(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 111159700 A
(43)申请公布日 2020.05.15

(21)申请号 201911222649.7

(22)申请日 2019.12.03

(71)申请人 北京工业大学
地址 100022 北京市朝阳区平乐园100号

(72)发明人 张建标 王凯 郭雪松 刘国杰

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 王宇杨

(51)Int.Cl.
G06F 21/51(2013.01)
G06F 21/57(2013.01)
G06F 9/4401(2018.01)

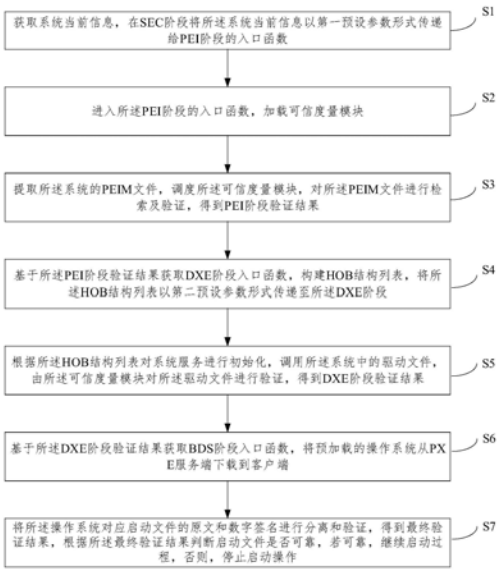
权利要求书2页 说明书9页 附图5页

(54)发明名称

一种基于UEFI系统的计算机远程安全启动方法及系统

(57)摘要

本发明实施例提供一种基于UEFI系统的计算机远程安全启动方法及系统。该方法包括：获取系统当前信息，在SEC阶段传递给PEI阶段；进入PEI阶段，加载可信度量模块；调度可信度量模块，对PEIM文件进行检索及验证；将HOB结构列表以第二预设参数形式传递至DXE阶段；根据HOB结构列表对系统服务进行初始化，调用系统中的驱动文件，由可信度量模块对驱动文件进行验证；将操作系统从PXE服务端下载到客户端；将操作系统对应启动文件的原文和数字签名进行分离和验证，得到最终验证结果，根据最终验证结果判断启动文件是否可靠。本发明实施例通过对UEFI系统各阶段的可信度量，从而保证了计算机从上电到加载操作系统的安全性。



CN 111159700 A

1.一种基于UEFI系统的计算机远程安全启动方法,其特征在于,包括:

获取系统当前信息,在SEC阶段将所述系统当前信息以第一预设参数形式传递给PEI阶段的入口函数;

进入所述PEI阶段的入口函数,加载可信度量模块;

提取所述系统的PEIM文件,调度所述可信度量模块,对所述PEIM文件进行检索及验证,得到PEI阶段验证结果;

基于所述PEI阶段验证结果获取DXE阶段入口函数,构建HOB结构列表,将所述HOB结构列表以第二预设参数形式传递至所述DXE阶段;

根据所述HOB结构列表对系统服务进行初始化,调用所述系统中的驱动文件,由所述可信度量模块对所述驱动文件进行验证,得到DXE阶段验证结果;

基于所述DXE阶段验证结果获取BDS阶段入口函数,将预加载的操作系统从PXE服务端下载到客户端;

将所述操作系统对应启动文件的原文和数字签名进行分离和验证,得到最终验证结果,根据所述最终验证结果判断启动文件是否可靠,若可靠,继续启动过程,否则,停止启动操作。

2.根据权利要求1所述的基于UEFI系统的计算机远程安全启动方法,其特征在于,所述获取系统当前信息,在SEC阶段将所述系统当前信息以第一预设参数形式传递给PEI阶段的入口函数,之前还包括:

所述PXE服务端配置预设的服务协议,并将预设文件集合发送至所述客户端。

3.根据权利要求2所述的基于UEFI系统的计算机远程安全启动方法,其特征在于,所述预设的服务协议包括DHCP服务协议和TFTP服务协议;所述预设文件集合包括initrd文件、vmlinux文件和bootloader.bin文件。

4.根据权利要求1所述的基于UEFI系统的计算机远程安全启动方法,其特征在于,所述系统当前信息包括系统当前状态、可启动固件地址、可启动固件大小、栈地址和栈大小。

5.根据权利要求1所述的基于UEFI系统的计算机远程安全启动方法,其特征在于,所述基于所述PEI阶段验证结果获取DXE阶段入口函数,具体包括:

所述系统基于所述PEI阶段验证结果,若验证通过,则调用DXE IPL PPI的Entry服务,获取DXE阶段入口函数。

6.根据权利要求1所述的基于UEFI系统的计算机远程安全启动方法,其特征在于,所述将所述操作系统对应启动文件的原文和数字签名进行分离和验证,得到最终验证结果,根据所述最终验证结果判断启动文件是否可靠,若可靠,继续启动过程,否则,停止启动操作,具体包括:

将所述原文和所述数字签名进行分离,并分别划分至第一缓冲区和第二缓冲区;

从所述可信度量模块中获取所述PXE服务端的公钥,基于所述公钥将所述数字签名转化为第一摘要,将所述原文采用哈希算法转化为第二摘要;

比较所述第一摘要和所述第二摘要,若相等,则判断所述启动文件可靠,继续执行启动操作,否则,判断所述启动文件不可靠,停止执行启动操作。

7.一种基于UEFI系统的计算机远程安全启动系统,其特征在于,包括:

获取模块,用于获取系统当前信息,在SEC阶段将所述系统当前信息以第一预设参数形

式传递给PEI阶段的入口函数；

PEI加载模块，用于进入所述PEI阶段的入口函数，加载可信度量模块；

PEI验证模块，用于提取所述系统的PEIM文件，调度所述可信度量模块，对所述PEIM文件进行检索及验证，得到PEI阶段验证结果；

DXE加载模块，用于基于所述PEI阶段验证结果获取DXE阶段入口函数，构建HOB结构列表，将所述HOB结构列表以第二预设参数形式传递至所述DXE阶段；

DXE验证模块，用于根据所述HOB结构列表对系统服务进行初始化，调用所述系统中的驱动文件，由所述可信度量模块对所述驱动文件进行验证，得到DXE阶段验证结果；

BDS加载模块，用于基于所述DXE阶段验证结果获取BDS阶段入口函数，将预加载的操作系统从PXE服务端下载到客户端；

BDS判断处理模块，用于将所述操作系统对应启动文件的原文和数字签名进行分离和验证，得到最终验证结果，根据所述最终验证结果判断启动文件是否可靠，若可靠，继续启动过程，否则，停止启动操作。

8.根据权利要求7所述的基于UEFI系统的计算机远程安全启动系统，其特征在于，所述系统还包括：

PXE服务端预设模块，用于所述PXE服务端配置预设的服务协议，并将预设文件集合发送至所述客户端。

9.一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如权利要求1至6任一项所述基于UEFI系统的计算机远程安全启动方法的步骤。

10.一种非暂态计算机可读存储介质，其上存储有计算机程序，其特征在于，该计算机程序被处理器执行时实现如权利要求1至6任一项所述基于UEFI系统的计算机远程安全启动方法的步骤。

一种基于UEFI系统的计算机远程安全启动方法及系统

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种基于UEFI系统的计算机远程安全启动方法及系统。

背景技术

[0002] 在计算机应用领域，常见的启动方式包括硬盘启动和网络启动，网络启动是利用PXE(Preboot Execution Environment)协议实现的，PXE全称是预启动执行环境，它提供了一种通过网络接口的方式启动计算机，这种方式最大优点是计算机可以摆脱已安装的操作系统或者本地存储设备而启动，同时不需要人工干预，自动完成装载运行。PXE工作于Client/Server(客户端/服务端)的网络模式，欲通过网络方式启动的计算机作为客户端，提供操作系统镜像和客户端启动所需文件的一端作为服务端。

[0003] 因为是通过网络的方式进行文件传输，所以这些文件存在被篡改的可能性。现有技术中有针对PXE协议的网络攻击方法，通过篡改PXE服务端发往客户端的启动文件起到注入木马病毒的效果。还有一种现有技术中针对PXE协议提出了一种攻击手段，其攻击原理是在网络上向DHCP服务器发送大量伪造的DHCP请求，这样做的目的是耗尽DHCP服务器可以分配的所有IP地址。此时，如果有合法的用户访问DHCP服务器，将无法提供服务。等到DHCP服务器彻底沦陷之后，网络攻击者在网络上放置假冒的DHCP服务器，通过此服务器为客户端提供地址和其他网络信息，从而导致中间人攻击。另有一种针对启动文件网络传输阶段的攻击手段，但是该论文并没有提出针对此种攻击方式的安全措施。另一方面，基于UEFI系统的计算机启动是一个“漫长”过程，UEFI系统从上电、启动到关机一共经历七个阶段：SEC(安全验证)、PEI(EFI初始化准备)、DXE(驱动执行环境)、BDS(启动设备选择)、TSL(操作系统前期阶段)、RT(系统运行)、AL(结束运行)。网络启动是在BDS阶段执行，在该阶段之前的PEI和DXE阶段会加载固件中的驱动文件，这些驱动文件都是以固件文件形式存储于Flash芯片之中，而UEFI系统并没有对这些驱动文件的正确性进行验证，攻击者可以通过伪造驱动文件并写入固件中达到攻击的效果。

发明内容

[0004] 本发明实施例提供一种基于UEFI系统的计算机远程安全启动方法及系统，用以解决现有技术中以网络方式启动客户端时，通过网络传输的操作系统文件容易受到攻击，安全性不高的缺陷。

[0005] 第一方面，本发明实施例提供一种基于UEFI系统的计算机远程安全启动方法，包括：

[0006] 获取系统当前信息，在SEC阶段将所述系统当前信息以第一预设参数形式传递给PEI阶段的入口函数；

[0007] 进入所述PEI阶段的入口函数，加载可信度量模块；

[0008] 提取所述系统的PEIM文件，调度所述可信度量模块，对所述PEIM文件进行检索及

验证，得到PEI阶段验证结果；

[0009] 基于所述PEI阶段验证结果获取DXE阶段入口函数，构建HOB结构列表，将所述HOB结构列表以第二预设参数形式传递至所述DXE阶段；

[0010] 根据所述HOB结构列表对系统服务进行初始化，调用所述系统中的驱动文件，由所述可信度量模块对所述驱动文件进行验证，得到DXE阶段验证结果；

[0011] 基于所述DXE阶段验证结果获取BDS阶段入口函数，将预加载的操作系统从PXE服务端下载到客户端；

[0012] 将所述操作系统对应启动文件的原文和数字签名进行分离和验证，得到最终验证结果，根据所述最终验证结果判断启动文件是否可靠，若可靠，继续启动过程，否则，停止启动操作。

[0013] 优选地，所述获取系统当前信息，在SEC阶段将所述系统当前信息以第一预设参数形式传递给PEI阶段的入口函数，之前还包括：

[0014] 所述PXE服务端配置预设的服务协议，并将预设文件集合发送至所述客户端。

[0015] 优选地，所述预设的服务协议包括DHCP服务协议和TFTP服务协议；所述预设文件集合包括initrd文件、vmlinux文件和bootloader.bin文件。

[0016] 优选地，所述系统当前信息包括系统当前状态、可启动固件地址、可启动固件大小、栈地址和栈大小。

[0017] 优选地，所述基于所述PEI阶段验证结果获取DXE阶段入口函数，具体包括：

[0018] 所述系统基于所述PEI阶段验证结果，若验证通过，则调用DXE IPL PPI的Entry服务，获取DXE阶段入口函数。

[0019] 优选地，所述将所述操作系统对应启动文件的原文和数字签名进行分离和验证，得到最终验证结果，根据所述最终验证结果判断启动文件是否可靠，若可靠，继续启动过程，否则，停止启动操作，具体包括：

[0020] 将所述原文和所述数字签名进行分离，并分别划分至第一缓冲区和第二缓冲区；

[0021] 从所述可信度量模块中获取所述PXE服务端的公钥，基于所述公钥将所述数字签名转化为第一摘要，将所述原文采用哈希算法转化为第二摘要；

[0022] 比较所述第一摘要和所述第二摘要，若相等，则判断所述启动文件可靠，继续执行启动操作，否则，判断所述启动文件不可靠，停止执行启动操作。

[0023] 第二方面，本发明实施例提供一种基于UEFI系统的计算机远程安全启动系统，包括：

[0024] 获取模块，用于获取系统当前信息，在SEC阶段将所述系统当前信息以第一预设参数形式传递给PEI阶段的入口函数；

[0025] PEI加载模块，用于进入所述PEI阶段的入口函数，加载可信度量模块；

[0026] PEI验证模块，用于提取所述系统的PEIM文件，调度所述可信度量模块，对所述PEIM文件进行检索及验证，得到PEI阶段验证结果；

[0027] DXE加载模块，用于基于所述PEI阶段验证结果获取DXE阶段入口函数，构建HOB结构列表，将所述HOB结构列表以第二预设参数形式传递至所述DXE阶段；

[0028] DXE验证模块，用于根据所述HOB结构列表对系统服务进行初始化，调用所述系统中的驱动文件，由所述可信度量模块对所述驱动文件进行验证，得到DXE阶段验证结果；

[0029] BDS加载模块，用于基于所述DXE阶段验证结果获取BDS阶段入口函数，将预加载的操作系统从PXE服务端下载到客户端；

[0030] BDS判断处理模块，用于将所述操作系统对应启动文件的原文和数字签名进行分离和验证，得到最终验证结果，根据所述最终验证结果判断启动文件是否可靠，若可靠，继续启动过程，否则，停止启动操作。

[0031] 优选地，所述系统还包括：

[0032] PXE服务端预设模块，用于所述PXE服务端配置预设的服务协议，并将预设文件集合发送至所述客户端。

[0033] 第三方面，本发明实施例提供一种电子设备，包括：

[0034] 存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现任一项所述基于UEFI系统的计算机远程安全启动方法的步骤。

[0035] 第四方面，本发明实施例提供一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现任一项所述基于UEFI系统的计算机远程安全启动方法的步骤。

[0036] 本发明实施例提供的基于UEFI系统的计算机远程安全启动方法及系统，通过对UEFI系统各阶段的可信度量，从而保证了计算机从上电到加载操作系统的安全性。

附图说明

[0037] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0038] 图1为本发明实施例提出的信任链传递机制示意图；

[0039] 图2为本发明实施例提出的一种基于UEFI系统的计算机远程安全启动方法流程图；

[0040] 图3为本发明实施例提出的PEI、DXE阶段度量过程示意图；

[0041] 图4为本发明实施例提出的BDS阶段度量流程示意图；

[0042] 图5为本发明实施例提出的启动文件封装示意图；

[0043] 图6为本发明实施例提出的一种基于UEFI系统的计算机远程安全启动系统结构图；

[0044] 图7为本发明实施例提供的电子设备的结构框图。

具体实施方式

[0045] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0046] 本发明实施例提出了一种基于UEFI系统的计算机远程安全启动方法，可以有效保证计算机从上电开始到PXE网络引导操作系统的安全。

[0047] 要特别指出的是，本发明实施例中安全启动的实现方式是通过软件模拟TPM，对UEFI系统各个阶段进行度量，整个流程如图1所示。SEC阶段和可信度量模块作为整个系统的可信根，SEC是作为系统启动的第一个阶段，可信验证模块对系统各个阶段的完整性进行检测。确立了可信根之后，就要从可信根开始建立一条基于UEFI启动过程的信任链，只有当前阶段验证通过才能进入下一阶段，如果某一阶段不可信则停止计算机的启动。

[0048] 网络启动是基于PXE协议实现的，PXE协议分为服务端和客户端两部分，PXE客户端在网卡的ROM中，当计算机引导时，UEFI把PXE客户端调入内存执行，并显示出命令菜单，经用户选择后，PXE客户端将放置在服务端的操作系统和启动文件通过网络下载到本地运行。所以首先要在服务端搭建PXE服务，因为在网络过程中启动文件存在被篡改的可能性，所以对每一个启动文件添加数字签名进行封装。服务端搭建完成之后，客户端就可以上电，然后在PEI、DXE阶段通过可信度量模块验证加载的驱动文件是否可靠，如果不可靠停止计算机的启动；否则系统运行至BDS阶段，通过PXE服务端下载操作系统镜像和启动文件，然后对启动文件数字签名进行验证，如果不可信则停止计算机的启动，否则加载操作系统镜像，完成计算机的开启。

[0049] 图2为本发明实施例提出的一种基于UEFI系统的计算机远程安全启动方法流程图，如图2所示，包括：

[0050] S1，获取系统当前信息，在SEC阶段将所述系统当前信息以第一预设参数形式传递给PEI阶段的入口函数；

[0051] S2，进入所述PEI阶段的入口函数，加载可信度量模块；

[0052] S3，提取所述系统的PEIM文件，调度所述可信度量模块，对所述PEIM文件进行检索及验证，得到PEI阶段验证结果；

[0053] S4，基于所述PEI阶段验证结果获取DXE阶段入口函数，构建HOB结构列表，将所述HOB结构列表以第二预设参数形式传递至所述DXE阶段；

[0054] S5，根据所述HOB结构列表对系统服务进行初始化，调用所述系统中的驱动文件，由所述可信度量模块对所述驱动文件进行验证，得到DXE阶段验证结果；

[0055] S6，基于所述DXE阶段验证结果获取BDS阶段入口函数，将预加载的操作系统从PXE服务端下载到客户端；

[0056] S7，将所述操作系统对应启动文件的原文和数字签名进行分离和验证，得到最终验证结果，根据所述最终验证结果判断启动文件是否可靠，若可靠，继续启动过程，否则，停止启动操作。

[0057] 具体地，首先执行PEI和DXE阶段的度量过程，如图3所示：

[0058] 步骤S1中，首先获取系统当前信息，SEC阶段是UEFI系统上电的第一个阶段，SEC阶段的工作都是为PEI做准备，将控制权转交给PEI阶段的同时还要将系统的当前信息以参数的形式，即第一预设参数形式传递给PEI阶段的入口函数；

[0059] 步骤S2中，由PEI阶段的入口函数进入，并加载可信度量模块，可信度量模块是以驱动文件的形式加载的，它的工作是检索当前阶段的固件文件并且进行完整性验证，度量中的基准值是在UEFI BIOS固件首次启动或是更新时计算而得；

[0060] 步骤S3中，提取系统的PEIM文件，此处PEIM文件是负责计算机处理器、硬件设备、芯片等的二进制代码文件，PEIM是以驱动文件形式存在的，所以系统运行到此阶段时，度量

模块会对这些PEIM验证，验证未通过则停止计算机的启动；

[0061] 步骤S4中，基于步骤S3中得到的PEI阶段验证结果，待所有的PEIM执行完毕之后，获取到DXE阶段入口函数，同时构建HOB结构列表，HOB是系统框架结构中用于将系统状态信息从PEI阶段传递到DXE阶段的体系结构机制，PEI阶段构建的HOB结构以参数的形式，即第二预设参数形式传递到DXE阶段；

[0062] 步骤S5中，由于HOB列表中包含有PEI阶段发现的系统内存信息以及固件设备信息，固件设备信息中提供了固件卷所在的内存位置，DXE阶段的调度程序加载、执行存在于固件卷中的驱动程序之前，度量模块要先对这些驱动文件进行完整性度量，验证未通过则停止计算机的启动；否则按照顺序执行驱动文件；

[0063] 步骤S6中，基于DEX阶段验证结果，之后系统进入BDS阶段，BDS阶段的主要功能是按照启动策略加载操作系统，本发明实施例研究的是网络启动过程中的计算机的安全性，所以预先设置的启动方式为PXE启动；为了保证所传输文件的可靠性，服务端对所传输的操作系统启动文件进行了数据签名并且添加到了原始文件的尾部，那么客户端在接收到文件之后就要进行相应的逆操作，工作流程如图4所示；

[0064] 步骤S7中，最后将操作系统对应启动文件的原文和数字签名进行分离和验证，得到最终验证结果，根据该最终验证结果判断启动文件是否可靠，若可靠，继续启动过程，否则，停止启动操作。

[0065] 综上所述，客户端整个启动过程可分为两部分，第一部分是PEI、DXE阶段，在这两个阶段主要是可信度量模块对驱动文件完整性进行验证，以保证操作系统加载前阶段的安全性；第二部分是BDS阶段，运行至该阶段，系统会根据系统启动顺序决定操作系统的加载方式。在远程启动的环境下，本地客户端会去PXE服务端请求启动文件和镜像，下载完成之后通过文件尾部的数字签名对各个文件进行完整性校验，如果可信则在TSL阶段引导加载程序，之后在RT阶段完成操作系统的启动。

[0066] 本发明实施例通过对UEFI系统各阶段的可信度量，从而保证了计算机从上电到加载操作系统的安全性。

[0067] 基于上述实施例，所述获取系统当前信息，在SEC阶段将所述系统当前信息以第一预设参数形式传递给PEI阶段的入口函数，之前还包括：

[0068] 所述PXE服务端配置预设的服务协议，并将预设文件集合发送至所述客户端。

[0069] 其中，所述预设的服务协议包括DHCP服务协议和TFTP服务协议；所述预设文件集合包括initrd文件、vmlinux文件和bootloader.bin文件。

[0070] 具体地，在SEC阶段之前，先要对PXE服务端进行预设，服务端所做的工作具体包括：

[0071] 1)配置DHCP服务，以使客户端在网络环境中动态的获得IP地址、Gateway地址，能够在服务端和客户端之间建立通信过程；

[0072] 2)安装TFTP服务，这是一个文件协议，用于将操作系统启动文件和镜像文件通过网络传输到本地服务器。

[0073] 由PXE服务端发往客户端的文件包括：

[0074] 1)initrd文件，这是在实际根文件系统可用之前挂载到系统中的一个初始根文件系统文件，initrd与内核绑定在一起，并作为内核引导过程的一部分进行加载。内核然后会

将这个initrd文件作为其阶段引导过程的一部分来加载模块,这样才能在以后的引导过程中使用真正的文件系统,并挂载实际的根文件系统;

[0075] 2)vmlinux文件,为未压缩的内核文件,即编译出来的最原始的文件,用于kerneldebug,产生system.map符号表;

[0076] 3)bootloader.bin文件,硬件启动的引导程序文件,是运行操作系统的前提。在操作系统内核或用户应用程序运行之前运行的一段小代码,对硬件进行相应的初始化和设定,最终为操作系统准备好环境。

[0077] 为了保证所传输文件的完整性,服务端在传输文件之前,为每一个文件计算数字签名,并且添加到原始文件完成启动文件的封装,工作流程如图5所示,因为数字摘要中采用的哈希算法是MD5,文件经过MD5哈希之后产生出一个128位(16字节)长度的哈希值,数字摘要由服务端私钥签名之后,生成的数字签名大小为64字节,所以每一个封装完成的启动文件大小为原始文件大小+64字节。

[0078] 本发明实施例通过对PXE服务端进行一系列的预先设置,实现了在客户端通过服务端进行启动调用之前的预实施方案。

[0079] 基于上述任一实施例,所述系统当前信息包括系统当前状态、可启动固件地址、可启动固件大小、栈地址和栈大小。

[0080] 具体地,在SEC阶段,获取的系统当前信息以参数行书传递给PEI阶段,该信息包括了:系统当前状态、可启动固件的地址和大小、栈地址和大小等等。

[0081] 基于上述任一实施例,所述基于所述PEI阶段验证结果获取DXE阶段入口函数,具体包括:

[0082] 所述系统基于所述PEI阶段验证结果,若验证通过,则调用DXE IPL PPI的Entry服务,获取DXE阶段入口函数。

[0083] 具体地,待所有的PEIM执行完毕之后,系统调用DXE IPL PPI的Entry服务,然后找到DXE Image的入口函数。

[0084] 基于上述任一实施例,所述将所述操作系统对应启动文件的原文和数字签名进行分离和验证,得到最终验证结果,根据所述最终验证结果判断启动文件是否可靠,若可靠,继续启动过程,否则,停止启动操作,具体包括:

[0085] 将所述原文和所述数字签名进行分离,并分别划分至第一缓冲区和第二缓冲区;

[0086] 从所述可信度量模块中获取所述PXE服务端的公钥,基于所述公钥将所述数字签名转化为第一摘要,将所述原文采用哈希算法转化为第二摘要;

[0087] 比较所述第一摘要和所述第二摘要,若相等,则判断所述启动文件可靠,继续执行启动操作,否则,判断所述启动文件不可靠,停止执行启动操作。

[0088] 具体地,首先PXE服务端搭建并且正常开启,也就是说PXE客户端可以通过服务端分配IP地址并且获取到TFTP服务器的地址信息,之后由TFTP服务器将经过数字签名之后启动文件以及操作系统镜像经过网络传输到客户端,客户端首要对原始文件和数字签名进行拆分,将原始文件和数字签名划分到两个缓冲区中,从可信度量模块中获取服务端生成的公钥并将数字签名转化为第一摘要,因为服务端采用的哈希算法是MD5,所以客户端同样采用MD5对原始文件加密形成第二摘要,然后比较第一摘要和第二摘要的值,如果相等就认为文件在网络传输过程中未收到篡改;反之,则认为文件不可靠,停止计算机的启动。

[0089] 本发明实施例在BDS阶段通过对预加载的启动文件进行拆分验证，较为可靠地验证了文件在传输过程中是否被攻击的状态，保证后续计算机启动的安全性。

[0090] 图6为本发明实施例提出的一种基于UEFI系统的计算机远程安全启动系统结构图，如图6所示，包括：获取模块61、PEI加载模块62、PEI验证模块63、DXE加载模块64、DXE验证模块65、BDS加载模块66和BDS判断处理模块67；其中：

[0091] 获取模块61用于获取系统当前信息，在SEC阶段将所述系统当前信息以第一预设参数形式传递给PEI阶段的入口函数；PEI加载模块62用于进入所述PEI阶段的入口函数，加载可信度量模块；PEI验证模块63用于提取所述系统的PEIM文件，调度所述可信度量模块，对所述PEIM文件进行检索及验证，得到PEI阶段验证结果；DXE加载模块64用于基于所述PEI阶段验证结果获取DXE阶段入口函数，构建HOB结构列表，将所述HOB结构列表以第二预设参数形式传递至所述DXE阶段；DXE验证模块65用于根据所述HOB结构列表对系统服务进行初始化，调用所述系统中的驱动文件，由所述可信度量模块对所述驱动文件进行验证，得到DXE阶段验证结果；BDS加载模块66用于基于所述DXE阶段验证结果获取BDS阶段入口函数，将预加载的操作系统从PXE服务端下载到客户端；BDS判断处理模块67用于将所述操作系统对应启动文件的原文和数字签名进行分离和验证，得到最终验证结果，根据所述最终验证结果判断启动文件是否可靠，若可靠，继续启动过程，否则，停止启动操作。

[0092] 本发明实施例通过对UEFI系统各阶段的可信度量，从而保证了计算机从上电到加载操作系统的安全性。

[0093] 基于上述任一实施例，该系统还包括PXE服务端预设模块68，所述PXE服务端预设模块68用于所述PXE服务端配置预设的服务协议，并将预设文件集合发送至所述客户端。其中，所述预设的服务协议包括DHCP服务协议和TFTP服务协议；所述预设文件集合包括initrd文件、vmlinux文件和bootloader.bin文件。

[0094] 本发明实施例通过对PXE服务端进行一系列的预先设置，实现了在客户端通过服务端进行启动调用之前的预实施方案。

[0095] 基于上述任一实施例，所述获取模块61中的所述系统当前信息包括系统当前状态、可启动固件地址、可启动固件大小、栈地址和栈大小。

[0096] 基于上述任一实施例，所述DXE加载模块64中的所述基于所述PEI阶段验证结果获取DXE阶段入口函数，具体包括：

[0097] 所述系统基于所述PEI阶段验证结果，若验证通过，则调用DXE IPL PPI的Entry服务，获取DXE阶段入口函数。

[0098] 基于上述任一实施例，所述BDS判断处理模块67包括：分离子模块671、转化子模块672和比较子模块673；其中：

[0099] 分离子模块671用于将所述原文和所述数字签名进行分离，并分别划分至第一缓冲区和第二缓冲区；转化子模块672用于从所述可信度量模块中获取所述PXE服务端的公钥，基于所述公钥将所述数字签名转化为第一摘要，将所述原文采用哈希算法转化为第二摘要；比较子模块673用于比较所述第一摘要和所述第二摘要，若相等，则判断所述启动文件可靠，继续执行启动操作，否则，判断所述启动文件不可靠，停止执行启动操作。

[0100] 本发明实施例在BDS阶段通过对预加载的启动文件进行拆分验证，较为可靠地验证了文件在传输过程中是否被攻击的状态，保证后续计算机启动的安全性。

[0101] 图7示例了一种电子设备的实体结构示意图，如图7所示，该电子设备可以包括：处理器(processor)710、通信接口(Communications Interface)720、存储器(memory)730和通信总线740，其中，处理器710，通信接口720，存储器730通过通信总线740完成相互间的通信。处理器710可以调用存储器730中的逻辑指令，以执行如下方法：获取系统当前信息，在SEC阶段将所述系统当前信息以第一预设参数形式传递给PEI阶段的入口函数；进入所述PEI阶段的入口函数，加载可信度量模块；提取所述系统的PEIM文件，调度所述可信度量模块，对所述PEIM文件进行检索及验证，得到PEI阶段验证结果；基于所述PEI阶段验证结果获取DXE阶段入口函数，构建HOB结构列表，将所述HOB结构列表以第二预设参数形式传递至所述DXE阶段；根据所述HOB结构列表对系统服务进行初始化，调用所述系统中的驱动文件，由所述可信度量模块对所述驱动文件进行验证，得到DXE阶段验证结果；基于所述DXE阶段验证结果获取BDS阶段入口函数，将预加载的操作系统从PXE服务端下载到客户端；将所述操作系统对应启动文件的原文和数字签名进行分离和验证，得到最终验证结果，根据所述最终验证结果判断启动文件是否可靠，若可靠，继续启动过程，否则，停止启动操作。

[0102] 此外，上述的存储器730中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random AccessMemory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0103] 另一方面，本发明实施例还提供一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现以执行上述各实施例提供的传输方法，例如包括：获取系统当前信息，在SEC阶段将所述系统当前信息以第一预设参数形式传递给PEI阶段的入口函数；进入所述PEI阶段的入口函数，加载可信度量模块；提取所述系统的PEIM文件，调度所述可信度量模块，对所述PEIM文件进行检索及验证，得到PEI阶段验证结果；基于所述PEI阶段验证结果获取DXE阶段入口函数，构建HOB结构列表，将所述HOB结构列表以第二预设参数形式传递至所述DXE阶段；根据所述HOB结构列表对系统服务进行初始化，调用所述系统中的驱动文件，由所述可信度量模块对所述驱动文件进行验证，得到DXE阶段验证结果；基于所述DXE阶段验证结果获取BDS阶段入口函数，将预加载的操作系统从PXE服务端下载到客户端；将所述操作系统对应启动文件的原文和数字签名进行分离和验证，得到最终验证结果，根据所述最终验证结果判断启动文件是否可靠，若可靠，继续启动过程，否则，停止启动操作。

[0104] 以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

[0105] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可

借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在计算机可读存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行各个实施例或者实施例的某些部分所述的方法。

[0106] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

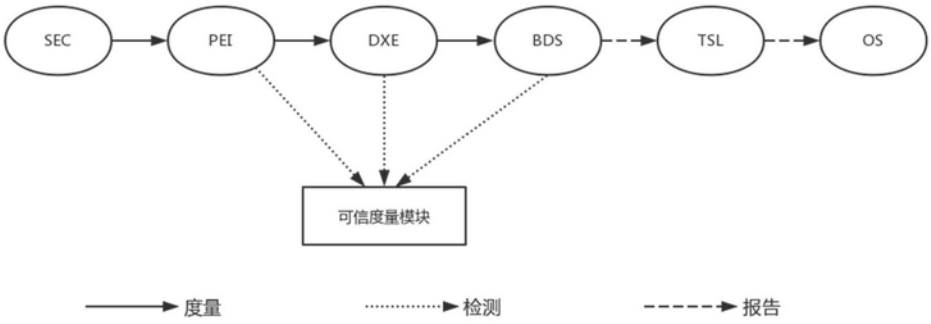


图1

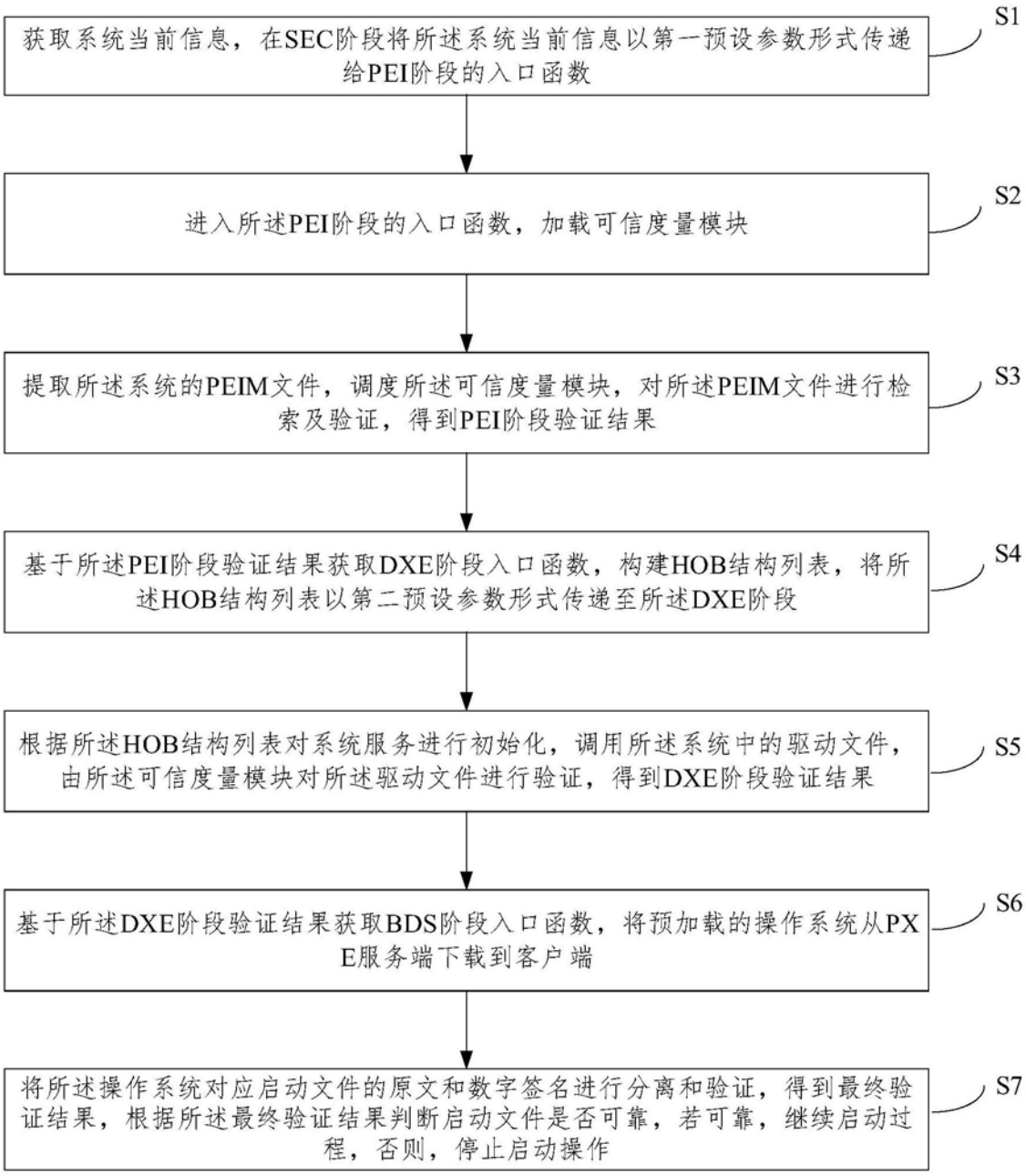

获取系统当前信息，在SEC阶段将所述系统当前信息以第一预设参数形式传递给PEI阶段的入口函数
S1
进入所述PEI阶段的入口函数，加载可信度量模块
S2
提取所述系统的PEIM文件，调度所述可信度量模块，对所述PEIM文件进行检索及验证，得到PEI阶段验证结果
S3
基于所述PEI阶段验证结果获取DXE阶段入口函数，构建HOB结构列表，将所述HOB结构列表以第二预设参数形式传递至所述DXE阶段
S4
根据所述HOB结构列表对系统服务进行初始化，调用所述系统中的驱动文件，由所述可信度量模块对所述驱动文件进行验证，得到DXE阶段验证结果
S5
基于所述DXE阶段验证结果获取BDS阶段入口函数，将预加载的操作系统从PXE服务端下载到客户端
S6
将所述操作系统对应启动文件的原文和数字签名进行分离和验证，得到最终验证结果，根据所述最终验证结果判断启动文件是否可靠，若可靠，继续启动过程，否则，停止启动操作
S7

图2

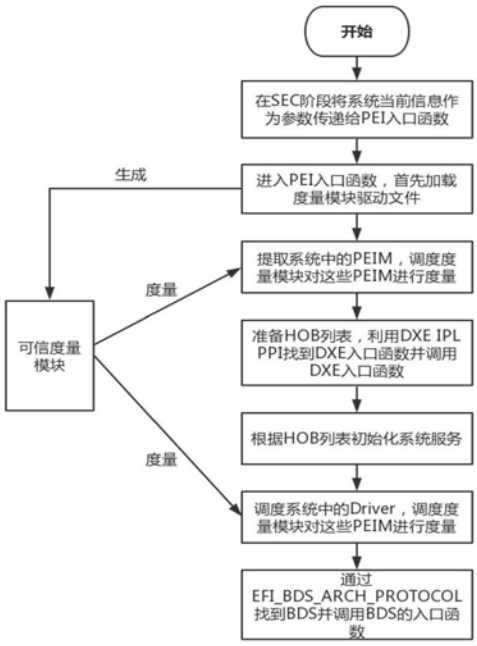

开始
在SEC阶段将系统当前信息作为参数传递给PEI入口函数
进入PEI入口函数，首先加载度量模块驱动文件
生成
提取系统中的PEIM，调度度量模块对这些PEIM进行度量
度量
可信度量模块
准备HOB列表，利用DXE IPL PPI找到DXE入口函数并调用DXE入口函数
根据HOB列表初始化系统服务
度量
调度系统中的Driver，调度度量模块对这些PEIM进行度量
通过EFI_BDS_ARCH_PROTOCOL找到BDS并调用BDS的入口函数

图3

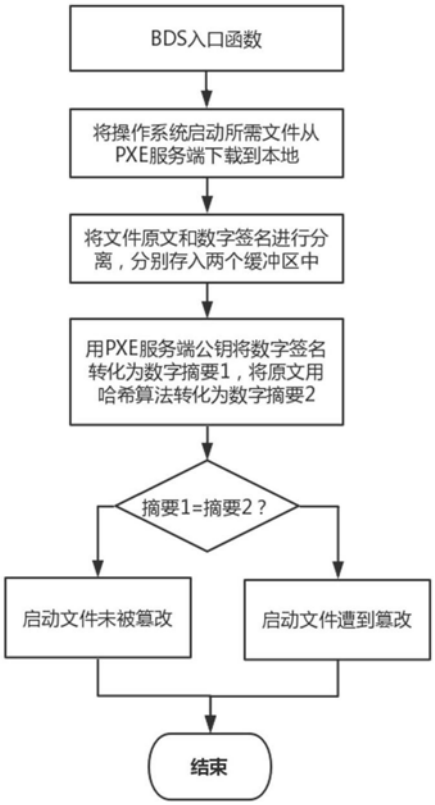

BDS入口函数
将操作系统启动所需文件从PXE服务端下载到本地
将文件原文和数字签名进行分离，分别存入两个缓冲区中
用PXE服务端公钥将数字签名转化为数字摘要1，将原文用哈希算法转化为数字摘要2
摘要1=摘要2？
启动文件未被篡改
启动文件遭到篡改
结束

图4

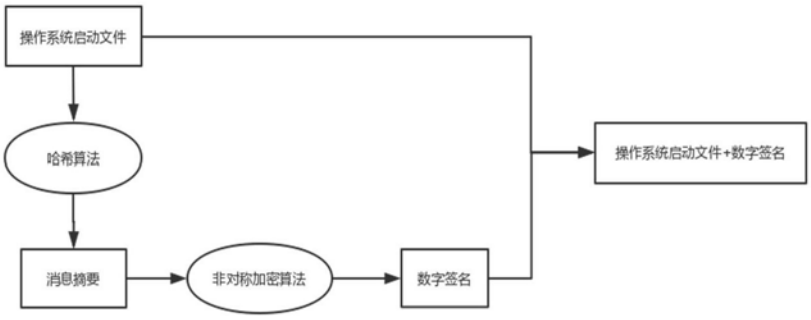

操作系统启动文件
哈希算法
消息摘要
非对称加密算法
数字签名
操作系统启动文件+数字签名

图5

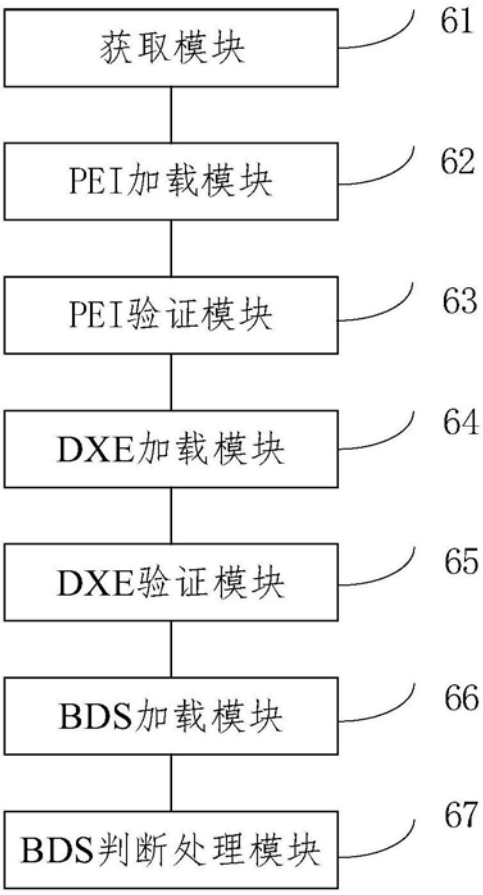

获取模块
61
PEI加载模块
62
PEI验证模块
63
DXE加载模块
64
DXE验证模块
65
BDS加载模块
66
BDS判断处理模块
67

图6

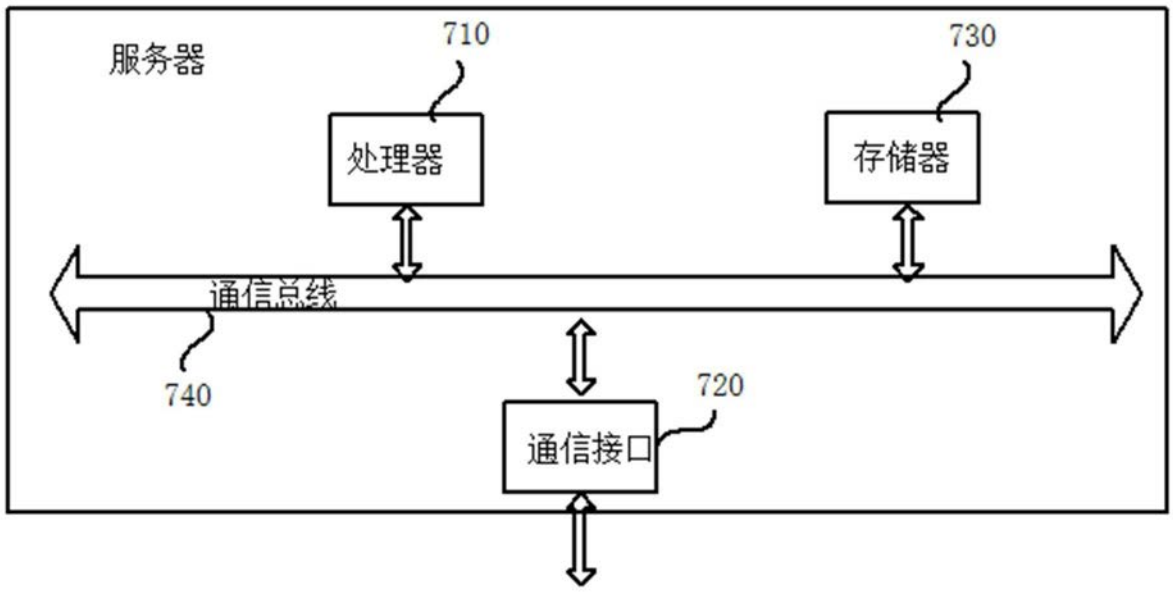


图7