OS。存放 OS FW 的存储设备在不使用时进行下电。

[0021] 本发明将 OS 内置到 BIOS 中，从而防止用户任意安装、修改 OS，满足云服务器厂商等部署安全可靠且不会被非法修改的 OS 的需求。

[0022] 本领域的技术人员容易理解，以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

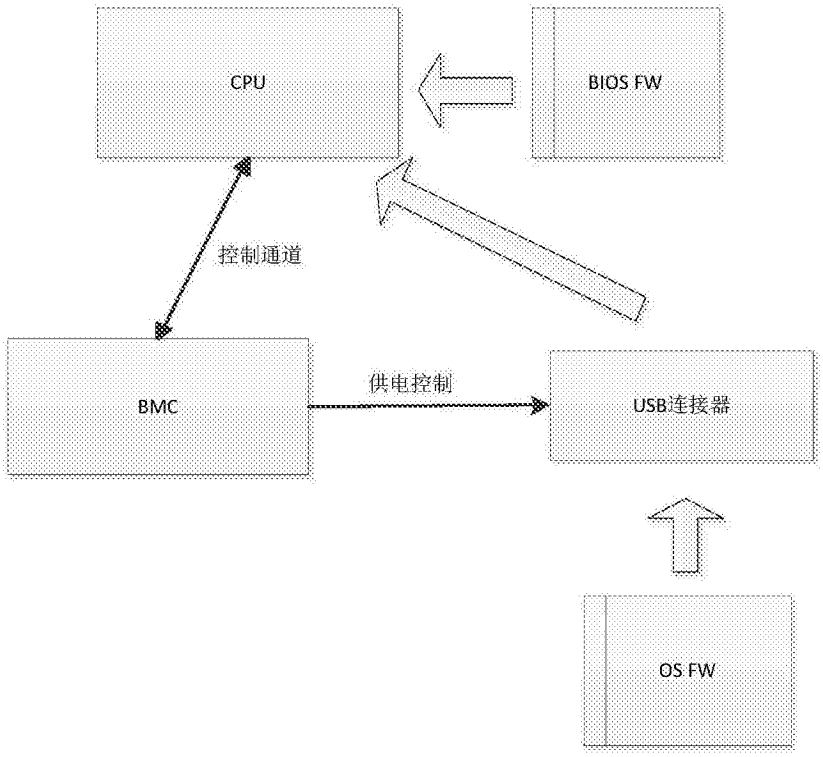


图 1