(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 105975842 A
(43)申请公布日 2016.09.28

(21)申请号 201610306991.5

(22)申请日 2016.05.11

(71)申请人 浪潮集团有限公司
地址 250101 山东省济南市高新区舜雅路1036号

(72)发明人 于晓艳 于治楼 梁智豪

(74)专利代理机构 济南信达专利事务所有限公司 37100
代理人 姜明

(51)Int.Cl.
G06F 21/34(2013.01)
G06F 21/44(2013.01)

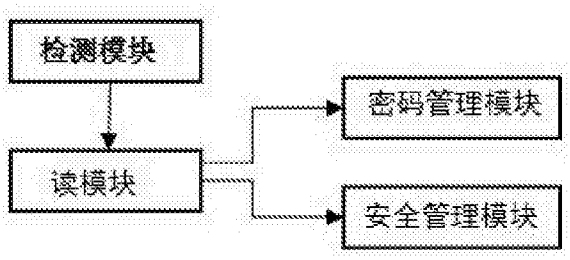
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种UEFI中基于KEY的BIOS安全认证方法及系统

(57)摘要

本发明公开一种UEFI中基于KEY的BIOS安全认证方法及系统，属于BIOS管理技术领域；利用UEFI，在UEFI的DXE阶段后之后，BDS之前，通过接口检测连接到电脑的KEY设备，并将KEY初始化为启动设备，根据读请求读取KEY中相关信息，并将相关信息存储到UEFI中，进行初始化密码信息加密解密设置，利用读取的KEY中相关信息设置KEY初始化密码，同时生成随机数验证密码，均存储到UEFI中；比较验证从KEY中读取的初始化密码与UEFI中的相应存储的密码信息，如果相等则进行下个阶段操作，直至启动系统，如果不等则继续请求等待，防止系统启动。



CN 105975842 A

1.一种UEFI中基于KEY的BIOS安全认证方法，其特征是利用UEFI，在UEFI的DXE阶段后之后，BDS之前，通过接口检测连接到电脑的KEY设备，并将KEY初始化为启动设备，根据读请求读取KEY中相关信息，并将相关信息存储到UEFI中，进行初始化密码信息加密解密设置，利用读取的KEY中相关信息设置KEY初始化密码，同时生成随机数验证密码，均存储到UEFI中；比较验证从KEY中读取的初始化密码与UEFI中的相应存储的密码信息，如果相等则进行下个阶段操作，直至启动系统，如果不等则继续请求等待，防止系统启动。

2.根据权利要求1所述的方法，其特征是所述初始化密码信息加密解密设置：利用读取的KEY中相关信息设置KEY初始化密码为密码1，同时生成随机数验证密码为密码2，将密码2加密为密码3，密码3解密为密码4，分别存储到KEY和UEFI中。

3.根据权利要求2所述的方法，其特征是比较验证从KEY中读取的密码1与UEFI中的相应存储的密码1信息是否相等，不相等则验证不通过，继续发送请求读取KEY内的密码1，如果相等则验证通过，继续通过读模块读取KEY内密码3。

4.根据权利要求3所述的方法，其特征是读取KEY内密码3与UEFI中存储的密码4验证比较，如果相等则加载后续操作系统，运行BDS、TSL、RT阶段，系统启动，如果不等则验证未通过，继续发送请求读取KEY内的密码1，系统不能启动。

5.一种UEFI中基于KEY的BIOS安全认证系统，其特征是包括检测模块、读模块、安全管理模块、密码管理模块，均内嵌于UEFI固件中，且在UEFI的DXE阶段后之后，BDS之前执行各自功能，

检测模块负责通过接口检测连接到电脑的KEY设备，并将KEY初始化为启动设备，

读模块与检测模块通信，根据读请求读取KEY中相关信息，并将相关信息存储到UEFI中，

安全管理模块与读模块通信，利用读取的KEY中相关信息设置KEY初始化密码，同时生成随机数验证密码，比较验证从KEY中读取的初始化密码与UEFI中的相应密码信息，如果相等则进行下个阶段操作，直至启动系统，如果不等则继续请求等待，防止系统启动。

6.密码管理模块与读模块通信，负责配合安全管理模块进行初始化密码信息加密解密设置。

一种UEFI中基于KEY的BIOS安全认证方法及系统

技术领域

[0001] 本发明公开一种UEFI中BIOS安全认证方法及系统，属于BIOS管理技术领域，具体地说是一种UEFI中基于KEY的BIOS安全认证方法及系统。

背景技术

[0002] 随着计算机的使用越来越普遍，人们对计算机的安全性要求也不断提高。传统的方法是设置BIOS密码，开机之后输入密码验证进入系统，这种方法的单个密码极易受到攻击，不能满足人们更高安全性要求。改进的方法利用USB KEY除包括基本的flash存储模块，也包含密码芯片作为安全管理模块，包含可启动操作系统，保护计算机系统安全，但是需要提前安装USBKEY 的设备驱动，时常造成使用的不便。本发明公开了一种UEFI中基于KEY的BIOS安全认证方法及系统，利用UEFI的启动过程，将硬件加密认证过程设置在UEFI启动过程中DXE阶段之后，BDS阶段之前执行。利用UEFI，在UEFI的DXE阶段后之后，BDS之前，通过接口检测连接到电脑的KEY设备，并将KEY初始化为启动设备，根据读请求读取KEY中相关信息，并将相关信息存储到UEFI中，进行初始化密码信息加密解密设置，利用读取的KEY中相关信息设置KEY初始化密码，同时生成随机数验证密码，均存储到UEFI中；比较验证从KEY中读取的初始化密码与UEFI中的相应存储的密码信息，如果相等则进行下个阶段操作，直至启动系统，如果不等则继续请求等待，防止系统启动。

[0003] UEFI的启动包括SEC、PEI、DXE、BDS、TSL、RT几个阶段，其中SEC即security设置CPU的保护模式，PEI即EFI前初始化PEI，DXE即执行驱动、安装Device handle、安装protocol，BDS 即开机设备选择，TSL即暂时性系统载入，RT即运行时间等几个阶段。在不同的阶段增加密码验证，使安全保护程度不同。

发明内容

[0004] 本发明针对现有技术的问题，提供一种UEFI中基于KEY的BIOS安全认证方法及系统，通过初始化KEY和UEFI 固件，用硬件加密认证来达到保护计算机系统安全的目的。

[0005] 本发明提出的具体方案是：

一种UEFI中基于KEY的BIOS安全认证方法，利用UEFI，在UEFI的DXE阶段后之后，BDS之前，通过接口检测连接到电脑的KEY设备，并将KEY初始化为启动设备，根据读请求读取KEY中相关信息，并将相关信息存储到UEFI中，进行初始化密码信息加密解密设置，利用读取的KEY中相关信息设置KEY初始化密码，同时生成随机数验证密码，均存储到UEFI中；比较验证从KEY中读取的初始化密码与UEFI中的相应存储的密码信息，如果相等则进行下个阶段操作，直至启动系统，如果不等则继续请求等待，防止系统启动。

[0006] 所述初始化密码信息加密解密设置：利用读取的KEY中相关信息设置KEY初始化密码为密码1，同时生成随机数验证密码为密码2，将密码2加密为密码3，密码3解密为密码4，分别存储到KEY和UEFI中。

[0007] 比较验证从KEY中读取的密码1与UEFI中的相应存储的密码1信息是否相等，不相

等则验证不通过，继续发送请求读取KEY内的密码1，如果相等则验证通过，继续通过读模块读取KEY内密码3。

[0008] 读取KEY内密码3与UEFI中存储的密码4验证比较，如果相等则加载后续操作系统，运行BDS、TSL、RT阶段，系统启动，如果不等则验证未通过，继续发送请求读取KEY内的密码1，系统不能启动。

[0009] 一种UEFI中基于KEY的BIOS安全认证系统，包括检测模块、读模块、安全管理模块、密码管理模块，均内嵌于UEFI固件中，且在UEFI的DXE阶段后之后，BDS之前执行各自功能，

检测模块负责通过接口检测连接到电脑的KEY设备，并将KEY初始化为启动设备，

读模块与检测模块通信，根据读请求读取KEY中相关信息，并将相关信息存储到UEFI中，

安全管理模块与读模块通信，利用读取的KEY中相关信息设置KEY初始化密码，同时生成随机数验证密码，比较验证从KEY中读取的初始化密码与UEFI中的相应密码信息，如果相等则进行下个阶段操作，直至启动系统，如果不等则继续请求等待，防止系统启动。

[0010] 密码管理模块与读模块通信，负责配合安全管理模块进行初始化密码信息加密解密设置。

[0011] 本发明的有益之处是：

本发明提供一种UEFI中基于KEY的BIOS安全认证方法及系统，利用UEFI，在UEFI的DXE阶段后之后，BDS之前，通过接口检测连接到电脑的KEY设备，并将KEY初始化为启动设备，根据读请求读取KEY中相关信息，并将相关信息存储到UEFI中，进行初始化密码信息加密解密设置，利用读取的KEY中相关信息设置KEY初始化密码，同时生成随机数验证密码，均存储到UEFI中；比较验证从KEY中读取的初始化密码与UEFI中的相应存储的密码信息，如果相等则进行下个阶段操作，直至启动系统，如果不等则继续请求等待，防止系统启动；利用本发明方法及系统通过初始化KEY和UEFI 固件，用硬件加密认证来达到保护计算机系统安全的目的。

附图说明

[0012] 图1是本发明系统框架示意图；

图2是本发明方法流程示意图。

具体实施方式

[0013] 一种UEFI中基于KEY的BIOS安全认证方法，利用UEFI，在UEFI的DXE阶段后之后，BDS之前，通过接口检测连接到电脑的KEY设备，并将KEY初始化为启动设备，根据读请求读取KEY中相关信息，并将相关信息存储到UEFI中，进行初始化密码信息加密解密设置，利用读取的KEY中相关信息设置KEY初始化密码，同时生成随机数验证密码，均存储到UEFI中；比较验证从KEY中读取的初始化密码与UEFI中的相应存储的密码信息，如果相等则进行下个阶段操作，直至启动系统，如果不等则继续请求等待，防止系统启动。

[0014] 相应的系统包括检测模块、读模块、安全管理模块、密码管理模块，均内嵌于UEFI固件中，且在UEFI的DXE阶段后之后，BDS之前执行各自功能，

检测模块负责通过接口检测连接到电脑的KEY设备，并将KEY初始化为启动设备，

读模块与检测模块通信，根据读请求读取KEY中相关信息，并将相关信息存储到UEFI中，

安全管理模块与读模块通信，利用读取的KEY中相关信息设置KEY初始化密码，同时生成随机数验证密码，比较验证从KEY中读取的初始化密码与UEFI中的相应密码信息，如果相等则进行下个阶段操作，直至启动系统，如果不等则继续请求等待，防止系统启动。

[0015] 密码管理模块与读模块通信，负责配合安全管理模块进行初始化密码信息加密解密设置。

[0016] 利用上述方法及系统，结合附图对本发明做进一步说明。

[0017] 具体实施时，检测模块检测到通过接口连接到电脑的KEY设备，检测到KEY，并将KEY初始化为启动设备，进行初始化密码信息加密解密设置，利用读取的KEY中相关信息设置KEY初始化密码为密码1，同时生成随机数验证密码为密码2，将密码2加密为密码3，密码3解密为密码4，分别存储到KEY和UEFI中；

重新启动计算机，检测到KEY之后，当UEFI执行完SEC、PEI、DXE阶段之后对KEY发送请求，读取模块读取KEY的密码信息；

比较验证从KEY中读取的密码1与UEFI中的相应存储的密码1信息是否相等，不相等则验证不通过，继续发送请求读取KEY内的密码1，如果相等则验证通过，继续通过读模块读取KEY内密码3；

读取KEY内密码3与UEFI中存储的密码4验证比较，如果相等则加载后续操作系统，运行BDS、TSL、RT阶段，系统启动，如果不等则验证未通过，继续发送请求读取KEY内的密码1，系统不能启动，重复进行验证过程。直至验证成功或手动进行处理。利用本发明方法及系统通过初始化KEY和UEFI 固件，用硬件加密认证来达到保护计算机系统安全的目的。

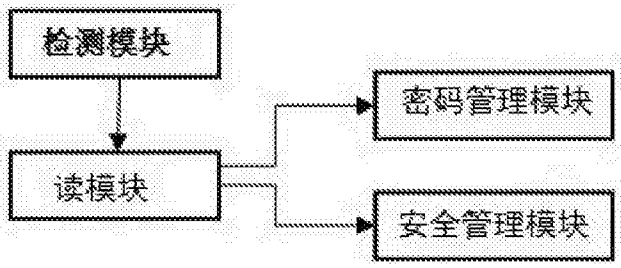

检测模块
读模块
密码管理模块
安全管理模块

图1

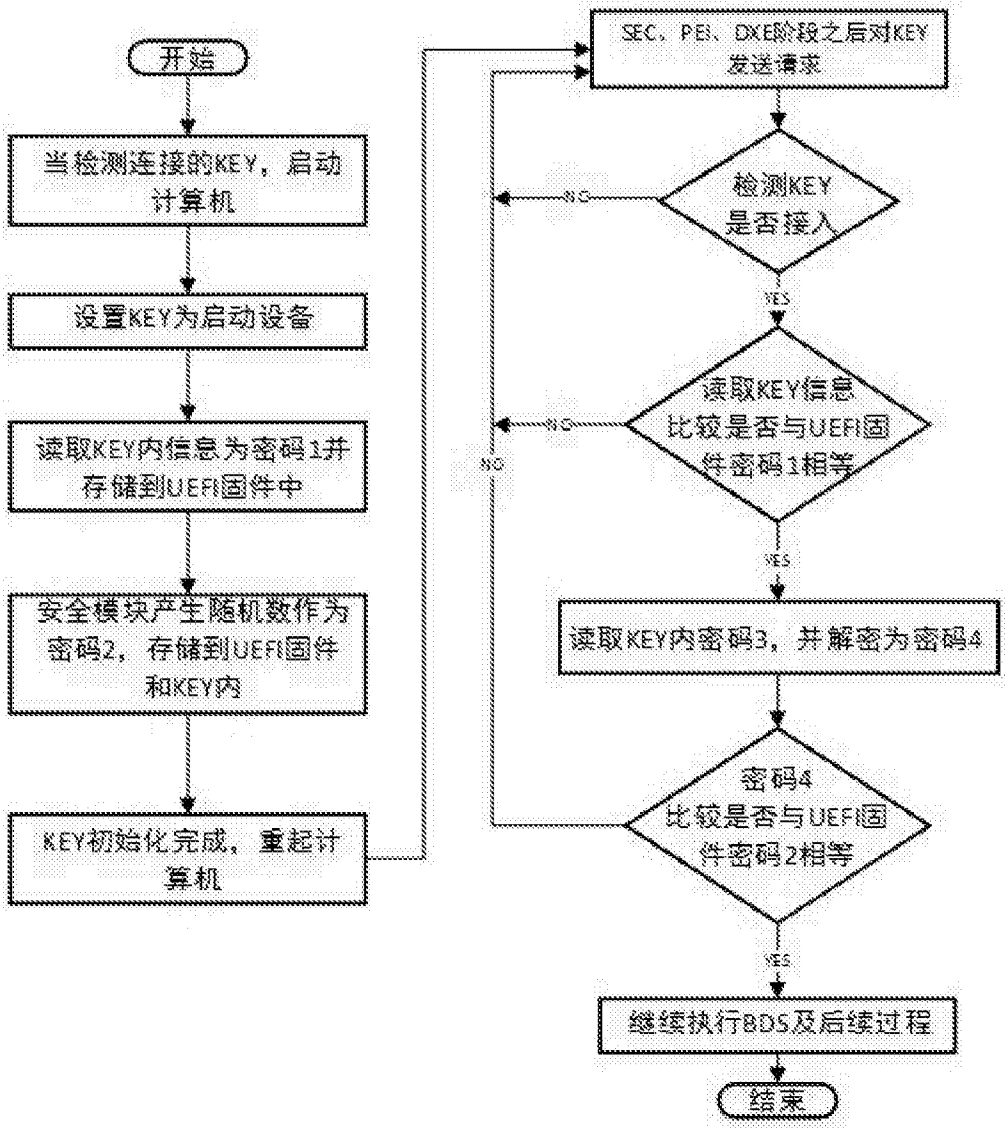

开始
当检测连接的KEY，启动计算机
设置KEY为启动设备
读取KEY内信息为密码1并存储到UEFI固件中
安全模块产生随机数作为密码2，存储到UEFI固件和KEY内
KEY初始化完成，重起计算机
SEC、PEI、DXE阶段之后对KEY发送请求
检测KEY是否接入
NO
YES
读取KEY信息比较是否与UEFI固件密码1相等
NO
NO
YES
读取KEY内密码3，并解密为密码4
密码4比较是否与UEFI固件密码2相等
YES
继续执行BDS及后续过程
结束

图2