(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 108959973 A
(43)申请公布日 2018.12.07

(21)申请号 201810681480.0

(22)申请日 2018.06.27

(71)申请人 郑州云海信息技术有限公司
地址 450018 河南省郑州市郑东新区心怡路278号16层1601室

(72)发明人 曾科

(74)专利代理机构 济南诚智商标专利事务所有限公司 37105
代理人 李修杰

(51)Int.Cl.
G06F 21/71(2013.01)
G06F 21/75(2013.01)
G06F 8/65(2018.01)
G06F 8/61(2018.01)

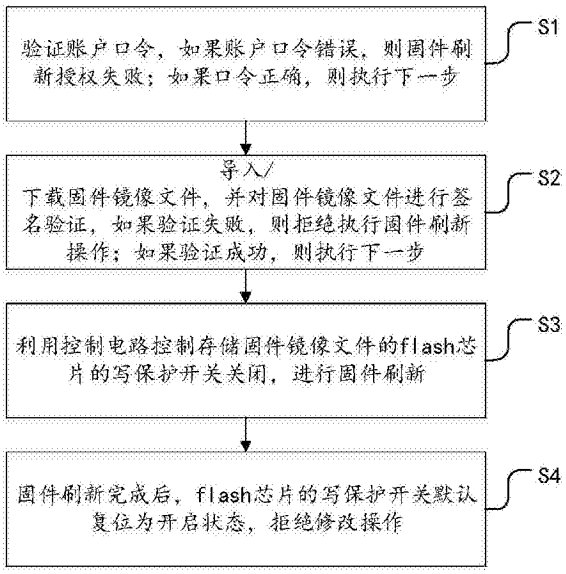
权利要求书1页 说明书4页 附图1页

(54)发明名称

一种针对BMC固件刷新的保护方法与系统

(57)摘要

本发明提供了一种针对BMC固件刷新的保护方法与系统，包括以下步骤：S1、验证账户口令，如果账户口令错误，则固件刷新授权失败；如果口令正确，则执行下一步；S2、导入/下载固件镜像文件，并对固件镜像文件进行签名验证，如果验证失败，则拒绝执行固件刷新操作；如果验证成功，则执行下一步；S3、利用控制电路控制存储固件镜像文件的flash芯片的写保护开关关闭，进行固件刷新；S4、固件刷新完成后，flash芯片的写保护开关默认复位为开启状态，拒绝修改操作。本发明解决了现有技术BMC固件刷新保护机制不能全面防护威胁攻击的问题，实现固件从刷新到运行全方位的保护，极大的防范了服务器管理软件BMC固件面临的风险。



CN 108959973 A

1.一种针对BMC固件刷新的保护方法,其特征在于,包括以下步骤:

S1、验证账户口令,如果账户口令错误,则固件刷新授权失败;如果口令正确,则执行下一步;

S2、导入/下载固件镜像文件,并对固件镜像文件进行签名验证,如果验证失败,则拒绝执行固件刷新操作;如果验证成功,则执行下一步;

S3、利用控制电路控制存储固件镜像文件的flash芯片的写保护开关关闭,进行固件刷新;

S4、固件刷新完成后,flash芯片的写保护开关默认复位为开启状态,拒绝修改操作。

2.根据权利要求1所述的一种针对BMC固件刷新的保护方法,其特征在于,所述对固件镜像文件进行签名验证具体操作为:

在BMC主板嵌入BMC固件数字签名的公钥;

利用公钥对固件镜像文件进行签名验证。

3.根据权利要求1所述的一种针对BMC固件刷新的保护方法,其特征在于,所述利用控制电路控制存储固件镜像文件的flash芯片的写保护开关关闭具体操作为:

将控制电路的引脚与存储固件镜像文件的flash芯片写保护引脚连接;

获得执行权限;

控制flash芯片的写保护开关设置为关。

4.根据权利要求1-3任意一项所述的一种针对BMC固件刷新的保护方法,其特征在于,所述账户为具备BMC固件刷新权限的管理员账户。

5.一种针对BMC固件刷新的保护系统,其特征在于,所述系统包括:

账户口令验证模块,用于验证账户口令;

固件签名验证模块,用于导入/下载固件镜像文件,并对固件镜像文件进行签名验证;

固件刷新模块,用于利用控制电路控制存储固件镜像文件的flash芯片的写保护开关关闭,进行固件刷新;

写保护模块,用于固件刷新完成后,flash芯片的写保护开关默认复位为开启状态,拒绝修改操作。

6.根据权利要求5所述的一种针对BMC固件刷新的保护系统,其特征在于,所述固件签名验证模块包括:

公钥嵌入单元,用于获取嵌入在主板的BMC固件数字签名的公钥;

验证单元,用于利用公钥对固件镜像文件进行签名验证。

7.根据权利要求5所述的一种针对BMC固件刷新的保护系统,其特征在于,所述固件刷新模块包括:

引脚连接单元,用于将控制电路的引脚与存储固件镜像文件的flash芯片写保护引脚连接;

权限获取单元,用于获得执行权限;

写保护关闭单元,用于控制flash芯片的写保护开关设置为关;

刷新单元,用于进行固件刷新。

8.根据权利要求5-7任意一项所述的一种针对BMC固件刷新的保护系统,其特征在于,所述账户为具备BMC固件刷新权限的管理员账户。

一种针对BMC固件刷新的保护方法与系统

技术领域

[0001] 本发明涉及固件刷新保护技术领域，特别是一种针对BMC固件刷新的保护方法与系统。

背景技术

[0002] BMC(Baseboard Management Controller,基板管理控制器)是一个独立于系统的管理软件，基于行业标准的IPMI规范，用于对服务器远程管理、固件升级、系统监控等一些操作。

[0003] 随着BMC技术在服务器行业的地位越来越高，针对服务器BMC系统的攻击层出不穷，有针对刷新控制的网络层攻击；有针对BMC固件存储区域的攻击；也有针对BMC固件更新镜像文件的攻击，一旦BMC遭受上述威胁攻击时，会造成服务器管理系统的崩溃，或导致服务器管理系统被攻击者控制，对服务器进行恶意操作控制。因此，安全的BMC固件刷新机制必须能够防范上述的恶意攻击，防止攻击者随意进行BMC固件刷新操作；防止攻击者对BMC固件存储区域的修改；防止攻击者使用嵌入恶意代码的BMC固件进行刷新。

[0004] 目前已经有一些对BMC固件刷新进行保护的机制，如生产厂家在固件出厂前对固件镜像文件进行数字签名，刷新时进行签名验证，保证固件镜像文件的完整性与合法性；或者将固件存储在具备写保护技术的flash芯片上；但是这些保护机制不能全方面的防护上述威胁攻击，更不能防止攻击者对BMC进行滥刷操作。

发明内容

[0005] 本发明的目的是提供一种针对BMC固件刷新的保护方法与系统，旨在解决现有技术BMC固件刷新保护机制不能全面防护威胁攻击的问题，实现固件刷新到运行进行全方位保护，防范BMC固件面临的风险。

[0006] 为达到上述技术目的，本发明提供了一种针对BMC固件刷新的保护方法，包括以下步骤：

[0007] S1、验证账户口令，如果账户口令错误，则固件刷新授权失败；如果口令正确，则执行下一步；

[0008] S2、导入/下载固件镜像文件，并对固件镜像文件进行签名验证，如果验证失败，则拒绝执行固件刷新操作；如果验证成功，则执行下一步；

[0009] S3、利用控制电路控制存储固件镜像文件的flash芯片的写保护开关关闭，进行固件刷新；

[0010] S4、固件刷新完成后，flash芯片的写保护开关默认复位为开启状态，拒绝修改操作。

[0011] 优选地，所述对固件镜像文件进行签名验证具体操作为：

[0012] 在BMC主板嵌入BMC固件数字签名的公钥；

[0013] 利用公钥对固件镜像文件进行签名验证。

[0014] 优选地，所述利用控制电路控制存储固件镜像文件的flash芯片的写保护开关关闭具体操作为：

[0015] 将控制电路的引脚与存储固件镜像文件的flash芯片写保护引脚连接；

[0016] 获得执行权限；

[0017] 控制flash芯片的写保护开关设置为关。

[0018] 优选地，所述账户为具备BMC固件刷新权限的管理员账户。

[0019] 本发明还提供了一种针对BMC固件刷新的保护系统，所述系统包括：

[0020] 账户口令验证模块，用于验证账户口令；

[0021] 固件签名验证模块，用于导入/下载固件镜像文件，并对固件镜像文件进行签名验证；

[0022] 固件刷新模块，用于利用控制电路控制存储固件镜像文件的flash芯片的写保护开关关闭，进行固件刷新；

[0023] 写保护模块，用于固件刷新完成后，flash芯片的写保护开关默认复位为开启状态，拒绝修改操作。

[0024] 优选地，所述固件签名验证模块包括：

[0025] 公钥嵌入单元，用于获取嵌入在主板的BMC固件数字签名的公钥；

[0026] 验证单元，用于利用公钥对固件镜像文件进行签名验证。

[0027] 优选地，所述固件刷新模块包括：

[0028] 引脚连接单元，用于将控制电路的引脚与存储固件镜像文件的flash芯片写保护引脚连接；

[0029] 权限获取单元，用于获得执行权限；

[0030] 写保护关闭单元，用于控制flash芯片的写保护开关设置为关；

[0031] 刷新单元，用于进行固件刷新。

[0032] 优选地，所述账户为具备BMC固件刷新权限的管理员账户。

[0033] 发明内容中提供的效果仅仅是实施例的效果，而不是发明所有的全部效果，上述技术方案中的一个技术方案具有如下优点或有益效果：

[0034] 与现有技术相比，本发明通过验证账户口令、对固件镜像文件进行签名验证以及控制存储固件镜像文件的存储芯片写保护开关的关闭，来实现固件刷新过程中防止攻击者通过网络仿冒合法账户进行滥刷操作以及BMC固件文件在运行过程中不被恶意修改，将用户最小权限技术、数字签名技术和flash芯片写保护技术结合起来，运用到BMC固件刷新过程中，实现固件从刷新端到运行端的三重保护。解决了现有技术BMC固件刷新保护机制不能全面防护威胁攻击的问题，实现固件从刷新到运行全方位的保护，极大的防范了服务器管理软件BMC固件面临的风险。

附图说明

[0035] 图1为本发明实施例中所提供的一种针对BMC固件刷新的保护方法流程图；

[0036] 图2为本发明实施例中所提供的一种针对BMC固件刷新的保护系统结构框图。

具体实施方式

[0037] 为了能清楚说明本方案的技术特点，下面通过具体实施方式，并结合其附图，对本发明进行详细阐述。下文的公开提供了许多不同的实施例或例子用来实现本发明的不同结构。为了简化本发明的公开，下文中对特定例子的部件和设置进行描述。此外，本发明可以在不同例子中重复参考数字和/或字母。这种重复是为了简化和清楚的目的，其本身不指示所讨论各种实施例和/或设置之间的关系。应当注意，在附图中所图示的部件不一定按比例绘制。本发明省略了对公知组件和处理技术及工艺的描述以避免不必要地限制本发明。

[0038] 下面结合附图对本发明实施例所提供的一种针对BMC固件刷新的保护方法与系统进行详细说明。

[0039] 如图1所示，本发明实施例公开了一种针对BMC固件刷新的保护方法，包括以下步骤：

[0040] S1、验证账户口令，如果账户口令错误，则固件刷新授权失败；如果口令正确，则执行下一步；

[0041] S2、导入/下载固件镜像文件，并对固件镜像文件进行签名验证，如果验证失败，则拒绝执行固件刷新操作；如果验证成功，则执行下一步；

[0042] S3、利用控制电路控制存储固件镜像文件的flash芯片的写保护开关关闭，进行固件刷新；

[0043] S4、固件刷新完成后，flash芯片的写保护开关默认复位为开启状态，拒绝修改操作。

[0044] 由于固件刷新操作中，只有具备BMC固件刷新权限的管理员账户才能发起固件刷新请求，普通用户无法进行该操作，在确认进行BMC固件刷新之前，需要对账户口令进行验证，只有当账户口令验证通过后，BMC固件刷新才可获得合法授权。如果账户口令错误，则BMC固件刷新授权失败，系统将会拒绝执行固件刷新；如果口令正确，则执行下一步。

[0045] 上述操作是针对BMC固件刷新的第一重保护机制。通过上述保护机制，可以有效防止攻击者通过网络仿冒合法账户进行滥刷操作。

[0046] 导入/下载镜像文件。BMC主板在出厂前便嵌入了BMC固件数字签名的公钥，固件镜像文件导入/下载后，系统将用嵌入的公钥对固件镜像文件进行签名验证操作，判断固件镜像文件的完整性与合法性。如果签名验证失败，系统将会拒绝执行固件刷新操作，如果签名验证成功，则将执行操作移交给控制电路。

[0047] 上述操作是针对BMC固件刷新的第二重保护机制。通过上述保护机制，保证了固件镜像文件的完整性与合法性。

[0048] 将BMC固件镜像文件存储在flash芯片中，将所述控制电路的引脚与存储BMC固件文件的flash芯片写保护引脚相连，控制电路获得执行权限后，便控制flash芯片的写保护开关设置为关，以便修改BMC固件文件。当存储BMC固件文件的flash芯片写保护开关关闭后，BMC固件开始进行刷新操作，当成功完成固件刷新后，flash芯片的写保护开关默认复位为开启状态，并拒绝一切的修改操作。

[0049] 上述操作时针对BMC固件刷新的第三重保护机制。通过上述保护机制，可以保证BMC固件文件在运行过程中不被恶意修改。

[0050] 本发明实施例通过验证账户口令、对固件镜像文件进行签名验证以及控制存储固件镜像文件的存储芯片写保护开关的关闭，来实现固件刷新过程中防止攻击者通过网络仿

冒合法账户进行滥刷操作以及BMC固件文件在运行过程中不被恶意修改，将用户最小权限技术、数字签名技术和flash芯片写保护技术结合起来，运用到BMC固件刷新过程中，实现固件从刷新端到运行端的三重保护。解决了现有技术BMC固件刷新保护机制不能全面防护威胁攻击的问题，实现固件从刷新到运行全方位的保护，极大的防范了服务器管理软件BMC固件面临的风险。

[0051] 如图2所示，本发明实施例还公开了一种针对BMC固件刷新的保护系统，所述系统包括：

[0052] 账户口令验证模块，用于验证账户口令；

[0053] 固件签名验证模块，用于导入/下载固件镜像文件，并对固件镜像文件进行签名验证；

[0054] 固件刷新模块，用于利用控制电路控制存储固件镜像文件的flash芯片的写保护开关关闭，进行固件刷新；

[0055] 写保护模块，用于固件刷新完成后，flash芯片的写保护开关默认复位为开启状态，拒绝修改操作。

[0056] 所述账户为具备BMC固件刷新权限的管理员账户，普通用户无法进行该操作，在确认进行BMC固件刷新之前，需要对账户口令进行验证，只有当账户口令验证通过后，BMC固件刷新才可获得合法授权。

[0057] 所述固件签名验证模块包括：

[0058] 公钥嵌入单元，用于获取嵌入在主板的BMC固件数字签名的公钥；

[0059] 验证单元，用于利用公钥对固件镜像文件进行签名验证。

[0060] BMC主板在出厂前便嵌入了BMC固件数字签名的公钥，固件镜像文件导入/下载后，系统将用嵌入的公钥对固件镜像文件进行签名验证操作，判断固件镜像文件的完整性与合法性。

[0061] 所述固件刷新模块包括：

[0062] 引脚连接单元，用于将控制电路的引脚与存储固件镜像文件的flash芯片写保护引脚连接；

[0063] 权限获取单元，用于获得执行权限；

[0064] 写保护关闭单元，用于控制flash芯片的写保护开关设置为关；

[0065] 刷新单元，用于进行固件刷新。

[0066] 将BMC固件镜像文件存储在flash芯片中，将所述控制电路的引脚与存储BMC固件文件的flash芯片写保护引脚相连，控制电路获得执行权限后，便控制flash芯片的写保护开关设置为关，以便修改BMC固件文件。当存储BMC固件文件的flash芯片写保护开关关闭后，BMC固件开始进行刷新操作，当成功完成固件刷新后，flash芯片的写保护开关默认复位为开启状态，并拒绝一切的修改操作。

[0067] 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。

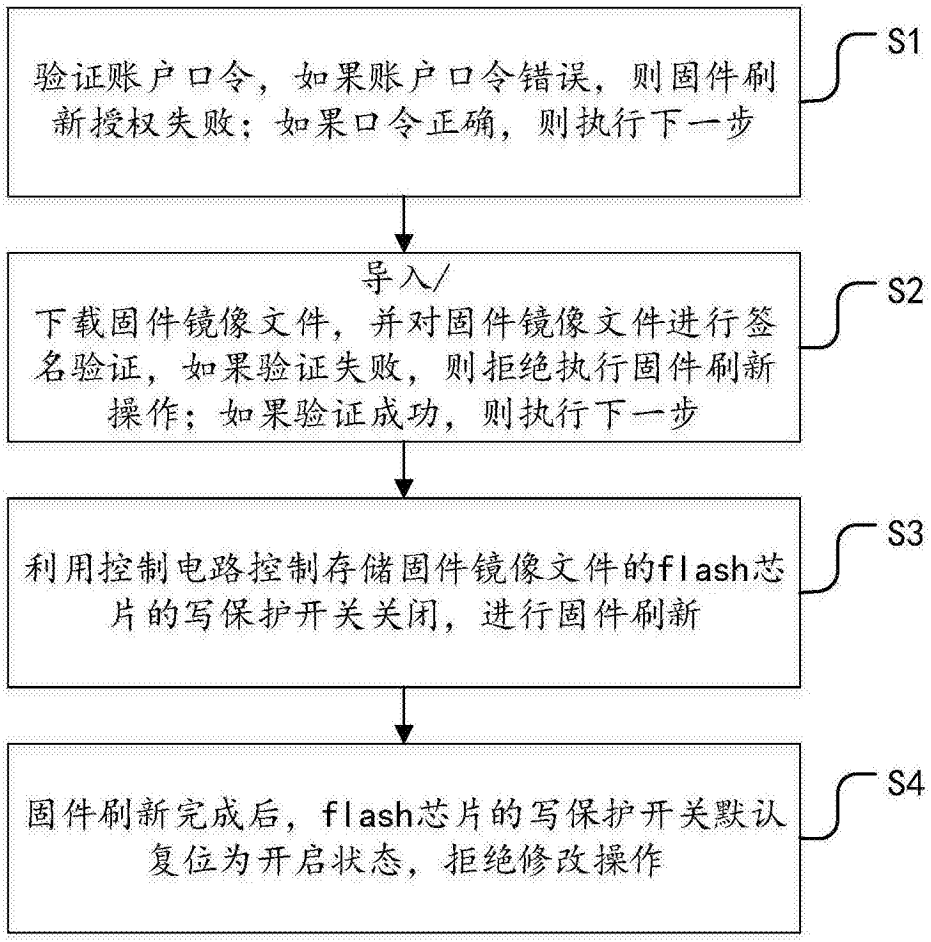

验证账户口令，如果账户口令错误，则固件刷新授权失败；如果口令正确，则执行下一步
S1
导入/
下载固件镜像文件，并对固件镜像文件进行签名验证，如果验证失败，则拒绝执行固件刷新操作；如果验证成功，则执行下一步
S2
利用控制电路控制存储固件镜像文件的flash芯片的写保护开关关闭，进行固件刷新
S3
固件刷新完成后，flash芯片的写保护开关默认复位为开启状态，拒绝修改操作
S4

图1

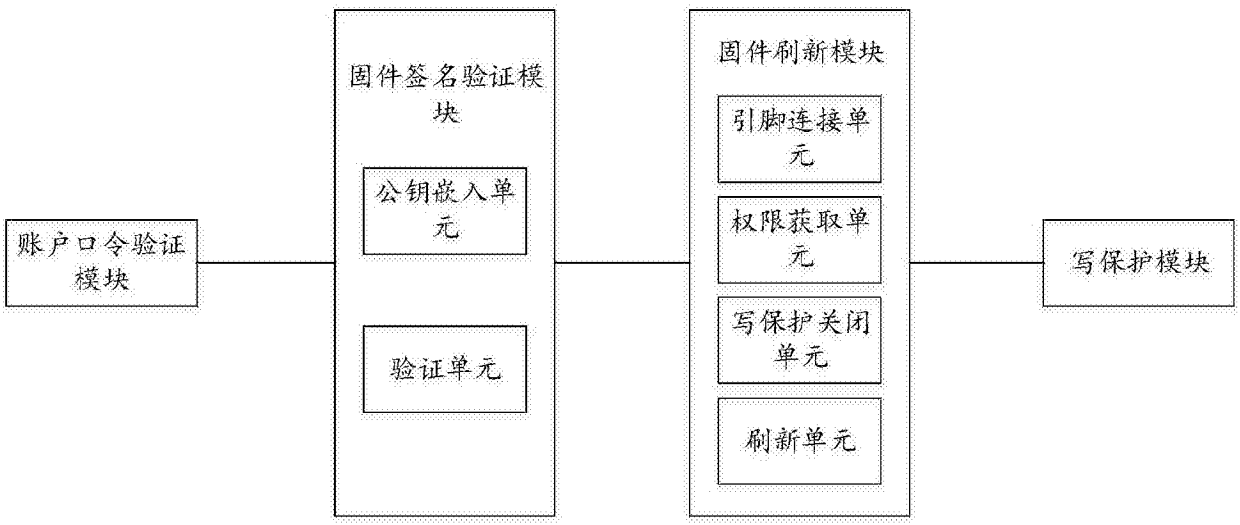

账户口令验证模块
固件签名验证模块
公钥嵌入单元
验证单元
固件刷新模块
引脚连接单元
权限获取单元
写保护关闭单元
刷新单元
写保护模块

图2