(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 110688653 A
(43)申请公布日 2020.01.14

(21)申请号 201910936996.X

(22)申请日 2019.09.29

(71)申请人 北京可信华泰信息技术有限公司
地址 100195 北京市海淀区闵庄路3号102幢三层04

(72)发明人 孙瑜 夏攀 杨成刚 王伟 何成成 王大海

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 董文倩

(51)Int.Cl.
G06F 21/55(2013.01)
G06F 21/62(2013.01)

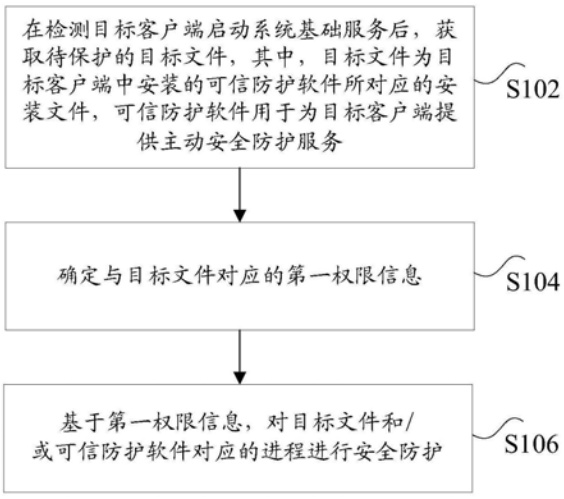
权利要求书2页 说明书9页 附图1页

(54)发明名称

客户端的安全防护方法及装置、终端设备

(57)摘要

本发明公开了一种客户端的安全防护方法及装置、终端设备。其中，该方法包括：在检测目标客户端启动系统基础服务后，获取待保护的目标文件，其中，目标文件为目标客户端中安装的可信防护软件所对应的安装文件，可信防护软件用于为目标客户端提供主动安全防护服务；确定与目标文件对应的第一权限信息；基于第一权限信息，对目标文件和/或可信防护软件对应的进程进行安全防护。本发明解决了相关技术中客户端采用的安全防护软件仅仅能进行被动防御，无法保证内部存储的文件的安全性的技术问题。



CN 110688653 A

1.一种客户端的安全防护方法,其特征在于,应用于目标客户端,包括:

在检测目标客户端启动系统基础服务后,获取待保护的目标文件,其中,所述目标文件为所述目标客户端中安装的可信防护软件所对应的安装文件,所述可信防护软件用于为所述目标客户端提供主动安全防护服务;

确定与所述目标文件对应的第一权限信息;

基于所述第一权限信息,对所述目标文件和/或所述可信防护软件对应的进程进行安全防护。

2.根据权利要求1所述的安全防护方法,其特征在于,所述安全防护方法还包括:

在启动所述可信防护软件后,获取所述目标客户端中的关键资源文件;

获取与所述关键资源文件对应的第二权限信息;

基于所述第二权限信息,对所述关键资源文件进行安全保护。

3.根据权利要求1所述的安全防护方法,其特征在于,所述安全防护方法还包括:

在所述目标客户端检测到注册表访问行为时,拦截所述注册表访问行为;

将所述注册表访问行为对应的访问注册表的路径与注册表访问策略进行对比;

若所述注册表访问策略中没有规定所述注册表访问行为对应的访问注册表的路径,则允许所述注册表访问行为执行;

若所述注册表访问策略中规定了所述注册表访问行为对应的访问注册表的路径,则禁止所述注册表访问行为执行。

4.根据权利要求1所述的安全防护方法,其特征在于,所述安全防护方法还包括:

在启动所述可信防护软件后,遍历所述目标客户端上的磁盘,得到所有磁盘文件;

从所述所有磁盘文件中识别出所述目标客户端当前运行环境中的可执行文件和支持脚本;

将所述可执行文件和与所述支持脚本对应的哈希值存入系统白名单;

基于所述系统白名单对所述目标客户端实现主动安全防护。

5.根据权利要求1所述的方法,其特征在于,所述安全防护方法还包括:

在启动所述可信防护软件之后,接收与所述目标客户端远程连接的管理中心传输的软件安装策略;

按照所述软件安装策略安装所述管理中心传输的软件包,并采集所述软件包安装过程中产生的白名单;

将采集到的所述白名单发送给所述管理中心,所述管理中心用于将所述白名单与所述软件安装策略对应存储。

6.根据权利要求1所述的方法,其特征在于,所述安全防护方法还包括:

所述目标客户端每隔预定时间段向与所述目标客户端远程连接的管理中心发送心跳数据,其中,所述心跳数据中携带有所述目标客户端的相关信息;

所述目标客户端接收所述管理中心在接收到所述心跳数据之后返回的通知消息,其中,所述通知消息用于通知所述目标客户端从所述管理中心获取目标策略;

所述目标客户端从所述管理中心获取并解析所述目标策略,并配置给内核;

所述目标客户端想所述管理中心发送确认消息,其中,所述确认消息用于通知所述管理中心所述目标策略已生效。

7.根据权利要求6所述的方法,其特征在于,所述安全防护方法还包括:

对所述目标客户端与所述管理中心之间的通信数据进行加密处理,其中,在进行加密处理时的加密算法至少包括:国密SM算法。

8.一种客户端的安全防护装置,其特征在于,包括:

获取单元,用于在检测目标客户端启动系统基础服务后,获取待保护的目标文件,其中,所述目标文件为所述目标客户端中安装的可信防护软件所对应的安装文件,所述可信防护软件用于为所述目标客户端提供主动安全防护服务;

确定单元,用于确定与所述目标文件对应的第一权限信息;

保护单元,用于基于所述第一权限信息,对所述目标文件和/或所述可信防护软件对应的进程进行安全保护。

9.一种终端设备,其特征在于,包括:

存储器,与所述存储器耦合的处理器,所述存储器和所述处理器通过总线系统相通信;

所述存储器用于存储程序,其中,所述程序在被处理器执行时控制所述存储器所在设备执行权利要求1至7中任意一项所述的客户端的安全防护方法,

所述处理器用于运行程序,其中,所述程序运行时执行权利要求1至7中任意一项所述的客户端的安全防护方法。

10.一种处理器,其特征在于,所述处理器用于运行程序,其中,所述程序运行时执行权利要求1至7中任意一项所述的客户端的安全防护方法。

客户端的安全防护方法及装置、终端设备

技术领域

[0001] 本发明涉及客户端信息处理技术领域，具体而言，涉及一种客户端的安全防护方法及装置、终端设备。

背景技术

[0002] 相关技术中，随着信息技术的不断发展，客户端上会存放很多的文件，为了保证这些文件的安全，常常采用外部安装的安全杀毒软件进行被动防御，这种安全杀毒软件往往是在有病毒攻击的情况下，才会进行杀毒识别，如果识别失败，则客户端会瘫痪，无法正常运行；这种采用安全杀毒软件进行被动防御的方式无法有效保证客户端内保存的文件的安全。

[0003] 针对上述的问题，目前尚未提出有效的解决方案。

发明内容

[0004] 本发明实施例提供了一种客户端的安全防护方法及装置、终端设备，以至少解决相关技术中客户端采用的安全防护软件仅仅能进行被动防御，无法保证内部存储的文件的安全性的技术问题。

[0005] 根据本发明实施例的一个方面，提供了一种客户端的安全防护方法，应用于目标客户端，包括：在检测目标客户端启动系统基础服务后，获取待保护的目标文件，其中，所述目标文件为所述目标客户端中安装的可信防护软件所对应的安装文件，所述可信防护软件用于为所述目标客户端提供主动安全防护服务；确定与所述目标文件对应的第一权限信息；基于所述第一权限信息，对所述目标文件和/或所述可信防护软件对应的进程进行安全防护。

[0006] 可选地，所述安全防护方法还包括：在启动所述可信防护软件后，获取所述目标客户端中的关键资源文件；获取与所述关键资源文件对应的第二权限信息；基于所述第二权限信息，对所述关键资源文件进行安全保护。

[0007] 可选地，所述安全防护方法还包括：在所述目标客户端检测到注册表访问行为时，拦截所述注册表访问行为；将所述注册表访问行为对应的访问注册表的路径与注册表访问策略进行对比；若所述注册表访问策略中没有规定所述注册表访问行为对应的访问注册表的路径，则允许所述注册表访问行为执行；若所述注册表访问策略中规定了所述注册表访问行为对应的访问注册表的路径，则禁止所述注册表访问行为执行。

[0008] 可选地，所述安全防护方法还包括：在启动所述可信防护软件后，遍历所述目标客户端上的磁盘，得到所有磁盘文件；从所述所有磁盘文件中识别出所述目标客户端当前运行环境中的可执行文件和支持脚本；将所述可执行文件和与所述支持脚本对应的哈希值存入系统白名单；基于所述系统白名单对所述目标客户端实现主动安全防护。

[0009] 可选地，所述安全防护方法还包括：在启动所述可信防护软件之后，接收与所述目标客户端远程连接的管理中心传输的软件安装策略；按照所述软件安装策略安装所述管理

中心传输的软件包，并采集所述软件包安装过程中产生的白名单；将采集到的所述白名单发送给所述管理中心，所述管理中心用于将所述白名单与所述软件安装策略对应存储。

[0010] 可选地，所述安全防护方法还包括：所述目标客户端每隔预定时间段向与所述目标客户端远程连接的管理中心发送心跳数据，其中，所述心跳数据中携带有所述目标客户端的相关信息；所述目标客户端接收所述管理中心在接收到所述心跳数据之后返回的通知消息，其中，所述通知消息用于通知所述目标客户端从所述管理中心获取目标策略；所述目标客户端从所述管理中心获取并解析所述目标策略，并配置给内核；所述目标客户端想所述管理中心发送确认消息，其中，所述确认消息用于通知所述管理中心所述目标策略已生效。

[0011] 可选地，所述安全防护方法还包括：对所述目标客户端与所述管理中心之间的通信数据进行加密处理，其中，在进行加密处理时的加密算法至少包括：国密SM算法。

[0012] 根据本发明实施例的另一方面，还提供了一种客户端的安全防护装置，包括：获取单元，用于在检测目标客户端启动系统基础服务后，获取待保护的目标文件，其中，所述目标文件为所述目标客户端中安装的可信防护软件所对应的安装文件，所述可信防护软件用于为所述目标客户端提供主动安全防护服务；确定单元，用于确定与所述目标文件对应的第一权限信息；保护单元，用于基于所述第一权限信息，对所述目标文件和/或所述可信防护软件对应的进程进行安全保护。

[0013] 可选地，所述客户端的安全防护装置还包括：第一确定模块，用于在启动所述可信防护软件后，获取所述目标客户端中的关键资源文件；第一获取模块，用于获取与所述关键资源文件对应的第二权限信息；第一保护模块，用于基于所述第二权限信息，对所述关键资源文件进行安全保护。

[0014] 可选地，所述安全防护装置还包括：拦截模块，用于在所述目标客户端检测到注册表访问行为时，拦截所述注册表访问行为；对比模块，用于将所述注册表访问行为对应的访问注册表的路径与注册表访问策略进行对比；允许模块，用于在所述注册表访问策略中没有规定所述注册表访问行为对应的访问注册表的路径时，允许所述注册表访问行为执行；禁止模块，用于在所述注册表访问策略中规定了所述注册表访问行为对应的访问注册表的路径时，禁止所述注册表访问行为执行。

[0015] 可选地，所述客户端的安全防护装置还包括：第一遍历模块，用于在启动所述可信防护软件后，遍历所述目标客户端上的磁盘，得到所有磁盘文件；第一识别模块，用于从所述所有磁盘文件中识别出所述目标客户端当前运行环境中的可执行文件和支持脚本；第一存储模块，用于将所述可执行文件和与所述支持脚本对应的哈希值存入系统白名单；第二保护模块，用于基于所述系统白名单对所述目标客户端实现主动安全防护。

[0016] 可选地，所述客户端的安全防护装置还包括：第一接收模块，用于在启动所述可信防护软件之后，接收与所述目标客户端远程连接的管理中心传输的软件安装策略；第一采集模块，用于按照所述软件安装策略安装所述管理中心传输的软件包，并采集所述软件包安装过程中产生的白名单；第一发送模块，用于将采集到的所述白名单发送给所述管理中心，所述管理中心用于将所述白名单与所述软件安装策略对应存储。

[0017] 可选地，所述客户端的安全防护装置还包括：第二发送模块，用于所述目标客户端每隔预定时间段向与所述目标客户端远程连接的管理中心发送心跳数据，其中，所述心跳

数据中携带有所述目标客户端的相关信息;第二接收模块,用于所述目标客户端接收所述管理中心在接收到所述心跳数据之后返回的通知消息,其中,所述通知消息用于通知所述目标客户端从所述管理中心获取目标策略;配置模块,用于所述目标客户端从所述管理中心获取并解析所述目标策略,并配置给内核;第三发送模块,用于所述目标客户端想所述管理中心发送确认消息,其中,所述确认消息用于通知所述管理中心所述目标策略已生效。

[0018] 可选地,所述客户端的安全防护装置还包括:加密模块,用于对所述目标客户端与所述管理中心之间的通信数据进行加密处理,其中,在进行加密处理时的加密算法至少包括:国密SM算法。

[0019] 根据本发明实施例的另一方面,还提供了一种终端设备,包括:存储器,与所述存储器耦合的处理器,所述存储器和所述处理器通过总线系统相通信;所述存储器用于存储程序,其中,所述程序在被处理器执行时控制所述存储器所在设备执行上述任意一项所述的客户端的安全防护方法,所述处理器用于运行程序,其中,所述程序运行时执行上述任意一项所述的客户端的安全防护方法。

[0020] 根据本发明实施例的另一方面,还提供了一种处理器,所述处理器用于运行程序,其中,所述程序运行时执行上述任意一项所述的客户端的安全防护方法。

[0021] 在本发明实施例中,采用在检测目标客户端启动系统基础服务后,获取待保护的目标文件,其中,目标文件为目标客户端中安装的可信防护软件所对应的安装文件,可信防护软件用于为目标客户端提供主动安全防护服务,并确定与目标文件对应的第一权限信息,然后基于第一权限信息,对目标文件和/或可信防护软件对应的进程进行安全防护。在该实施例中,可以通过可信防护软件实现对客户端的全面且稳定的安全防护,对需要存储的文件进行主动安全保护,并对自己的软件进程进行自保护,防止非法篡改或删除,提高文件的安全性,能够让用户实时了解到自己所使用的客户端的安全状态,提高用户使用可信防护软件的满意度,进而解决了相关技术中客户端采用的安全防护软件仅仅能进行被动防御,无法保证内部存储的文件的安全性的技术问题。

附图说明

[0022] 此处所说明的附图用来提供对本发明的进一步理解,构成本申请的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

[0023] 图1是根据本发明实施例的一种可选的客户端的安全防护方法的流程图;

[0024] 图2是根据本发明实施例的一种可选的客户端的安全防护装置的示意图。

具体实施方式

[0025] 为了使本技术领域的人员更好地理解本发明方案,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,所描述的实施例仅仅是本发明一部分的实施例,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,都应当属于本发明保护的范围。

[0026] 需要说明的是,本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。应该理解这样使用

的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0027] 本发明各实施例中的客户端的安全防护方法及装置的执行主体为目标客户端，该目标客户端可以理解为用户平常所使用的终端或可信计算平台，在进行主动安全防御时，采用可信安全管理平台(运行于服务器)对各个目标客户端或可信计算平台进行数据处理，下发主动防御任务等；目标客户端运行的系统包括并行的计算子系统与防护子系统，其中，计算子系统用于完成计算任务，而防护子系统用于使用可信防护软件，根据可信策略对计算子系统进行主动度量，目标客户端负责采集应用程序的访问行为数据，并上报给目标服务器，从而实时更新可信策略以及可信防护软件，提高安全防护性能。

[0028] 上述的目标客户端可以包括但不限于：平板、移动终端、PC、IPAD等。

[0029] 根据本发明实施例，提供了一种客户端的安全防护方法实施例，需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0030] 本发明实施例可以应用于目标客户端，可以对可信防护软件的软件进程实现自保护，并对客户端上需要保护的文件进行主动安全防护，放置非法修改或删除等。

[0031] 图1是根据本发明实施例的一种可选的客户端的安全防护方法的流程图，如图1所示，该方法包括如下步骤：

[0032] 步骤S102，在检测目标客户端启动系统基础服务后，获取待保护的目标文件，其中，目标文件为目标客户端中安装的可信防护软件所对应的安装文件，可信防护软件用于为目标客户端提供主动安全防护服务。

[0033] 上述的可信防护软件可以是目标客户端自行下载并安装上，在目标客户端开机后，控制系统启动系统基础服务，该系统基础服务可以是指开启客户端的基础运行软件等，如开启Windows，开启可信防护软件。待保护的目标文件可以是客户端控制系统指示需要进行保护的文件(如word文件、软件的安装包)。

[0034] 在目标客户端中安装可信防护软件时，可以包括：目标客户端通过管理中心或者U盘等外设工具将安装程序/安装包拷贝到目标文件目录下；安装系统常用运行库合集；运行安装程序/解压压缩包；安装程序自动扫描白名单并把安装信息上报至管理中心；向管理中心注册该目标客户端以及报告程序安装完毕。可选的，本发明实施例的安装包可以为EXE格式的。

[0035] 步骤S104，确定与目标文件对应的第一权限信息。

[0036] 第一权限信息用于指示是否可以对目标文件或可信防护软件的软件进程进行修改、删除等操作，如对于可信防护软件的软件进程和目标文件的权限配置为只读权限，则在有修改指令时，对目标文件或软件进程进行安全防护，放置被修改。这样外部指令无法随意杀死软件进程，无法修改、删除目标文件。

[0037] 步骤S106，基于第一权限信息，对目标文件和/或可信防护软件对应的进程进行安

全防护。

[0038] 通过上述步骤，可以采用在检测目标客户端启动系统基础服务后，获取待保护的目标文件，其中，目标文件为目标客户端中安装的可信防护软件所对应的安装文件，可信防护软件用于为目标客户端提供主动安全防护服务，并确定与目标文件对应的第一权限信息，然后基于第一权限信息，对目标文件和/或可信防护软件对应的进程进行安全防护。在该实施例中，可以通过可信防护软件实现全面且稳定的安全防护，对需要存储的文件进行主动安全保护，并对自己的软件进程进行自保护，防止非法篡改或删除，提高文件的安全性，能够让用户实时了解到自己所使用的客户端的安全状态，提高用户使用可信防护软件的满意度，从而解决相关技术中客户端采用的安全防护软件仅仅能进行被动防御，无法保证内部存储的文件的安全性的技术问题。

[0039] 作为本发明可选的实施例，在对客户端进行安全防护，除了通过权限信息来进行防护外，还可以通过其它的方式来进行安全防护。可选的，安全防护方法还包括：在启动可信防护软件后，获取目标客户端中的关键资源文件；获取与关键资源文件对应的第二权限信息；基于资源权限，对关键资源文件进行权限配置；基于第二权限信息，对关键资源文件进行安全保护。

[0040] 一种可选的实施方式，关键资源文件包括下述至少之一：系统注册表、系统核心文件。关键资源文件可以为系统管理员自行定义输入的需要保护的文件(可携带绝对路径)。

[0041] 上述的第二权限信息可以对关键资源文件进行权限保护，防止篡改和防止删除关键资源文件，例如，设置对关键资源文件只有读权限无写权限，无修改和删除权限；同时在客户端的控制系统重启后关键资源文件的第二权限信息保护不失效。

[0042] 另一种可选的，在进行安全防护时，还可以在启动可信防护软件后，遍历目标客户端上的磁盘，得到所有磁盘文件；从所有磁盘文件中识别出目标客户端当前运行环境中的可执行文件和支持脚本；将可执行文件和与支持脚本对应的哈希值存入系统白名单；基于系统白名单对目标客户端实现主动安全防护。

[0043] 上述安全防护功能可以理解为白名单采集，白名单可以理解为将应用程序或软件经过特定算法计算得到一个摘要值，该摘要值即为该软件或程序的白名单值，简称白名单；将客户端的控制系统或者操作系统当前运行环境中所有可执行文件及支持脚本采集到系统白名单中，采集白名单的文件格式是：Windows系统支持(文件判断PE头，凡是带PE头的文件都支持)：EXE、DLL、OCX、SYS、COM和脚本(.msi、.msu、.bat、.cmd)等格式。在可信防护软件安装并运行后，可以开始白名单采集操作，同时可以在客户端界面告知用户正在扫描白名单，对全盘的可执行文件可使用加密算法进行hash值计算，并把计算得到哈希值作为基准值存入系统白名单或写入预设白名单数据库，同时可告知管理中心白名单采集完成，通过系统白名单对目标客户端进行主动安全防护(防护时可以先计算hash值，然后与数据库中的基准值进行校验，通过校验的可正常执行)。

[0044] 作为本发明可选的实施例，在对目标客户端进行安全防护时，还可以进行注册表保护，包括：在目标客户端检测到注册表访问行为时，拦截注册表访问行为；将注册表访问行为对应的访问注册表的路径与注册表访问策略进行对比；若注册表访问策略中没有规定注册表访问行为对应的访问注册表的路径，则允许注册表访问行为执行；若注册表访问策略中规定了注册表访问行为对应的访问注册表的路径，则禁止注册表访问行为执行。

[0045] 即本发明实施例中，注册表访问控制的功能是根据注册表访问策略进行放行决策，当驱动加载的时候可以初始化访问策略表，并且注册自己的通讯接口，最后向系统注册注册表操作的钩子，通过该钩子拦截注册表访问行为，可以将注册表访问信息拦截到注册表输入/输出模块，然后查询访问策略表，根据策略表判断结果选择放行或者拦截(即禁止注册表访问行为执行)。

[0046] 上述注册表保护可以是指在注册表访问前，进行权限检查，控制系统里各个软件的进程和用户对这些受保护的注册表资源只有读权限，不能修改和删除；即使控制系统重启后注册表保护策略也不失效。

[0047] 作为本发明可选的实施例，在对目标客户端进行安全防护时，还可以在启动可信防护软件之后，接收与目标客户端远程连接的管理中心传输的软件安装策略；按照软件安装策略安装管理中心传输的软件包，并采集软件包安装过程中产生的白名单；将采集到的白名单发送给管理中心，管理中心用于将白名单与软件安装策略对应存储。

[0048] 另一种可选的，在对目标客户端进行安全防护时，还可以进行心跳数据上传，包括：目标客户端每隔预定时间段向与目标客户端远程连接的管理中心发送心跳数据，其中，心跳数据中携带有目标客户端的相关信息；目标客户端接收管理中心在接收到心跳数据之后返回的通知消息，其中，通知消息用于通知目标客户端从管理中心获取目标策略；目标客户端从管理中心获取并解析目标策略，并配置给内核；目标客户端想管理中心发送确认消息，其中，确认消息用于通知管理中心目标策略已生效。

[0049] 上述预定时间段可以自行设置，例如，10秒。客户端每隔10秒钟向管理中心发送一次心跳数据。该心跳数据包括但不限于：客户端CPU运行状态、内存占比、磁盘信息、进程列表。

[0050] 另一种可选的，安全防护方法还包括：对目标客户端与管理中心之间的通信数据进行加密处理，其中，在进行加密处理时的加密算法至少包括：国密SM算法。

[0051] 作为本发明可选的实施例，在对目标客户端进行安全防护时，还可以对审计信息进行处理，包括：获取数据库在最近一段时间内产生的所有审计信息；对审计信息中的重复内容进行去重处理；过滤审计信息；将过滤后的审计信息上报给管理中心；记录当前已处理的审计信息的位置和数量，避免重复处理；上报审计信息处理日志。

[0052] 通过上述实施例，可以利用可信防护软件在每个目标客户端进行主动安全防护，包括实现软件自保护、文件主动安全防护、数据加密、审计信息处理、心跳数据上报、关键资源保护、白名单采集，通过多个方面的保护可以提高客户端的安全性能，使得客户端能够安全运行，保证客户端的安全。

[0053] 图2是根据本发明实施例的一种可选的客户端的安全防护装置的示意图，如图2所示，该安全防护装置可以包括：获取单元21，确定单元23，保护单元25，其中，

[0054] 获取单元21，用于在检测目标客户端启动系统基础服务后，获取待保护的目标文件，其中，目标文件为目标客户端中安装的可信防护软件所对应的安装文件，可信防护软件用于为目标客户端提供主动安全防护服务；

[0055] 确定单元23，用于确定与目标文件对应的第一权限信息；

[0056] 保护单元25，用于基于第一权限信息，对目标文件和/或可信防护软件对应的进程进行安全防护。

[0057] 上述客户端的安全防护装置，可以通过获取单元21采用在检测目标客户端启动系统基础服务后，获取待保护的目标文件，其中，目标文件为目标客户端中安装的可信防护软件所对应的安装文件，可信防护软件用于为目标客户端提供主动安全防护服务，并通过确定单元23确定与目标文件对应的第一权限信息，然后通过保护单元25基于第一权限信息，对目标文件和/或可信防护软件对应的进程进行安全防护。在该实施例中，可以通过可信防护软件实现主动安全防护，对需要存储的文件实现全面且稳定的安全保护，并对自己的软件进程进行自保护，防止非法篡改或删除，提高文件的安全性，能够让用户实时了解到自己所使用的客户端的安全状态，提高用户使用可信防护软件的满意度，从而解决相关技术中客户端采用的安全防护软件仅仅能进行被动防御，无法保证内部存储的文件的安全性的技术问题。

[0058] 可选的，客户端的安全防护装置还包括：第一确定模块，用于在启动可信防护软件后，获取目标客户端中的关键资源文件；第一获取模块，用于获取与关键资源文件对应的第二权限信息；第一配置模块，用于基于资源权限，对关键资源文件进行权限配置；第一保护模块，用于基于第二权限信息，对关键资源文件进行安全保护。

[0059] 可选的，关键资源文件包括下述至少之一：系统注册表、系统核心文件。

[0060] 可选地，安全防护装置还包括：拦截模块，用于在目标客户端检测到注册表访问行为时，拦截注册表访问行为；对比模块，用于将注册表访问行为对应的访问注册表的路径与注册表访问策略进行对比；允许模块，用于在注册表访问策略中没有规定注册表访问行为对应的访问注册表的路径时，允许注册表访问行为执行；禁止模块，用于在注册表访问策略中规定了注册表访问行为对应的访问注册表的路径时，禁止注册表访问行为执行。

[0061] 另一种可选的，客户端的安全防护装置还包括：第一遍历模块，用于在启动可信防护软件后，遍历目标客户端上的磁盘，得到所有磁盘文件；第一识别模块，用于从所有磁盘文件中识别出目标客户端当前运行环境中的可执行文件和支持脚本；第一存储模块，用于将可执行文件和与支持脚本对应的哈希值存入系统白名单；第二保护模块，用于基于系统白名单对目标客户端实现主动安全防护。

[0062] 作为本发明可选的实施例，客户端的安全防护装置还包括：第一接收模块，用于在启动可信防护软件之后，接收与目标客户端远程连接的管理中心传输的软件安装策略；第一采集模块，用于按照软件安装策略安装管理中心传输的软件包，并采集软件包安装过程中产生的白名单；第一发送模块，用于将采集到的白名单发送给管理中心，管理中心用于将白名单与软件安装策略对应存储。

[0063] 可选的，客户端的安全防护装置还包括：第二发送模块，用于目标客户端每隔预定时间段向与目标客户端远程连接的管理中心发送心跳数据，其中，心跳数据中携带有目标客户端的相关信息；第二接收模块，用于目标客户端接收管理中心在接收到心跳数据之后返回的通知消息，其中，通知消息用于通知目标客户端从管理中心获取目标策略；第二配置模块，用于目标客户端从管理中心获取并解析目标策略，并配置给内核；第三发送模块，用于目标客户端想管理中心发送确认消息，其中，确认消息用于通知管理中心目标策略已生效。

[0064] 可选的，客户端的安全防护装置还包括：加密模块，用于对目标客户端与管理中心之间的通信数据进行加密处理，其中，在进行加密处理时的加密算法至少包括：国密SM算

法。

[0065] 上述的客户端的安全防护装置还可以包括处理器和存储器，上述获取单元21，确定单元23，保护单元25等均作为程序单元存储在存储器中，由处理器执行存储在存储器中的上述程序单元来实现相应的功能。

[0066] 上述处理器中包含内核，由内核去存储器中调取相应的程序单元。内核可以设置一个或以上，通过调整内核参数来对目标客户端进行主动安全防护。

[0067] 上述存储器可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)，存储器包括至少一个存储芯片。

[0068] 根据本发明实施例的另一方面，还提供了一种终端设备，包括：存储器，与存储器耦合的处理器，存储器和处理器通过总线系统相通信；存储器用于存储程序，其中，程序在被处理器执行时控制存储器所在设备执行上述任意一项的客户端的安全防护方法，处理器用于运行程序，其中，程序运行时执行上述任意一项的客户端的安全防护方法。

[0069] 根据本发明实施例的另一方面，还提供了一种处理器，处理器用于运行程序，其中，程序运行时执行上述任意一项的客户端的安全防护方法。

[0070] 本申请还提供了一种计算机程序产品，当在数据处理设备上执行时，适于执行初始化有如下方法步骤的程序：在检测目标客户端启动系统基础服务后，获取待保护的目标文件，其中，目标文件为目标客户端中安装的可信防护软件所对应的安装文件，可信防护软件用于为目标客户端提供主动安全防护服务；确定与目标文件对应的第一权限信息；基于第一权限信息，对目标文件和/或可信防护软件对应的进程进行安全防护。

[0071] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0072] 在本发明的上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0073] 在本申请所提供的几个实施例中，应该理解到，所揭露的技术内容，可通过其它的方式实现。其中，以上所描述的装置实施例仅仅是示意性的，例如所述单元的划分，可以为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，单元或模块的间接耦合或通信连接，可以是电性或其它的形式。

[0074] 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单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0075] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0076] 所述集成的单元如果以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全部或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(可为个人计算机、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、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0077] 以上所述仅是本发明的优选实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也应视为本发明的保护范围。

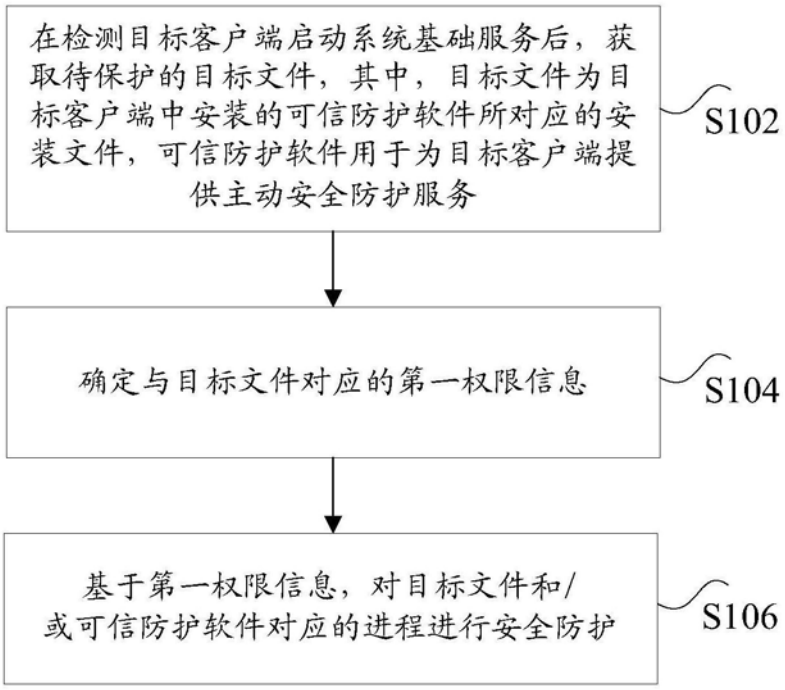

在检测目标客户端启动系统基础服务后，获取待保护的目标文件，其中，目标文件为目标客户端中安装的可信防护软件所对应的安装文件，可信防护软件用于为目标客户端提供主动安全防护服务
S102
确定与目标文件对应的第一权限信息
S104
基于第一权限信息，对目标文件和/或可信防护软件对应的进程进行安全防护
S106

图1


获取单元21
确定单元23
保护单元25

图2