(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 106295352 A
(43)申请公布日 2017.01.04

(21)申请号 201610620808.9

(22)申请日 2016.07.29

(71)申请人 北京三未信安科技发展有限公司
地址 100101 北京市朝阳区北苑路170号3号楼22层1单元2602

(72)发明人 张玉国 桑洪波

(74)专利代理机构 北京轻创知识产权代理有限公司 11212
代理人 杨立

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

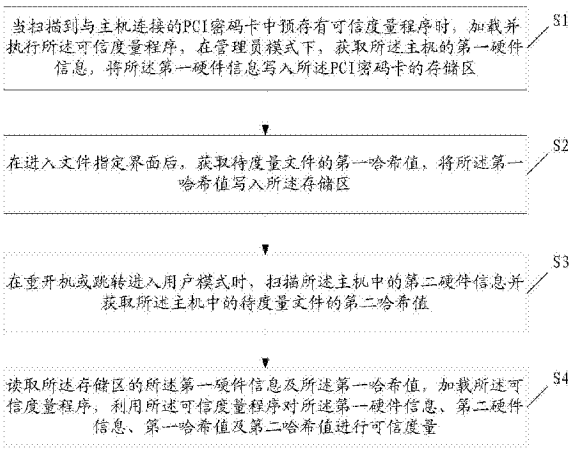
权利要求书2页 说明书8页 附图2页

(54)发明名称

基本输入输出系统环境下可信度量的方法、主机及系统

(57)摘要

本发明涉及一种基本输入输出系统环境下可信度量的方法、主机及系统，应用于主机中，该方法包括：当扫描到与主机连接的PCI密码卡中预存有可信度量程序时，加载并执行所述可信度量程序，在管理员模式下，获取所述主机的第一硬件信息，将所述第一硬件信息写入所述PCI密码卡的存储区；在进入文件指定界面后，获取待度量文件的第一哈希值，将第一哈希值写入存储区；在重开机或跳转进入用户模式时，扫描主机中的第二硬件信息并获取主机中的待度量文件的第二哈希值；读取存储区的第一硬件信息及第一哈希值，加载可信度量程序，利用可信度量程序对第一硬件信息、第二硬件信息、第一哈希值及第二哈希值进行可信度量。本发明实现对主机启动过程的静态可信度量，提高了系统信息的安全性。



CN 106295352 A

1.一种基本输入输出系统环境下可信度量的方法，应用于主机中，其特征在于，包括：

当扫描到与主机连接的PCI密码卡中预存有可信度量程序时，加载并执行所述可信度量程序，在管理员模式下，获取所述主机的第一硬件信息，将所述第一硬件信息写入所述PCI密码卡的存储区；

在进入文件指定界面后，获取待度量文件的第一哈希值，将所述第一哈希值写入所述存储区；

在重开机或跳转进入用户模式时，扫描所述主机中的第二硬件信息并获取所述主机中的待度量文件的第二哈希值；

读取所述存储区的所述第一硬件信息及所述第一哈希值，加载所述可信度量程序，利用所述可信度量程序对所述第一硬件信息、第二硬件信息、第一哈希值及第二哈希值进行可信度量。

2.根据权利要求1所述一种基本输入输出系统环境下可信度量的方法，其特征在于，还包括：

在可信度量通过时，获取控制权并完成操作系统的装载，以进入所述操作系统；

在可信度量未通过时，返回所述管理员模式以再次执行可信度量。

3.根据权利要求2所述一种基本输入输出系统环境下可信度量的方法，其特征在于，还包括：

在所述管理员模式下，修改管理员口令。

4.根据权利要求3所述一种基本输入输出系统环境下可信度量的方法，其特征在于，所述在可信度量未通过时，返回所述管理员模式以再次执行可信度量的步骤包括：

在可信度量未通过，返回所述管理员模式之前，输入修改后的所述管理员口令，根据所述管理员口令返回所述管理员模式以再次执行可信度量。

5.根据权利要求1至4任一项所述一种基本输入输出系统环境下可信度量的方法，其特征在于，所述在进入文件指定界面后，获取待度量文件的第一哈希值，将所述第一哈希值写入所述存储区的步骤包括：

在进入文件指定界面后，设置文件路径，根据所述文件路径获取待度量文件；

获取所述待度量文件的二进制数据，对所述二进制数据进行哈希运算，得到所述第一哈希值，将所述第一哈希值写入所述存储区。

6.一种主机，其特征在于，所述主机包括：

第一写入模块，用于当扫描到与主机连接的PCI密码卡中预存有可信度量程序时，加载并执行所述可信度量程序，在管理员模式下，获取所述主机的第一硬件信息，将所述第一硬件信息写入所述PCI密码卡的存储区；

第二写入模块，用于在进入文件指定界面后，获取待度量文件的第一哈希值，将所述第一哈希值写入所述存储区；

扫描模块，用于在重开机或跳转进入用户模式时，扫描所述主机中的第二硬件信息并获取所述主机中的待度量文件的第二哈希值；

可信度量模块，用于读取所述存储区的所述第一硬件信息及所述第一哈希值，加载所述可信度量程序，利用所述可信度量程序对所述第一硬件信息、第二硬件信息、第一哈希值及第二哈希值进行可信度量。

7.根据权利要求6所述一种主机，其特征在于，所述主机还包括：

装载模块，用于在可信度量通过时，获取控制权并完成操作系统的装载，以进入所述操作系统；

返回模块，用于在可信度量未通过时，返回所述管理员模式以再次执行可信度量。

8.根据权利要求7所述一种主机，其特征在于，所述主机还包括：

修改模块，用于在所述管理员模式下，修改管理员口令。

9.根据权利要求8所述一种主机，其特征在于，所述返回模块具体用于在可信度量未通过，返回所述管理员模式之前，输入修改后的所述管理员口令，根据所述管理员口令返回所述管理员模式以再次执行可信度量。

10.根据权利要求6至9任一项所述一种主机，其特征在于，所述第二写入模块具体用于在进入文件指定界面后，设置文件路径，根据所述文件路径获取待度量文件；获取所述待度量文件的二进制数据，对所述二进制数据进行哈希运算，得到所述第一哈希值，将所述第一哈希值写入所述存储区。

11.一种系统，包括PCI密码卡及权利要求6-10任一项所述的主机，所述PCI密码卡用于预存可信度量程序；在与所述主机连接后并在所述主机处于管理员模式下，接收所述主机发送的第一硬件信息及待度量文件的第一哈希值并存储；在所述主机进入用户模式时，发送所述第一硬件信息及所述第一哈希值至所述主机，供所述主机在加载所述预存可信度量程序后进行可信度量。

基本输入输出系统环境下可信度量的方法、主机及系统

技术领域

[0001] 本发明涉及信息安全技术领域，尤其涉及一种基本输入输出系统环境下可信度量的方法、主机及系统。

背景技术

[0002] 基于密码学的信息安全技术已得到广泛的应用，如公钥基础设施(Public Key Infrastructure，PKI)，公钥基础设施是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。以PKI技术为基础的PCI密码卡，其可以用在需要密码卡运算和密钥管理等安全功能的、具有标准PCI/PCI Express接口的通信设备、计算机设备或安全保密设备上，安全性要求较高。在PCI密码卡插入主机后，只能在主机操作系统运行起来并加载驱动后才能实现信息安全的检测，而主机启动过程中加载的数据有可能是被篡改的，是不可信的，这给PCI密码卡的后续应用造成安全隐患。

发明内容

[0003] 本发明所要解决的技术问题是提供一种基本输入输出系统环境下可信度量的方法、主机及系统。

[0004] 本发明解决上述技术问题的技术方案如下：一种基本输入输出系统环境下可信度量的方法，应用于主机中，包括：

[0005] 当扫描到与主机连接的PCI密码卡中预存有可信度量程序时，加载并执行所述可信度量程序，在管理员模式下，获取所述主机的第一硬件信息，将所述第一硬件信息写入所述PCI密码卡的存储区；

[0006] 在进入文件指定界面后，获取待度量文件的第一哈希值，将所述第一哈希值写入所述存储区；

[0007] 在重开机或跳转进入用户模式时，扫描所述主机中的第二硬件信息并获取所述主机中的待度量文件的第二哈希值；

[0008] 读取所述存储区的所述第一硬件信息及所述第一哈希值，加载所述可信度量程序，利用所述可信度量程序对所述第一硬件信息、第二硬件信息、第一哈希值及第二哈希值进行可信度量。

[0009] 本发明的有益效果是：在启动过程中的BIOS环境下，在管理员模式时将主机的第一硬件信息及待度量文件的第一哈希值存入PCI密码卡，在用户模式下时调用PCI密码卡中预存有可信度量程序，通过可信度量程序对第一硬件信息、第二硬件信息、第一哈希值及第二哈希值进行可信度量，从而实现对主机启动过程的静态可信度量，使得主机启动过程加载的数据是可信的，未被篡改的，为后续PCI密码卡的使用提供安全保障，提高了系统信息的安全性。

[0010] 在上述技术方案的基础上，本发明还可以做如下改进。

[0011] 进一步，还包括：

[0012] 在可信度量通过时，获取控制权并完成操作系统的装载，以进入所述操作系统；

[0013] 在可信度量未通过时，返回所述管理员模式以再次执行可信度量。

[0014] 采用上述进一步方案的有益效果是：在可信度量通过时方进入操作系统，使得主机启动过程加载的数据是可信的，而在可信度量未通过时不可进入操作系统，提高了系统信息的安全性。

[0015] 进一步，还包括：

[0016] 在所述管理员模式下，修改管理员口令。

[0017] 采用上述进一步方案的有益效果是：进一步提高了系统信息的安全性。

[0018] 进一步，所述在可信度量未通过时，返回所述管理员模式以再次执行可信度量的步骤包括：

[0019] 在可信度量未通过，返回所述管理员模式之前，输入修改后的所述管理员口令，根据所述管理员口令返回所述管理员模式以再次执行可信度量。

[0020] 采用上述进一步方案的有益效果是：通过输入修改后的管理员口令返回管理员模式，使得他人不能随意进入管理员模式来修改相关信息，进一步提高了系统信息的安全性。

[0021] 进一步，所述在进入文件指定界面后，获取待度量文件的第一哈希值，将所述第一哈希值写入所述存储区的步骤包括：

[0022] 在进入文件指定界面后，设置文件路径，根据所述文件路径获取待度量文件；

[0023] 获取所述待度量文件的二进制数据，对所述二进制数据进行哈希运算，得到所述第一哈希值，将所述第一哈希值写入所述存储区。

[0024] 采用上述进一步方案的有益效果是：通过将待度量文件的二进制数据计算得到哈希值，便于后续的可信度量。

[0025] 本发明解决上述技术问题的技术方案还如下：一种主机，所述主机包括：

[0026] 第一写入模块，用于当扫描到与主机连接的PCI密码卡中预存有可信度量程序时，加载并执行所述可信度量程序，在管理员模式下，获取所述主机的第一硬件信息，将所述第一硬件信息写入所述PCI密码卡的存储区；

[0027] 第二写入模块，用于在进入文件指定界面后，获取待度量文件的第一哈希值，将所述第一哈希值写入所述存储区；

[0028] 扫描模块，用于在重开机或跳转进入用户模式时，扫描所述主机中的第二硬件信息并获取所述主机中的待度量文件的第二哈希值；

[0029] 可信度量模块，用于读取所述存储区的所述第一硬件信息及所述第一哈希值，加载所述可信度量程序，利用所述可信度量程序对所述第一硬件信息、第二硬件信息、第一哈希值及第二哈希值进行可信度量。

[0030] 进一步，所述主机还包括：

[0031] 装载模块，用于在可信度量通过时，获取控制权并完成操作系统的装载，以进入所述操作系统；

[0032] 返回模块，用于在可信度量未通过时，返回所述管理员模式以再次执行可信度量。

[0033] 进一步，所述主机还包括：

[0034] 修改模块，用于在所述管理员模式下，修改管理员口令。

[0035] 进一步，所述返回模块具体用于在可信度量未通过，返回所述管理员模式之前，输

入修改后的所述管理员口令，根据所述管理员口令返回所述管理员模式以再次执行可信度量。

[0036] 进一步，所述第二写入模块具体用于在进入文件指定界面后，设置文件路径，根据所述文件路径获取待度量文件；获取所述待度量文件的二进制数据，对所述二进制数据进行哈希运算，得到所述第一哈希值，将所述第一哈希值写入所述存储区。

[0037] 本发明解决上述技术问题的技术方案还如下：一种系统，包括PCI密码卡及上述的主机，所述PCI密码卡用于预存可信度量程序；在与所述主机连接后并在所述主机处于管理员模式下，接收所述主机发送的第一硬件信息及待度量文件的第一哈希值并存储；在所述主机进入用户模式时，发送所述第一硬件信息及所述第一哈希值至所述主机，供所述主机在加载所述预存可信度量程序后进行可信度量。

附图说明

[0038] 图1为本发明基本输入输出系统环境下可信度量的方法一实施例的流程示意图；

[0039] 图2为图1所示的详细流程示意图；

[0040] 图3为本发明主机的结构示意图。

具体实施方式

[0041] 以下结合附图对本发明的原理和特征进行描述，所举实例只用于解释本发明，并非用于限定本发明的范围。

[0042] 如图1所示，图1为本发明基本输入输出系统环境下可信度量的方法一实施例的流程示意图，应用于主机中，该方法包括：

[0043] S1，当扫描到与主机连接的PCI密码卡中预存有可信度量程序时，加载并执行所述可信度量程序，在管理员模式下，获取所述主机的第一硬件信息，将所述第一硬件信息写入所述PCI密码卡的存储区；

[0044] 本实施例中，主机在开机启动时处于基本输入输出系统(Basic Input Output System，BIOS)环境下，BIOS是一组固化到主机内主板上一个ROM芯片上的程序，它保存着主机最重要的基本输入输出的程序、开机后自检程序和系统自启动程序，其主要功能是为主机提供最底层的、最直接的硬件设置和控制。

[0045] PCI密码卡第一次插在主机上时，在管理员模式下，需要将主机上的与可信度量相关的信息存储到PCI密码卡中，以便后续进行可信度量。本实施例为静态可信度量。

[0046] 本实施例主机在BIOS环境下调用PCI密码卡，相比于主机进入操作系统后存在一定难度，因为进入操作系统后有很多封装好的函数可以调用，因此在可信度量程序中含有小型的文件系统代码。本实施例通过相关的设置，可在利用BIOS的相关功能枚举设备并分配硬件资源后，查询作为扩展设备的PCI密码卡是否存在扩展ROM，如果PCI密码卡存在扩展ROM，查询相应的寄存器的标志位，例如如果标志位为“1”，则PCI密码上存在扩展ROM，扩展ROM中可以存储有可信度量程序或代码，然后扫描获取主机的第一硬件信息，利用BIOS的相关功能将第一硬件信息通过PCI/PCI Express接口写入PCI密码卡的存储区，以作为后续进行可信度量之用。BIOS将主动将扩展ROM中的程序及代码加载到内存执行。

[0047] 其中，该PCI密码卡的扩展ROM及存储区为预先建立的，存储区中可以存储可信度

量的相关信息。第一硬件信息例如可以是主机的硬盘、光驱、扩展设备等的硬件配置信息。

[0048] S2,在进入文件指定界面后,获取待度量文件的第一哈希值,将所述第一哈希值写入所述存储区;

[0049] 在BIOS环境下无文件系统解析代码,因此,需要在可信度量程序加入简单的文件系统程序,便于文件的指定与查找,本实施例通过将待度量文件计算得到哈希值,便于后续的可信度量。

[0050] 本实施例中,在管理员模式下进入文件指定界面,该文件指定界面用于供用户指定相关的待度量文件,这些待度量文件为与信息安全相关的重要文件,例如为内核的相关文件。在用户指定待度量文件后,采用哈希算法对待度量文件进行计算,得到待度量文件的第一哈希值。然后,同样利用BIOS的相关功能将第一哈希值通过PCI/PCI Express接口写入PCI密码卡的存储区,以作为后续进行可信度量之用。

[0051] 至此,在管理员模式下的相关操作或配置完成,退出管理员模式。

[0052] S3,在重开机或跳转进入用户模式时,扫描所述主机中的第二硬件信息并获取所述主机中的待度量文件的第二哈希值;

[0053] 本实施例中,在主机重开机或跳转时进入用户模式,用户模式也处于BIOS环境下,在进入用户模式后主机执行可信度量。

[0054] 在进入用户模式后,主机重新扫描第二硬件信息,第二硬件信息与上述第一硬件信息的主体对应,即对应地为主机的硬盘、光驱、扩展设备等的硬件配置信息,但第二硬件信息相对于第一硬件信息可能已经由于被篡改或其他操作发生了变化。

[0055] 另外,主机重新获取待度量文件,并计算待度量文件的第二哈希值。第二哈希值与第一哈希值对应的待度量文件是对应相同的,但第二哈希值相对于第一哈希值可能已经由于被篡改或其他操作发生了变化。

[0056] S4,读取所述存储区的所述第一硬件信息及所述第一哈希值,加载所述可信度量程序,利用所述可信度量程序对所述第一硬件信息、第二硬件信息、第一哈希值及第二哈希值进行可信度量。

[0057] 本实施例中,调用BIOS的相关功能读取PCI密码卡中的存储区中存储的第一硬件信息及第一哈希值,然后主机加载PCI密码卡的扩展ROM中预存有可信度量程序,通过可信度量程序对第一硬件信息、第二硬件信息、第一哈希值及第二哈希值进行可信度量。

[0058] 本实施例中,将第一硬件信息与第二硬件信息进行匹配,且将第一哈希值及第二哈希值进行匹配,如果得到的匹配结果是两者都相同,则可信度量通过,否则,可信度量未通过,值得说明的是,所有的匹配操作是在PCI密码卡上完成,以确保安全性。

[0059] 与现有技术相比,本实施例主机在启动过程中的BIOS环境下,在管理员模式时将主机的第一硬件信息及待度量文件的第一哈希值存入PCI密码卡,在用户模式下时调用PCI密码卡中预存有可信度量程序,通过可信度量程序对第一硬件信息、第二硬件信息、第一哈希值及第二哈希值进行可信度量,从而实现对主机启动过程的静态可信度量,使得主机启动过程加载的数据是可信的,未被篡改的,为后续PCI密码卡的使用提供安全保障,提高了系统信息的安全性;另外,本实施例主机在进入操作系统后,PCI密码卡仍可按照传统的PCI密码卡的操作方式进行操作,兼容性较好。

[0060] 在一优选的实施例中,在上述图1的实施例的基础上,该方法还包括:

[0061] 在可信度量通过时，获取控制权并完成操作系统的装载，以进入所述操作系统；在可信度量未通过时，返回所述管理员模式以再次执行可信度量。

[0062] 本实施例中，在可信度量通过时，主机获取控制权并返回给BIOS，继续完成操作系统的装载，以进入操作系统；在可信度量未通过时，返回管理员模式，重复执行上述图1中的步骤以再次执行系统配置的重新写入，也可理解为初始化。具体地，若当前的主机系统的硬件配置以及指定文件的哈希值与PCI密码卡上存储区的分别对应相同，主机系统可顺利进入操作系统，否则不允许主机进入操作系统。

[0063] 本实施例中，在可信度量通过时方进入操作系统，使得主机启动过程加载的数据是可信的，而在可信度量未通过时不可进入操作系统，提高了系统信息的安全性。

[0064] 在一优选的实施例中，在上述实施例的基础上，该方法还包括：在所述管理员模式下，修改管理员口令。

[0065] 本实施例中，在初次进入管理员模式时，使用的是默认的管理员口令，在初次进入管理员模式时或者在管理员模式的任意时机下，可以修改管理员口令，使得他人不能随意进入管理员模式来修改相关信息，进一步提高了系统信息的安全性。

[0066] 在一优选的实施例中，在上述实施例的基础上，在可信度量未通过，返回所述管理员模式之前，输入修改后的所述管理员口令，根据所述管理员口令返回所述管理员模式以再次执行可信度量。

[0067] 本实施例中，在可信度量未通过，返回所述管理员模式之前，输入经修改后的管理员口令，主机判断该管理员口令是正确的口令后，进入管理员模式以再次执行可信度量，本实施例通过输入修改后的管理员口令返回管理员模式，使得他人不能随意进入管理员模式来修改相关信息，进一步提高了系统信息的安全性。

[0068] 在一优选的实施例中，在上述图1的实施例的基础上，上述步骤S2包括：在进入文件指定界面后，设置文件路径，根据所述文件路径获取待度量文件；获取所述待度量文件的二进制数据，对所述二进制数据进行哈希运算，得到所述第一哈希值，将所述第一哈希值写入所述存储区。

[0069] 本实施例中，在管理员模式下进入文件指定界面后，用户可以指定待度量文件，在文件指定界面中设置待度量文件的文件路径，然后根据文件路径获取待度量文件，将待度量文件的二进制数据进行哈希运算，即将待度量文件的任意长度的二进制值映射为较短的固定长度的二进制值，即得到第一哈希值。

[0070] 本实施例中，在BIOS环境下无文件系统解析代码，因此，无法直接通过路径识别文件，本实施例通过将待度量文件的二进制数据计算得到哈希值，便于后续的可信度量。

[0071] 为了便于理解，图2中给出了本发明的详细流程图，在图2中，包括：

[0072] 步骤S10，在主机启动时，判断预定时间内是否有输入，若是，则进入步骤S20，若否，则进入步骤S60；

[0073] 步骤S20，在管理员登录界面中输入管理员口令；

[0074] 步骤S30，判断管理员口令是否正确，且判断输入管理员口令的次数是否不大于3次，若判断的结果均为是，则进入步骤S40，若管理员口令错误且输入的次数不大于3次时，返回步骤S20，若管理员口令错误且输入的次数大于3次时，进入步骤S70；

[0075] 步骤S40，当扫描到与主机连接的PCI密码卡中预存有可信度量程序时，加载并执

行所述可信度量程序，在管理员模式下，获取所述主机的第一硬件信息，将所述第一硬件信息写入所述PCI密码卡的存储区；在进入文件指定界面后，获取待度量文件的第一哈希值，将所述第一哈希值写入所述存储区；并可修改管理员口令；

[0076] 步骤S50，配置管理完成，主机重启系统或者跳转至用户模式；

[0077] 步骤S60，进入用户模式时，扫描主机中的第二硬件信息Info2并获取主机中的待度量文件的第二哈希值Val2；

[0078] 步骤S70，主机重启系统；

[0079] 步骤S80，读取所述存储区的所述第一硬件信息Info1及所述第一哈希值Val1，加载所述可信度量程序；

[0080] 步骤S90，利用所述可信度量程序对所述第一硬件信息、第二硬件信息、第一哈希值及第二哈希值进行可信度量：判断Info1与Info2是否相同，且判断Val1与Val2是否相同，若判断的结果均为是，则进入步骤S100，否则进入步骤S20；

[0081] 步骤S100，获取控制权并完成操作系统的装载，以进入所述操作系统。

[0082] 如图3所示，图3为本发明主机一实施例的结构示意图，主机包括：

[0083] 第一写入模块，用于当扫描到与主机连接的PCI密码卡中预存有可信度量程序时，加载并执行所述可信度量程序，在管理员模式下，获取所述主机的第一硬件信息，将所述第一硬件信息写入所述PCI密码卡的存储区；

[0084] 本实施例中，主机在开机启动时处于基本输入输出系统(Basic Input Output System，BIOS)环境下，BIOS是一组固化到主机内主板上一个ROM芯片上的程序，它保存着主机最重要的基本输入输出的程序、开机后自检程序和系统自启动程序，其主要功能是为主机提供最底层的、最直接的硬件设置和控制。

[0085] PCI密码卡第一次插在主机上时，在管理员模式下，需要将主机上的与可信度量相关的信息存储到PCI密码卡中，以便后续进行可信度量。本实施例为静态可信度量。

[0086] 本实施例主机在BIOS环境下调用PCI密码卡，相比于主机进入操作系统后存在一定难度，因为进入操作系统后有很多封装好的函数可以调用，因此在可信度量程序中含有小型的文件系统代码。本实施例通过相关的设置，可在利用BIOS的相关功能枚举设备并分配硬件资源后，查询作为扩展设备的PCI密码卡是否存在扩展ROM，如果PCI密码卡存在扩展ROM，查询相应的寄存器的标志位，例如如果标志位为“1”，则PCI密码上存在扩展ROM，扩展ROM中可以存储有可信度量程序或代码，然后扫描获取主机的第一硬件信息，利用BIOS的相关功能将第一硬件信息通过PCI/PCI Express接口写入PCI密码卡的存储区，以作为后续进行可信度量之用。BIOS将主动将扩展ROM中的程序及代码加载到内存执行。

[0087] 其中，该PCI密码卡的扩展ROM及存储区为预先建立的，存储区中可以存储可信度量的相关信息。第一硬件信息例如可以是主机的硬盘、光驱、扩展设备等的硬件配置信息。

[0088] 第二写入模块，用于在进入文件指定界面后，获取待度量文件的第一哈希值，将所述第一哈希值写入所述存储区；

[0089] 在BIOS环境下无文件系统解析代码，因此，需要在可信度量程序加入简单的文件系统程序，便于文件的指定与查找，本实施例通过将待度量文件计算得到哈希值，便于后续的可信度量。

[0090] 本实施例中，在管理员模式下进入文件指定界面，该文件指定界面用于供用户指

定相关的待度量文件，这些待度量文件为与信息安全相关的重要文件，例如为内核的相关文件。在用户指定待度量文件后，采用哈希算法对待度量文件进行计算，得到待度量文件的第一哈希值。然后，同样利用BIOS的相关功能将第一哈希值通过PCI/PCI Express接口写入PCI密码卡的存储区，以作为后续进行可信度量之用。

[0091] 至此，在管理员模式下的相关操作或配置完成，退出管理员模式。

[0092] 扫描模块，用于在重开机或跳转进入用户模式时，扫描所述主机中的第二硬件信息并获取所述主机中的待度量文件的第二哈希值；

[0093] 本实施例中，在主机重开机或跳转时进入用户模式，用户模式也处于BIOS环境下，在进入用户模式后主机执行可信度量。

[0094] 在进入用户模式后，主机重新扫描第二硬件信息，第二硬件信息与上述第一硬件信息的主体对应，即对应地为主机的硬盘、光驱、扩展设备等的硬件配置信息，但第二硬件信息相对于第一硬件信息可能已经由于被篡改或其他操作发生了变化。

[0095] 另外，主机重新获取待度量文件，并计算待度量文件的第二哈希值。第二哈希值与第一哈希值对应的待度量文件是对应相同的，但第二哈希值相对于第一哈希值可能已经由于被篡改或其他操作发生了变化。

[0096] 可信度量模块，用于读取所述存储区的所述第一硬件信息及所述第一哈希值，加载所述可信度量程序，利用所述可信度量程序对所述第一硬件信息、第二硬件信息、第一哈希值及第二哈希值进行可信度量。

[0097] 本实施例中，调用BIOS的相关功能读取PCI密码卡中的存储区中存储的第一硬件信息及第一哈希值，然后主机加载PCI密码卡的扩展ROM中预存有可信度量程序，通过可信度量程序对第一硬件信息、第二硬件信息、第一哈希值及第二哈希值进行可信度量。

[0098] 本实施例中，将第一硬件信息与第二硬件信息进行匹配，且将第一哈希值及第二哈希值进行匹配，如果得到的匹配结果是两者都相同，则可信度量通过，否则，可信度量未通过，值得说明的是，所有的匹配操作是在PCI密码卡上完成，以确保安全性。

[0099] 在一优选的实施例中，在上述图3的实施例的基础上，主机还包括：

[0100] 装载模块，用于在可信度量通过时，获取控制权并完成操作系统的装载，以进入所述操作系统；返回模块，用于在可信度量未通过时，返回所述管理员模式以再次执行可信度量。

[0101] 本实施例中，在可信度量通过时，主机获取控制权并返回给BIOS，继续完成操作系统的装载，以进入操作系统；在可信度量未通过时，返回管理员模式，再次执行可信度量。具体地，若当前的主机系统的硬件配置以及指定文件的哈希值与PCI密码卡上存储区的分别对应相同，主机系统可顺利进入操作系统，否则不允许主机进入操作系统。

[0102] 本实施例中，在可信度量通过时方进入操作系统，使得主机启动过程加载的数据是可信的，而在可信度量未通过时不可进入操作系统，提高了系统信息的安全性。

[0103] 在一优选的实施例中，在上述实施例的基础上，主机还包括：修改模块，用于在所述管理员模式下，修改管理员口令。

[0104] 本实施例中，在初次进入管理员模式时，使用的是默认的管理员口令，在初次进入管理员模式或者在管理员模式的任意时机下时，可以修改管理员口令，使得他人不能随意进入管理员模式来修改相关信息，进一步提高了系统信息的安全性。

[0105] 在一优选的实施例中，在上述实施例的基础上，上述返回模块具体用于在可信度量未通过，返回所述管理员模式之前，输入修改后的所述管理员口令，根据所述管理员口令返回所述管理员模式以再次执行可信度量。

[0106] 本实施例中，在可信度量未通过，返回所述管理员模式之前，输入经修改后的管理员口令，主机判断该管理员口令是正确的口令后，进入管理员模式以再次执行可信度量，本实施例通过输入修改后的管理员口令返回管理员模式，使得他人不能随意进入管理员模式来修改相关信息，进一步提高了系统信息的安全性。

[0107] 在一优选的实施例中，在上述图3实施例的基础上，第二写入模块具体用于在进入文件指定界面后，设置文件路径，根据所述文件路径获取待度量文件；获取所述待度量文件的二进制数据，对所述二进制数据进行哈希运算，得到所述第一哈希值，将所述第一哈希值写入所述存储区。

[0108] 本实施例中，在管理员模式下进入文件指定界面后，用户可以指定待度量文件，在文件指定界面中设置待度量文件的文件路径，然后根据文件路径获取待度量文件，将待度量文件的二进制数据进行哈希运算，即将待度量文件的任意长度的二进制值映射为较短的固定长度的二进制值，即得到第一哈希值。

[0109] 本实施例中，在BIOS环境下无文件系统解析代码，因此，无法直接通过路径识别文件，本实施例通过将待度量文件的二进制数据计算得到哈希值，便于后续的可信度量。

[0110] 本发明还提供一种系统，包括PCI密码卡及上述的主机，PCI密码卡用于预存可信度量程序，在与主机连接后并在主机处于管理员模式下，接收主机发送的第一硬件信息及待度量文件的第一哈希值并存储，在主机进入用户模式时，发送第一硬件信息及第一哈希值至主机，供主机在加载预存可信度量程序后进行可信度量。

[0111] 以上所述仅为本发明的较佳实施例，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、改进等，均应包含在本发明的保护范围之内。

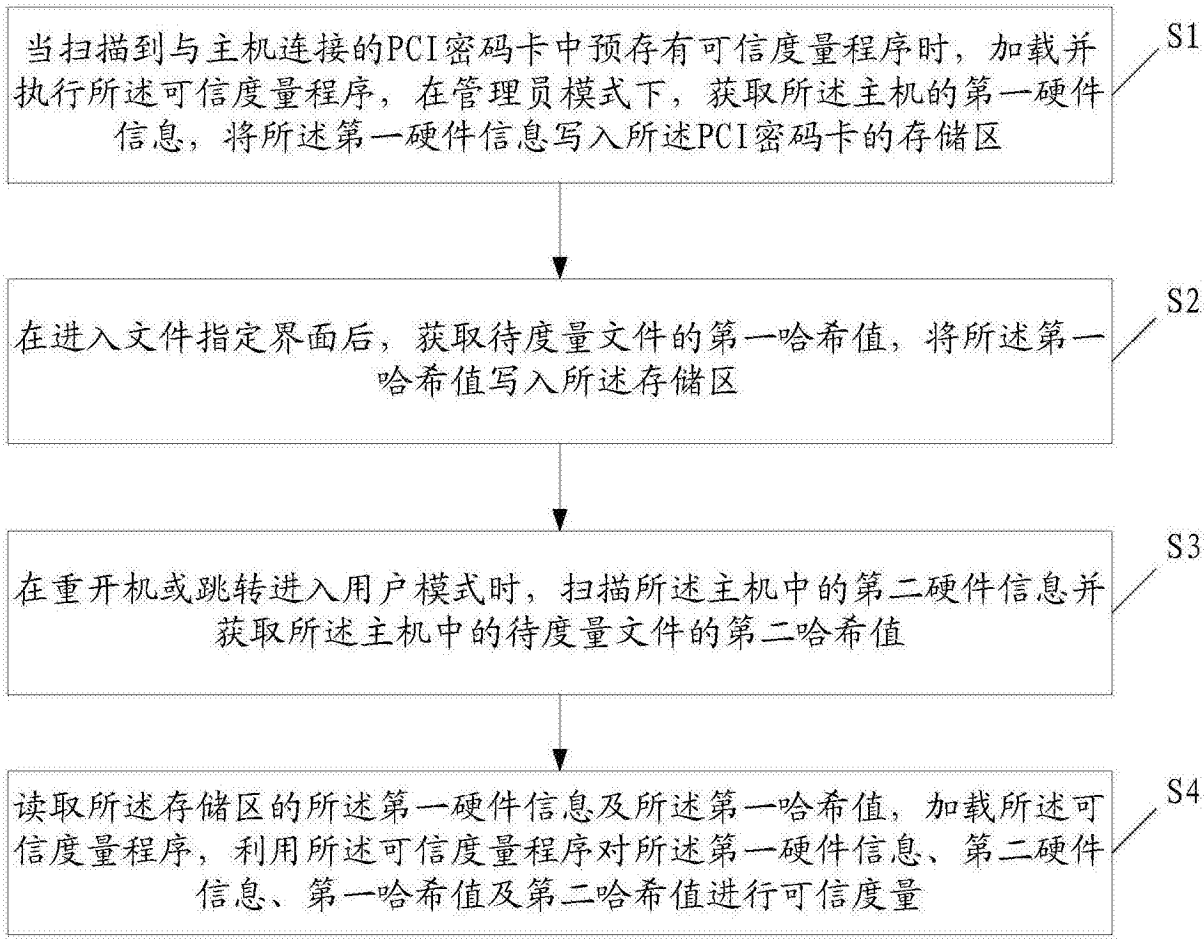

当扫描到与主机连接的PCI密码卡中预存有可信度量程序时，加载并执行所述可信度量程序，在管理员模式下，获取所述主机的第一硬件信息，将所述第一硬件信息写入所述PCI密码卡的存储区
S1
在进入文件指定界面后，获取待度量文件的第一哈希值，将所述第一哈希值写入所述存储区
S2
在重开机或跳转进入用户模式时，扫描所述主机中的第二硬件信息并获取所述主机中的待度量文件的第二哈希值
S3
读取所述存储区的所述第一硬件信息及所述第一哈希值，加载所述可信度量程序，利用所述可信度量程序对所述第一硬件信息、第二硬件信息、第一哈希值及第二哈希值进行可信度量
S4

图1

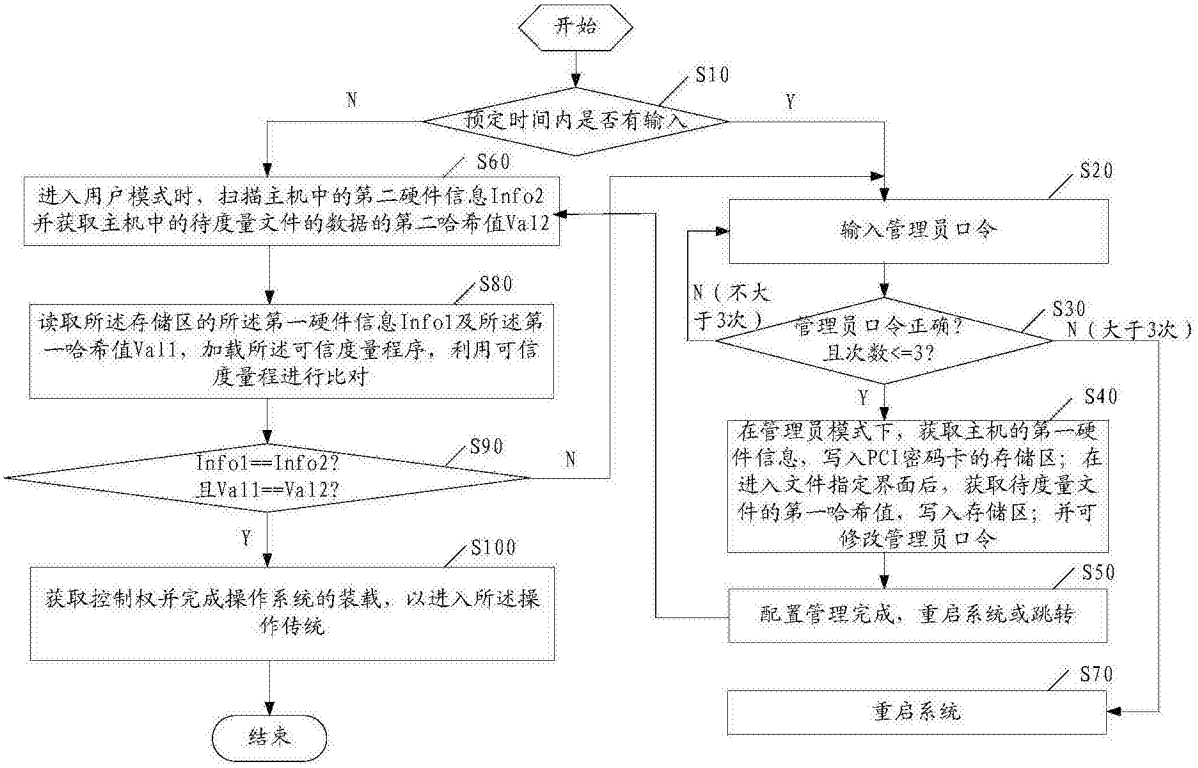

开始
S10
预定时间内是否有输入
N
Y
S60
进入用户模式时，扫描主机中的第二硬件信息Info2并获取主机中的待度量文件的数据的第二哈希值Val2
S20
输入管理员口令
N（不大于3次）
管理员口令正确？且次数<=3?
S30
N（大于3次）
Y
S80
读取所述存储区的所述第一硬件信息Info1及所述第一哈希值Val1，加载所述可信度量程序，利用可信度量程进行比对
S40
在管理员模式下，获取主机的第一硬件信息，写入PCI密码卡的存储区；在进入文件指定界面后，获取待度量文件的第一哈希值，写入存储区；并可修改管理员口令
S90
Info1==Info2?且Val1==Val2?
N
Y
S50
配置管理完成，重启系统或跳转
S100
获取控制权并完成操作系统的装载，以进入所述操作传统
S70
重启系统
结束

图2

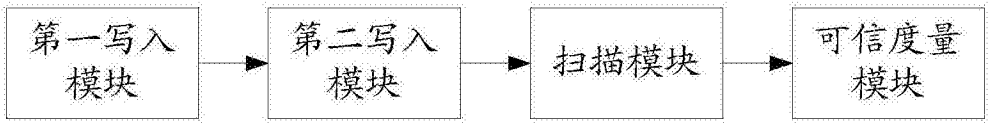

第一写入模块
第二写入模块
扫描模块
可信度量模块

图3