(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107679425 B
(45)授权公告日 2020.09.04

(21)申请号 201710881358.3

(22)申请日 2017.09.26

(65)同一申请的已公布的文献号
申请公布号 CN 107679425 A

(43)申请公布日 2018.02.09

(73)专利权人 麒麟软件有限公司
地址 300450 天津市滨海新区高新区塘沽海洋科技园信安创业广场3号楼6-8层

(72)发明人 李艳厚 史晶 张超 郭俊余 孔金珠 张冬松 魏立峰

(74)专利代理机构 北京国昊天诚知识产权代理有限公司 11315
代理人 刘昕

(51)Int.Cl.
G06F 21/78(2013.01)
G06F 21/60(2013.01)

(56)对比文件
CN 102270288 A,2011.12.07
CN 102830990 A,2012.12.19
CN 105825131 A,2016.08.03
CN 101770386 A,2010.07.07
王赛.基于TrueCrypt和USBKEY的整盘加密系统设计与实现.《中国优秀硕士学位论文全文数据库》.2017,(第3期),
张杨.移动终端安全认证的设计与实现.《中国优秀硕士学位论文全文数据库》.2013,(第2期),

审查员 范广坡

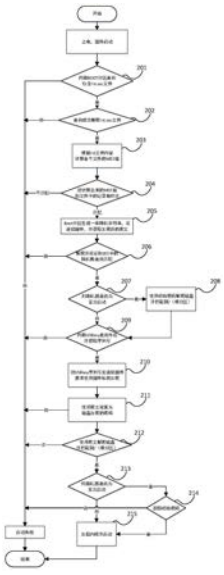
权利要求书4页 说明书8页 附图2页

(54)发明名称

一种基于固件和USBkey的联合全盘加密的可信启动方法

(57)摘要

一种基于固件和USBkey的联合全盘加密的可信启动方法,主要包括固件准备、boot分区准备、装机准备和开机可信启动;所述开机可信启动包括首次开机可信启动和非首次开机可信启动;所述首次开机可信启动和所述非首次开机可信启动均分为所述固件验证所述boot分区、所述boot分区验证所述固件和所述boot分区验证所述磁盘三个阶段。本申请的有益效果是:能够确保硬盘在不可信的情况下不会被打开,保证了硬盘中数据的安全;把秘钥存到固件中,避免了其他硬件的使用,降低了整机成本;增加了全盘加密,用于保护关机时的用户数据。



CN 107679425 B

1.一种基于固件和USBkey的联合全盘加密的可信启动方法,其特征在于:主要包括步骤:

固件准备:所述固件保存系统公钥和所述固件自己的固件私钥,用于在所述可信启动方法的步骤中进行加解密;所述固件具有MD5值计算功能,能够使用所述MD5值计算功能计算boot分区中文件的MD5值;

boot分区准备:对存储有所述boot分区中重要文件的MD5值的列表文件使用系统私钥进行签名,生成签名后的list.asc文件;生成用于发给所述固件获取所述固件的加密密文的字符串;提供公钥验签接口,用于验证固件身份;获取所述USBkey的序列号,并发送给所述固件,获取固件私钥签名后的密文,用于所述全盘加密的密码;

装机准备:对磁盘分区进行加密,设置初始密码;对存储有所述磁盘分区文件的MD5值的所述列表文件进行签名,放入所述boot分区;

开机可信启动:通过所述固件验证所述boot分区、所述boot分区验证所述固件和所述boot分区验证所述磁盘三个阶段,实现系统的可信启动;

具体为:所述固件获取所述boot分区中所述list.asc文件,使用系统公钥解密该文件,得到列表文件;验证所述boot分区中各重要文件的MD5是否匹配,若匹配,则启动所述boot分区;所述boot分区判断是否首次启动,若为首次启动,使用初始密码解密磁盘并挂载到/根分区;所述boot分区获取所述USBkey设备的序列号,并把该序列号发送给所述固件,所述固件返回一个使用固件私钥加密的密文;以该密文为密码对磁盘进行全盘加密;使用该密文解密磁盘,删除初始密码,启动系统。

2.根据权利要求1所述基于固件和USBkey的联合全盘加密的可信启动方法,其特征在于:所述列表文件中保存有文件grub.cfg、initrd.img的MD5值,所述列表文件使用所述系统私钥签名后得到list.asc文件。

3.根据权利要求1所述基于固件和USBkey的联合全盘加密的可信启动方法,其特征在于:所述装机准备的具体步骤包括:

S101、对所述磁盘进行分区,生成若干所述磁盘分区;

S102、对所述磁盘分区进行加密,设置一个初始密码;

S103、对所述磁盘分区进行解密,若解密失败,则创建系统盘失败,否则进入下一步;

S104、挂载所述磁盘,安装系统;

S105、计算所述boot分区中的grub.cfg,initrd.img文件的MD5值,保存到所述列表文件中;

S106、使用所述系统私钥对所述列表文件进行加密,得到list.asc文件,放入所述boot分区。

4.根据权利要求1所述基于固件和USBkey的联合全盘加密的可信启动方法,其特征在于:所述开机可信启动分为首次开机可信启动和非首次开机可信启动;所述首次开机可信启动和所述非首次开机可信启动均包括所述的三个阶段。

5.根据权利要求4所述基于固件和USBkey的联合全盘加密的可信启动方法,其特征在于:

所述固件验证所述boot分区的具体步骤包括:

S201、判断所述boot分区中是否包含所述list.asc文件,如果不包含,则启动失败,否

则进入下一步；

S202、使用所述系统公钥解密所述list.asc文件，得到所述列表文件，获取所述列表文件中保存的文件的MD5值，若解密失败，则启动失败；否则进入下一步；

S203、根据所述列表文件中的文件列表重新计算各个所述重要文件的MD5值；

S204、校验重新计算出来的所述重要文件的MD5值和所述列表文件中记录的所述重要文件的MD5值是否一致，若不一致，则启动失败；否则启动所述boot分区，进入下一步；

所述boot分区验证所述固件的具体步骤包括：

S205、所述boot分区生成一串字符串，把所述字符串传给所述固件，请求用所述固件私钥进行签名；所述固件收到私钥签名请求后，使用所述固件自己的固件私钥对所述字符串进行签名操作，将签名后的第一密文返回所述boot分区；

S206、所述boot分区收到所述第一密文后，使用保存在boot分区中的固件公钥进行验签，并验证所述固件的身份，若所述固件的身份验证未通过，则启动失败，否则进入下一步；

S207、所述boot分区判断当前系统是否是首次启动，若是首次启动，则进入下一步；否则跳过下一步，进入S209；

S208、所述boot分区使用所述装机准备中设置的初始密码解密所述磁盘并挂载；

所述boot分区验证所述磁盘的具体步骤包括：

S209、判断所述USBkey是否存在，若不存在，则启动失败；否则所述boot分区获取所述USBkey的序列号，进入下一步；

S210、所述boot分区把获取的所述序列号发送给所述固件，请求使用所述固件的固件私钥加密，加密后，所述固件返回使用所述固件私钥加密的第二密文；

S211、判断是否收到所述第二密文，若未收到，则启动失败；否则所述boot分区将收到的所述第二密文设置为所述全盘加密的密码；

S212、所述boot分区使用所述第二密文解密所述磁盘，若解密失败，则启动失败；否则挂载所述磁盘，进入下一步；

S213、所述boot分区判断当前系统是否是首次启动，若是首次启动，则进入下一步；否则跳过下一步，进入S215；

S214、删除所述装机准备中设置的初始密码，若删除失败，则启动失败，否则进入下一步；

S215、可信启动成功。

6.根据权利要求5所述基于固件和USBkey的联合全盘加密的可信启动方法，其特征在于：所述首次开机可信启动的具体步骤包括：

S201、判断所述boot分区中是否包含所述list.asc文件，如果不包含，则启动失败，否则进入下一步；

S202、固件使用所述系统公钥解密所述list.asc文件，得到所述列表文件，获取所述列表文件中保存的文件的MD5值，若解密失败，则启动失败；否则进入下一步；

S203、固件根据所述列表文件中的文件列表重新计算各个所述重要文件的MD5值；

S204、校验重新计算出来的所述重要文件的MD5值和所述列表文件中记录的所述重要文件的MD5值是否一致，若不一致，则启动失败；否则启动所述boot分区，进入下一步；

S205、所述boot分区生成一串字符串，把所述字符串传给所述固件，请求用所述固件私

钥进行签名;所述固件收到私钥签名请求后,使用所述固件自己的固件私钥对所述字符串进行签名操作,将签名后的第一密文返回所述boot分区;

S206、所述boot分区收到所述第一密文后,使用保存在boot分区中的所述固件公钥进行验签,并验证所述固件的身份,若所述固件的身份验证未通过,则启动失败,否则进入S208;

S208、所述boot分区使用所述装机准备中设置的初始密码解密所述磁盘并挂载;

S209、判断所述USBkey是否存在,若不存在,则启动失败;否则所述boot分区获取所述USBkey的序列号,进入下一步;

S210、所述boot分区把获取的所述序列号发送给所述固件,请求使用所述固件的固件私钥加密,加密后,所述固件返回使用所述固件私钥加密的第二密文;

S211、判断是否收到所述第二密文,若未收到,则启动失败;否则所述boot分区将收到的所述第二密文设置为所述全盘加密的密码;

S212、所述boot分区使用所述第二密文解密所述磁盘,若解密失败,则启动失败;否则挂载所述磁盘,进入S214;

S214、删除所述装机准备中设置的初始密码,若删除失败,则启动失败,否则进入下一步;

S215、可信启动成功。

7.根据权利要求5所述基于固件和USBkey的联合全盘加密的可信启动方法,其特征在于:所述非首次开机可信启动的具体步骤包括:

S201、判断所述boot分区中是否包含所述list.asc文件,如果不包含,则启动失败,否则进入下一步;

S202、固件使用所述系统公钥解密所述list.asc文件,得到所述列表文件,获取所述列表文件中保存的文件的MD5值,若解密失败,则启动失败;否则进入下一步;

S203、固件根据所述列表文件中的文件列表重新计算各个所述重要文件的MD5值;

S204、校验重新计算出来的所述重要文件的MD5值和所述列表文件中记录的所述重要文件的MD5值是否一致,若不一致,则启动失败;否则启动所述boot分区,进入下一步;

S205、所述boot分区生成一串字符串,把所述字符串传给所述固件,请求用所述固件私钥进行签名;所述固件收到私钥签名请求后,使用所述固件自己的固件私钥对所述字符串进行签名操作,将签名后的第一密文返回所述boot分区;

S206、所述boot分区收到所述第一密文后,使用保存在boot分区中的所述固件公钥进行验签,并验证所述固件的身份,若所述固件的身份验证未通过,则启动失败,否则进入S209;

S209、判断所述USBkey是否存在,若不存在,则启动失败;否则所述boot分区获取所述USBkey的序列号,进入下一步;

S210、所述boot分区把获取的所述序列号发送给所述固件,请求使用所述固件的固件私钥加密,加密后,所述固件返回使用所述固件私钥加密的第二密文;

S211、判断是否收到所述第二密文,若未收到,则启动失败;否则所述boot分区将收到的所述第二密文设置为所述全盘加密的密码;

S212、所述boot分区使用所述第二密文解密所述磁盘,若解密失败,则启动失败;否则

挂载所述磁盘，进入S215；

S215、可信启动成功。

一种基于固件和USBkey的联合全盘加密的可信启动方法

技术领域

[0001] 本申请属于可信启动技术领域，具体地说，涉及一种基于固件和USBkey的联合全盘加密的可信启动方法。

背景技术

[0002] 随着个人PC的普及和人们对信息安全的重视，保护计算机以及个人数据的安全，已经成为了至关重要的问题。在保护计算机安全方面，可信启动已经成为重要的技术手段之一。可信启动是使用具有可信计算功能的芯片，实现开机阶段的硬件的识别和可信任性的检测，提高了计算机的安全。

[0003] 1.可信启动

[0004] 国际上，可信计算组织提出了“可信链”和“可信度量”的概念，并认为：如果信息系统由一个初始的“可信根”开始，在平台控制权每一次转换时，通过完整性度量将这种信任传递给下一个组件，则平台计算环境就始终是可信的。可信启动，不仅需要一个“可信根”，而且还需要对可信根做回朔校验。

[0005] 在计算机系统中，启动过程是系统一切行为的基础。启动过程不但加载操作系统本身、负责初始化计算机系统的物理设备及操作系统本身状态，还启动系统维持正常运行所必要的可信进程及相关的服务程序。由于启动过程任何错误和疏漏都可能使操作系统进入不可预测的危险状态，因此启动过程是计算机系统实现可信计算的基础。

[0006] 2.固件

[0007] 固件就是写入EROM(可擦写只读存储器)或EEPROM(电可擦可编程只读存储器)中的程序。

[0008] 固件是指设备内部保存的设备“驱动程序”，通过固件，操作系统才能按照标准的设备驱动实现特定机器的运行动作，比如光驱、刻录机等都有内部固件。

[0009] 固件担任着一个系统最基础、最底层的工作，通常是硬件设备的灵魂。尤其当一些硬件设备除了固件以外没有其它软件组成时，固件也就决定着硬件设备的功能及性能。

[0010] 3.USBkey

[0011] USB Key是一种USB接口的硬件设备。它内置单片机或智能卡芯片，有一定的存储空间，可以存储用户的私钥以及数字证书，利用USB Key内置的公钥算法实现对用户身份的认证。由于用户私钥保存在密码锁中，理论上使用任何方式都无法读取，所以保证了用户认证的安全性。

[0012] 4.全盘加密

[0013] LUKS(Linux Unified Key Setup,Linux统一密钥设置)为linux硬盘分区加密提供了一种标准，它不仅能通用于不同的Linux发行版本，还支持多用户/口令。因为它的加密密钥独立于口令，所以即使口令失密，也可以迅速改变口令而无需重新加密真个硬盘。在使用它时必须首先对加密的卷进行解密，才能挂载其中的文件系统。

[0014] 现有的可信启动技术需要使用可信计算模块，需要增加硬件成本。另外，由于现有

大多数的可信启动技术都是使用可信根开始,单向的验证硬件信息的可信任性,并没有对用户数据做特别的保护处理,安全性差。

[0015] 中国发明专利“一种计算机可信启动方式”(申请号CN20140598064.6),该发明提供一种计算机可信启动方式,可信启动模块的引导过程主要分为两个阶段,即硬件平台的引导阶段和操作系统的启动阶段;其中:硬件平台的引导包括从平台加电、BIOS运行到BIOS将控制权交给Boot之前,这期间主要保证硬件环境的可信;操作系统的启动阶段是从主引导区调入操作系统装载程序一直到操作系统内核运行完毕,并运行初始化进程之前,该阶段主要保证系统的启动过程和操作系统内核的可信。该发明是面向龙芯处理器计算机设备提出的一种可信启动机制,是基于TCM芯片和FPGA芯片来实现可信启动方法,并没有涉及到基于固件和USBkey设备的联合全盘加密方法。

[0016] 中国发明专利“一种虚拟化平台服务器的可信启动方法及系统”(申请号CN201510821674.2),该申请公开了一种虚拟化平台服务器可信启动方法及系统,该方法包括:通过可信密码模块TCM对启动认证服务器操作系统的各个阶段进行校验,若校验通过,则建立从TCM至所述认证服务器的可信链;通过TCM校验虚拟化平台服务器核心库文件以及相关库文件,并生成校验结果;在所述校验结果表征文件校验通过时,通过预启动执行环境PXE协议保存核心库文件,并指示虚拟化平台服务器可信启动。该申请通过上述方法可以实现基于Extlinux的可信启动,但没有考虑基于grub的可信启动方案,也没有涉及到基于固件和USBkey设备的联合全盘加密方法。

[0017] 中国发明专利“一种内核可信启动方法和装置”(申请号CN201410114837.9),该发明提供一种内核可信启动方法和装置,所述方法包括:启动安全引导模块Boot loader;调用Boot loader、根据第一安全算法来度量平台配置寄存器PCR分区是否可信;若PCR分区可信,调用Boot loader将内核代码读取到内存中,并调用Boot loader根据第一完整算法以及分区内预存的内核代码的度量标准值来度量内核代码是否可信若内核代码可信,初始化内核代码以触发初始化的内核根据第二完整算法度量Boot loader是否可信;若Boot loader可信,启动内核。虽然该发明可以在一定程度上提高内核启动的安全性,并没有涉及到基于固件和USBkey设备的联合全盘加密方法。

发明内容

[0018] 有鉴于此,本申请所要解决的技术问题是提供了一种基于固件和USBkey的联合全盘加密的可信启动方法,能够确保硬盘在不可信的情况下不会被打开,保证了硬盘中数据的安全。

[0019] 为了解决上述技术问题,本申请公开了一种基于固件和USBkey的联合全盘加密的可信启动方法,并采用以下技术方案来实现。

[0020] 一种基于固件和USBkey的联合全盘加密的可信启动方法,主要包括步骤:

[0021] 固件准备:所述固件保存系统公钥和所述固件自己的固件私钥,用于在所述可信启动方法的步骤中进行加解密;所述固件具有MD5值计算功能,能够使用所述MD5值计算功能计算boot分区中文件的MD5值;

[0022] boot分区准备:对存储有所述boot分区中重要文件的MD5值的第一列表文件进行加密,并生成用于发给所述固件获取所述固件的加密密文的字符串;提供公钥解密接口,利

用所述USBkey的序列号获取用于所述全盘加密的密码；

[0023] 装机准备：对磁盘分区进行加密，设置初始密码；对存储有所述磁盘分区文件的MD5值的第二列表文件进行签名，放入所述boot分区；

[0024] 和开机可信启动：通过所述固件验证所述boot分区、所述boot分区验证所述固件和所述boot分区验证所述磁盘三个阶段，实现系统的可信启动。

[0025] 进一步的，所述第二列表文件中保存有文件grub.cfg、initrd.img的MD5值。

[0026] 进一步的，使用所述系统私钥对所述第二列表文件进行签名。

[0027] 进一步的，所述装机准备的具体步骤包括：

[0028] S101、对所述磁盘进行分区，生成若干所述磁盘分区；

[0029] S102、对所述磁盘分区进行加密，设置一个初始密码；

[0030] S103、对所述磁盘分区进行解密，若解密失败，则创建系统盘失败，否则进入下一步；

[0031] S104、挂载所述磁盘，安装系统；

[0032] S105、计算所述磁盘分区中文件的MD5值，保存到所述第二列表文件中；

[0033] S106、使用系统私钥对所述第二列表文件进行加密，放入所述boot分区。

[0034] 进一步的，所述开机可信启动分为首次开机可信启动和非首次开机可信启动；所述首次开机可信启动和所述非首次开机可信启动均包括所述的三个阶段。

[0035] 进一步的，所述固件验证所述boot分区的具体步骤包括：

[0036] S201、判断所述boot分区中是否包含所述第一列表文件，如果不包含，则启动失败，否则进入下一步；

[0037] S202、使用所述系统公钥解密所述第一列表文件，获取所述第一列表文件中保存的文件的MD5值，若解密失败，则启动失败；否则进入下一步；

[0038] S203、根据所述第一列表文件中的文件列表重新计算各个所述重要文件的MD5值；

[0039] S204、校验重新计算出来的所述重要文件的MD5值和所述第一列表文件中记录的所述重要文件的MD5值是否一致，若不一致，则启动失败；否则启动所述boot分区，进入下一步；

[0040] 所述boot分区验证所述固件的具体步骤包括：

[0041] S205、所述boot分区生成一串字符串，把所述字符串传给所述固件，请求用所述系统私钥进行加密；所述固件收到私钥加密请求后，使用所述固件自己的固件私钥对所述字符串进行加密操作，将加密后的第一密文返回所述boot分区；

[0042] S206、所述boot分区收到所述第一密文后，使用保存在固件中的所述系统公钥进行解密，并验证所述固件的身份，若所述固件的身份验证未通过，则启动失败，否则进入下一步；

[0043] S207、所述boot分区判断当前系统是否是首次启动，若是首次启动，则进入下一步；否则跳过下一步，进入S209；

[0044] S208、所述boot分区使用所述装机准备中设置的初始密码解密所述磁盘并挂载；

[0045] 所述boot分区验证所述磁盘的具体步骤包括：

[0046] S209、判断所述USBkey是否存在，若不存在，则启动失败；否则所述boot分区获取所述USBkey的序列号，进入下一步；

[0047] S210、所述boot分区把获取的所述序列号发送给所述固件，请求使用所述固件的固件私钥加密，加密后，所述固件返回使用所述固件私钥加密的第二密文；

[0048] S211、判断是否收到所述第二密文，若未收到，则启动失败；否则所述boot分区将收到的所述第二密文设置为所述全盘加密的密码；

[0049] S212、所述boot分区使用所述第二密文解密所述磁盘，若解密失败，则启动失败；否则挂载所述磁盘，进入下一步；

[0050] S213、所述boot分区判断当前系统是否是首次启动，若是首次启动，则进入下一步；否则跳过下一步，进入S215；

[0051] S214、删除所述装机准备中设置的初始密码，若删除失败，则启动失败，否则进入下一步；

[0052] S215、可信启动成功。

[0053] 进一步的，所述首次开机可信启动的具体步骤包括：

[0054] S201、判断所述boot分区中是否包含所述第一列表文件，如果不包含，则启动失败，否则进入下一步；

[0055] S202、使用所述系统公钥解密所述第一列表文件，获取所述第一列表文件中保存的文件的MD5值，若解密失败，则启动失败；否则进入下一步；

[0056] S203、根据所述第一列表文件中的文件列表重新计算各个所述重要文件的MD5值；

[0057] S204、校验重新计算出来的所述重要文件的MD5值和所述第一列表文件中记录的所述重要文件的MD5值是否一致，若不一致，则启动失败；否则启动所述boot分区，进入下一步；

[0058] S205、所述boot分区生成一串字符串，把所述字符串传给所述固件，请求用所述系统私钥进行加密；所述固件收到私钥加密请求后，使用所述固件自己的固件私钥对所述字符串进行加密操作，将加密后的第一密文返回所述boot分区；

[0059] S206、所述boot分区收到所述第一密文后，使用保存在固件中的所述系统公钥进行解密，并验证所述固件的身份，若所述固件的身份验证未通过，否则进入S208；

[0060] S208、所述boot分区使用所述装机准备中设置的初始密码解密所述磁盘并挂载；

[0061] S209、判断所述USBkey是否存在，若不存在，则启动失败；否则所述boot分区获取所述USBkey的序列号，进入下一步；

[0062] S210、所述boot分区把获取的所述序列号发送给所述固件，请求使用所述固件的固件私钥加密，加密后，所述固件返回使用所述固件私钥加密的第二密文；

[0063] S211、判断是否收到所述第二密文，若未收到，则启动失败；否则所述boot分区将收到的所述第二密文设置为所述全盘加密的密码；

[0064] S212、所述boot分区使用所述第二密文解密所述磁盘，若解密失败，则启动失败；否则挂载所述磁盘，进入S214；

[0065] S214、删除所述装机准备中设置的初始密码，若删除失败，则启动失败，否则进入下一步；

[0066] S215、可信启动成功。

[0067] 进一步的，所述非首次开机可信启动的具体步骤包括：

[0068] S201、判断所述boot分区中是否包含所述第一列表文件，如果不包含，则启动失

败,否则进入下一步;

[0069] S202、使用所述系统公钥解密所述第一列表文件,获取所述第一列表文件中保存的文件的MD5值,若解密失败,则启动失败;否则进入下一步;

[0070] S203、根据所述第一列表文件中的文件列表重新计算各个所述重要文件的MD5值;

[0071] S204、校验重新计算出来的所述重要文件的MD5值和所述第一列表文件中记录的所述重要文件的MD5值是否一致,若不一致,则启动失败;否则启动所述boot分区,进入下一步;

[0072] S205、所述boot分区生成一串字符串,把所述字符串传给所述固件,请求用所述系统私钥进行加密;所述固件收到私钥加密请求后,使用所述固件自己的固件私钥对所述字符串进行加密操作,将加密后的第一密文返回所述boot分区;

[0073] S206、所述boot分区收到所述第一密文后,使用保存在固件中的所述系统公钥进行解密,并验证所述固件的身份,若所述固件的身份验证未通过,则启动失败,否则进入S209;

[0074] S209、判断所述USBkey是否存在,若不存在,则启动失败;否则所述boot分区获取所述USBkey的序列号,进入下一步;

[0075] S210、所述boot分区把获取的所述序列号发送给所述固件,请求使用所述固件的固件私钥加密,加密后,所述固件返回使用所述固件私钥加密的第二密文;

[0076] S211、判断是否收到所述第二密文,若未收到,则启动失败;否则所述boot分区将收到的所述第二密文设置为所述全盘加密的密码;

[0077] S212、所述boot分区使用所述第二密文解密所述磁盘,若解密失败,则启动失败;否则挂载所述磁盘,进入S2015;

[0078] S215、可信启动成功。

[0079] 与现有技术相比,本申请可以获得包括以下技术效果:

[0080] (1)现有多数的可信启动技术都是设置一个可信根,然后基于可信根实现单向的可信启动验证,但这一设计可能存在机器不经过可信根启动就被启动的情况,本发明可以避免这一不安全情况的发生;

[0081] (2)现有可信启动大都使用TPM或者TCM实现秘钥的存储,本发明联合固件,把秘钥存到固件中,降低了整机成本;

[0082] (3)本发明相比普通的可信启动增加了全盘加密,用于保护关机时的用户数据;

[0083] (4)防止硬盘被窃取,用户数据泄露。

[0084] 当然,实施本申请的任一产品必不一定需要同时达到以上所述的所有技术效果。

附图说明

[0085] 此处所说明的附图用来提供对本申请的进一步理解,构成本申请的一部分,本申请的示意性实施例及其说明用于解释本申请,并不构成对本申请的不当限定。在附图中:

[0086] 图1是本申请装机准备流程的示意图。

[0087] 图2是本申请可信启动流程的示意图。

具体实施方式

[0088] 以下将配合附图及实施例来详细说明本申请的实施方式，藉此对本申请如何应用技术手段来解决技术问题并达成技术功效的实现过程能充分理解并据以实施。

[0089] 一种基于固件和USBkey的联合全盘加密的可信启动方法，包括如下步骤：固件准备、boot分区准备、装机准备和开机可信启动。其中，开机可信启动包括首次开机可信启动和非首次开机可信启动两个流程。

[0090] (一)固件准备：在固件中保存一个预先提供的公钥，用于解密boot分区中的文件；固件还需要保存自己的私钥，用于响应系统的私钥加密请求；另外固件具有MD5值计算功能，使用该功能计算boot分区中各文件的MD5值。

[0091] (二)boot分区准备：计算boot分区中各重要文件的MD5值，保存到指定文件(如list.asc文件)中，再使用系统私钥对其进行加密，用于固件检测boot分区中各重要文件的完整性；boot分区生成一串随机字符串，用于发给固件，获取固件加密的密文；提供公钥解密接口，用于解密固件加密的信息，检测固件身份；获取USBkey设备的序列号，发给固件，获取固件返回的密文，由于该密文是全盘加密的密码，所以使用该密文进行解密磁盘操作。

[0092] (三)装机准备：使用gparted对磁盘进行分区；然后使用cryptsetup进行分区加密，设置初始密码；计算grub.cfg、initrd.img等文件的MD5值，保存到list.asc文件中；再把list.asc文件使用系统私钥进行签名，放入boot分区。

[0093] 装机准备的详细步骤如图1所示，包括：

[0094] S101、使用gparted对磁盘进行分区；

[0095] S102、使用cryptsetup对分区进行加密，设置一个初始密码；

[0096] S103、对分区进行解密，如果解密失败，则提示创建系统盘失败，否则进入下一步；

[0097] S104、挂载磁盘到/mnt/root，安装系统；

[0098] S105、计算grub.cfg、initrd.img等文件的MD5值，保存到boot分区中指定的list.asc文件中；

[0099] S106、使用系统私钥对list.asc文件进行加密，放入boot分区。

[0100] (四)开机可信启动：分为首次开机可信启动和非首次开机可信启动两个流程。其中：

[0101] (1)首次开机可信启动：固件获取boot分区中list.asc文件，使用公钥解密该文件，然后验证boot分区中各重要文件的MD5是否匹配，若匹配，则启动boot分区；boot分区判断是否首次启动，若为首次启动，使用初始密码解密磁盘并挂载到/(根分区)；boot分区获取USBkey设备的序列号，并把该序列号发送给固件，固件返回一个使用固件私钥加密的密文；以该密文为密码对磁盘进行全盘加密；最后使用该密文解密磁盘，删除初始密码，启动系统。

[0102] 首次开机可信启动的详细步骤如图2所示，主要包括三个阶段，具体为：

[0103] 第一阶段：固件验证boot分区

[0104] S201、判断boot分区中是否包含list.asc文件，如果不包含，则启动失败，否则进入下一步；

[0105] S202、使用固件中系统公钥解密boot分区中指定的list.asc文件，获取list.asc文件中保存重要文件如grub.cfg和initrd.img文件的MD5值，如果解密失败，则启动失败，

否则进入下一步；

[0106] S203、解密成功后，再根据list.asc文件中重要文件的列表，分别计算各个重要文件如grub.cfg和initrd.img的MD5值；

[0107] S204、校验计算出来的重要文件MD5值和list.asc文件中记录的重要文件MD5值是否一致，如果不一致，则启动失败，否则启动boot分区，进入下一步。

[0108] 第二阶段：boot分区验证固件

[0109] S205、boot分区生成一串随机数，把随机数传给固件，请求用固件私钥加密；固件收到私钥加密请求后，使用固件自己的私钥进行加密操作，然后将加密后的密文返回boot分区；

[0110] S206、boot分区收到固件返回的密文后，使用保存在boot分区的固件公钥进行解密，并验证检测固件身份，如果解密后的密文和S205中的随机数不匹配，则启动失败，否则进入下一步；

[0111] S207、boot分区判断机器是否首次启动，如果是首次启动，则进入下一步，否则跳过下一步，直接进入步骤209；

[0112] S208、boot分区使用装机准备中设置的初始密码解密磁盘并挂载/(根分区)。

[0113] 第三阶段：boot分区验证磁盘

[0114] S209、判断USBkey设备是否存在，如果不存在，则启动失败，否则boot分区获取USBkey的序列号，进入下一步；

[0115] S210、boot分区把该序列号发送给固件，请求使用固件私钥加密，之后固件返回一个使用固件私钥加密的密文；

[0116] S211、判断是否收到固件加密后的密文，如果没有收到，则启动失败，否则boot分区将收到的密文设置为全盘加密的密码；

[0117] S212、boot分区使用前一步收到的密文解密磁盘，如果解密失败，则启动失败，否则挂载磁盘到/(根分区)，进入下一步；S213、boot分区判断机器是否首次启动，如果是首次启动，则进入下一步，否则跳过下一步，直接进入步骤215；

[0118] S214、删除装机准备中设置的初始密码，如果删除失败，则启动失败，否则进入下一步；

[0119] S215、启动系统。

[0120] (2)非首次开机可信启动：类似于首次开机可信启动的过程，通过固件验证boot分区、boot分区验证固件以及boot分区验证磁盘三个阶段，实现系统非首次开机可信启动。

[0121] 非首次开机可信启动流程的具体步骤也如图2所示，也包含固件验证boot分区、boot分区验证固件和boot分区验证磁盘等三个阶段，主要不同在于没有步骤208和步骤214，这是因为首次开机可信启动流程中已经删除了装机准备中设置的初始密码，非首次开机可信启动流程可以信任之前的开机可信启动流程。

[0122] 本申请的有益效果是：

[0123] (1)现有多数的可信启动技术都是设置一个可信根，然后基于可信根实现单向的可信启动验证，但这一设计可能存在机器不经过可信根启动就被启动的情况，本发明可以避免这一不安全情况的发生；

[0124] (2)现有可信启动大都使用TPM或者TCM实现秘钥的存储，本发明联合固件，把秘钥

存到固件中，降低了整机成本；

[0125] (3)本发明相比普通的可信启动增加了全盘加密，用于保护关机时的用户数据；

[0126] (4)防止硬盘被窃取，用户数据泄露。

[0127] 以上对本申请实施例所提供的一种基于固件和USBkey的联合全盘加密的可信启动方法，进行了详细介绍。以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

[0128] 如在说明书及权利要求当中使用了某些词汇来指称特定组件。本领域技术人员应可理解，不同机构可能会用不同名词来称呼同一个组件。本说明书及权利要求并不以名称的差异来作为区分组件的方式，而是以组件在功能上的差异来作为区分的准则。如在通篇说明书及权利要求当中所提及的“包含”为一开放式用语，故应解释成“包含但不限定于”。“大致”是指在可接收的误差范围内，本领域技术人员能够在一定误差范围内解决所述技术问题，基本达到所述技术效果。说明书后续描述为实施本申请的较佳实施方式，然所述描述乃以说明本申请的一般原则为目的，并非用以限定本申请的范围。本申请的保护范围当视所附权利要求所界定者为准。

[0129] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的商品或者系统不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种商品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的商品或者系统中还存在另外的相同要素。

[0130] 上述说明示出并描述了本申请的若干优选实施例，但如前所述，应当理解本申请并非局限于本文所披露的形式，不应看作是对其他实施例的排除，而可用于各种其他组合、修改和环境，并能够在本文所述发明创造构想范围内，通过上述教导或相关领域的技术或知识进行改动。而本领域人员所进行的改动和变化不脱离本申请的精神和范围，则都应在本申请所附权利要求的保护范围内。

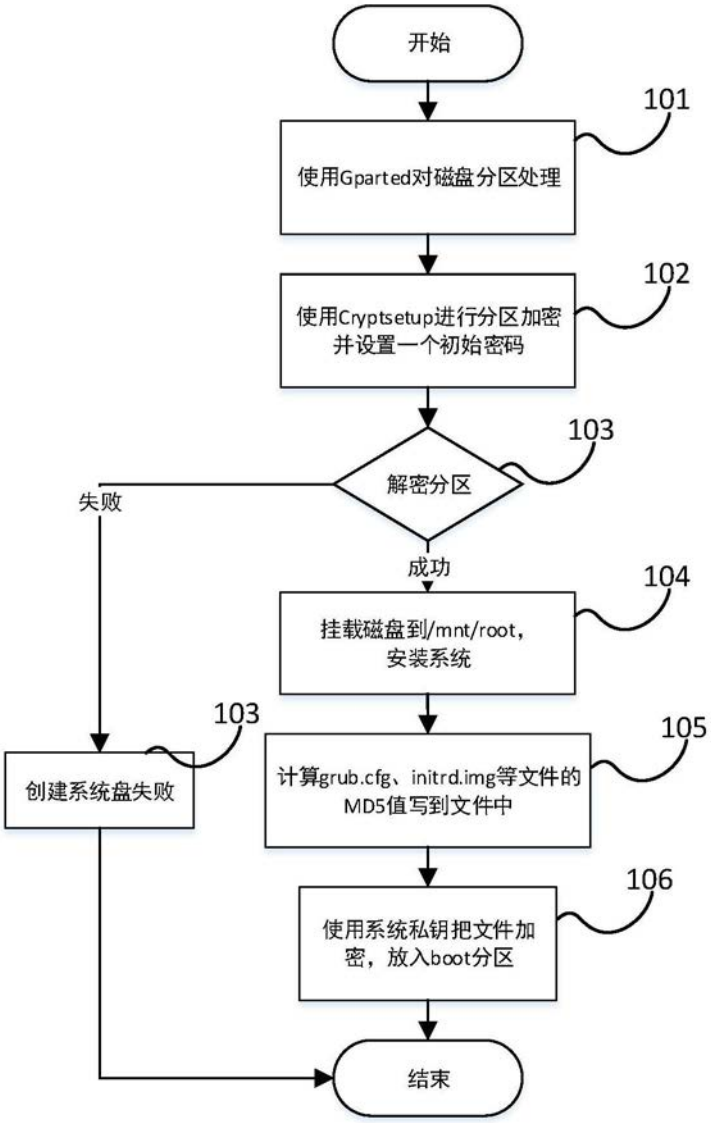

开始
101
使用Gparted对磁盘分区处理
102
使用Cryptsetup进行分区加密
并设置一个初始密码
103
解密分区
失败
成功
104
挂载磁盘到/mnt/root，
安装系统
103
创建系统盘失败
105
计算grub.cfg、initrd.img等文件的
MD5值写到文件中
106
使用系统私钥把文件加
密，放入boot分区
结束

图1

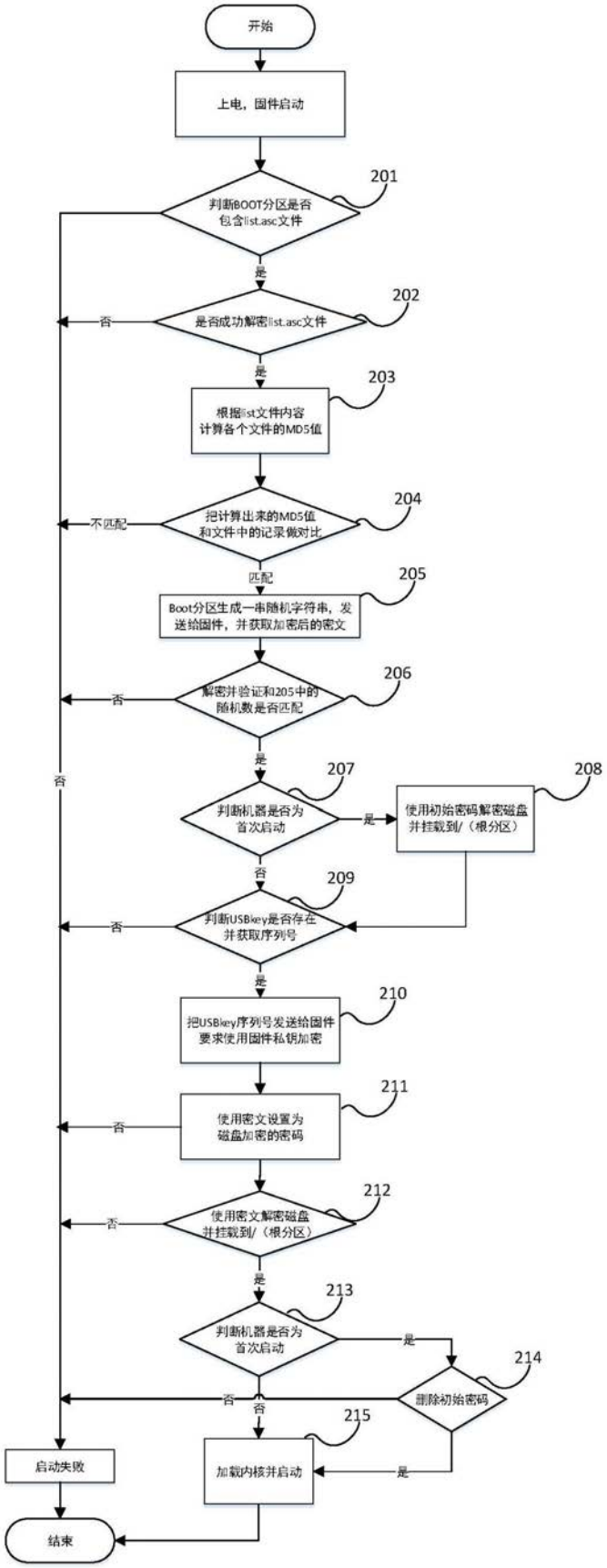

开始
上电，固件启动
判断BOOT分区是否包含list.asc文件
201
是
否
是否成功解密list.asc文件
202
是
根据list文件内容计算各个文件的MD5值
203
把计算出来的MD5值和文件中的记录做对比
204
不匹配
匹配
Boot分区生成一串随机字符串，发送给固件，并获取加密后的密文
205
解密并验证和205中的随机数是否匹配
206
否
是
否
判断机器是否为首次启动
207
是
使用初始密码解密磁盘并挂载到/（根分区）
208
否
判断USBkey是否存在并获取序列号
209
否
是
把USBkey序列号发送给固件要求使用固件私钥加密
210
使用密文设置为磁盘加密的密码
211
否
使用密文解密磁盘并挂载到/（根分区）
212
否
是
判断机器是否为首次启动
213
是
删除初始密码
214
否
否
加载内核并启动
215
是
启动失败
结束

图2