

# 说明书

## 发明名称：控制终端关闭的方法和系统、计算机存储介质

- [1] 本申请要求于2012年06月11日提交中国专利局、申请号为201210190831.0、发明名称为“控制终端关闭的方法和系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。
- [2] **【技术领域】**
- [3] 本发明涉及安全检测技术，特别是涉及一种控制终端关闭的方法和系统、计算机存储介质。
- [4] **【背景技术】**
- [5] 终端的关闭一般由终端的操作系统所控制。传统的控制终端关闭的方法通常是在检测到关机指令时，弹出关闭终端的对话框，包括待机、关闭和重新启动的选项，当用户选择关闭时，则直接将终端关闭。
- [6] 终端在使用一段时间后，往往会出现一些安全隐患。例如，受到木马病毒入侵、存在系统漏洞、软件需要升级等。终端在关闭的时候很可能处于病毒入侵、性能状况不良的状态。然而，传统的这种控制终端关闭的方式，由于是直接终端关闭，终端在下一次运行时很可能会处于不安全的环境中，也会影响终端下一次的启动速度、运行速度等。
- [7] **【发明内容】**
- [8] 基于此，有必要针对传统的控制终端关闭的方法会影响到终端下一次运行的安全性的问题，提供一种能提高安全性的控制终端关闭的方法。
- [9] 一种控制终端关闭的方法，包括以下步骤：拦截关机操作；根据预设的安全检测项执行对应的安全检测；对安全隐患进行对应处理，并在处理结束后关闭终端。
- [10] 此外，还有必要提供一种能提高安全性的控制终端关闭的系统。
- [11] 一种控制终端关闭的系统，包括：拦截模块，用于拦截关机操作；安全检测模块，用于根据预设的安全检测项执行对应的安全检测；安全关机模块，用于对安全隐患进行对应处理，并在处理结束后关闭终端。

- [12] 另外，还有必提供一个或多个能提高安全性的计算机存储介质。
- [13] 一个或多个包含计算机可执行指令的计算机存储介质，所述计算机可执行指令用于执行一种控制终端关闭的方法，所述方法包括以下步骤：
- [14] 拦截关机操作；
- [15] 根据预设的安全检测项执行对应的安全检测；
- [16] 对安全隐患进行对应处理，并在处理结束后关闭终端。
- [17] 上述控制终端关闭的方法和系统、计算机存储介质，在终端关闭时拦截关机操作，根据预设的安全检测项执行安全检测，并对安全隐患进行对应处理，在处理结束后才关闭终端。由于在终端关闭前处理了终端可能存在的一些安全隐患，能够提高终端的安全性，使得终端在下一次运行时处于更加安全的环境中，也改善了终端下一次的启动速度、运行速度等。
- [18] **【附图说明】**
- [19] 图1为一个实施例中控制终端关闭的方法的流程示意图；
- [20] 图2为一种操作系统中的安全关机选择界面的示意图；
- [21] 图3为一种操作系统中的安全关机操作界面的示意图；
- [22] 图4为一种操作系统中的安全关机处理界面的示意图；
- [23] 图5为一个实施例中控制终端关闭的系统的结构框图；
- [24] 图6为一个实施例中安全关机模块的结构框图；
- [25] 图7为另一个实施例中的安全关机模块的结构框图。
- [26] **【具体实施方式】**
- [27] 如图1所示，在一个实施例中，一种控制终端关闭的方法，包括以下步骤：
- [28] 步骤S102，拦截关机操作。
- [29] 进一步的，在一个实施例中，当触发关机操作时，需截取关机进程，调用安全检测进程，通过安全检测进程执行安全检测，待安全检测完成并对终端中的安全隐患进行对应处理后，再激活关机进程，从而关闭终端。
- [30] 在一个实施例中，当监测到关机指令时则拦截关机操作。该方式为自动拦截方式，即当用户一触发关机则拦截关机操作。
- [31] 在另一个实施例中，当监测到关机指令时进入安全关机选择界面，通过所述安

全关机选择界面获取安全关机指令，拦截关机操作。具体的，安全关机指令可以是通过安全关机选择界面选择的安全关机下拉列表项或安全关机按钮或安全关机扩展菜单项所生成的指令。该方式为用户触发拦截方式，即当用户触发关机后需选择预设的安全关机下拉列表项或安全关机按钮或安全关机扩展菜单项才拦截关机操作。

[32] 具体的，对于运行在终端上的不同的操作系统，设置安全关机选项的方式也有所不同。例如，可在原有的终端关闭选择界面中插入安全关机按钮，生成安全关机选择界面。进一步的，可通过HOOK调用的对话框函数，更改传入的对话框模板资源，并修改窗体过程函数，完成安全关机入口的按钮创建及响应。

[33] 如图2所示，为一种操作系统中的安全关机选择界面，当监测到用户触发的关机指令时，则进入到该安全关机选择界面，在该安全关机选择界面中包含了预设的安全关机按钮，用户点击该安全关机按钮，则拦截关机操作。对于其他类型的操作系统（如andriod、Mac OS系统等），则可在安全关机选择界面中创建安全关机下拉列表项或安全关机扩展菜单项。

[34] 步骤S104，根据预设的安全检测项执行对应的安全检测。

[35] 在一个实施例中，预设的安全检测项包括木马查杀、清理垃圾、清除痕迹、修补漏洞、安全体检和软件升级中的至少一种。

[36] 不同的安全检测项对应设置了不同的安全检测。具体的，在一个实施例中，步骤S104具体为：根据预设的安全检测项读取和/或扫描注册表；和/或根据预设的安全检测项扫描终端关键位置。

[37] 对于一些安全检测项，需读取注册表。例如，当预设的安全检测项包括软件升级，则读取软件注册表，获取软件当前的版本号，根据软件当前的版本号判断软件是否需要升级。

[38] 对于一些安全检测项，则需要扫描注册表和/或终端关键位置。终端关键位置包括但不限于木马病毒常存在的文件夹、注册表位置、常用软件垃圾产生的文件夹等。可在设置安全检测项时预先设置对应的终端关键位置。例如，当预设的安全检测项包括木马查杀，则扫描注册表和/或终端关键位置，当扫描到木马病毒时，生成扫描结果。当预设的安全检测项包括清除垃圾，则扫描常用软件

垃圾产生的文件夹，获取扫描到的垃圾文件，生成扫描结果。

[39] 步骤S106，对安全隐患进行对应处理，并在处理结束后关闭终端。

[40] 在一个实施例中，步骤S106具体包括：根据预设的安全检测结果与安全关机方式的对应关系获取与安全检测得到的结果对应的安全关机方式；通过安全关机操作界面展示获取的安全关机方式。

[41] 本实施例中，预先设置了不同的安全检测结果对应了不同的安全关机方式。例如，当扫描到木马病毒时可提醒用户进行木马病毒的查杀后再关闭终端；当检测到软件还有更新版本时可提醒用户进行软件升级后再关闭终端；当检测到操作系统存在漏洞时可提醒用户修复漏洞后再关闭终端；当检测到终端关键位置存在垃圾文件时可提醒用户清除垃圾后再关闭终端等等。进一步的，可通过安全关机操作界面展示安全关机方式。

[42] 如图3所示，为一种操作系统的安全关机操作界面，在该安全关机操作界面上展示了获取的与生成的安全检测结果对应的安全关机方式，包括全盘查杀木马病毒和清除痕迹的选项。用户可以通过选择相应的安全关机方式，并点击安全关机按钮，则可根据用户选择的安全关机方式对安全隐患进行处理。

[43] 在一个实施例中，步骤S106还包括：获取通过安全关机操作界面选择的安全关机方式，根据选择的安全关机方式对安全隐患进行处理，并在处理结束后关闭终端。

[44] 如图3所示，当用户选择全盘查杀病毒木马的选项并点击安全关机按钮时，则对终端进行全盘查杀病毒木马，在查杀结束后再关闭终端。在用户点击安全关机按钮后，由于终端在病毒木马查杀结束后会自动关闭，不会影响终端的其他应用程序的运行，也不会浪费用户时间。

[45] 在一个实施例中，还可在安全关机操作界面中设置直接关机按钮，用户点击该直接关机按钮，则跳过安全关机方式，直接控制终端关闭。如图4所示，在对终端的安全隐患进行处理的过程中，可通过安全关机处理界面提示用户正在进行处理安全隐患，处理结束后自动关闭终端，还可在该界面中设置直接关机选项，方便用户中断处理过程，直接关闭终端。在此说明的是，图4仅仅是一个实施例所提供的一种安全关机处理界面，并不用于限制本发明。

- [46] 在另一个实施例中，步骤S106还可包括：若检测到在设定时间内未获取到选择的安全关机方式，则在设定时间后自动选择安全关机方式，根据该选择的安全关机方式对安全隐患进行处理，并在处理结束后关闭终端。
- [47] 所述的设定时间可以设置为10秒、15秒、20秒或1分钟等。本实施例中，当通过安全关机操作界面展示安全关机方式后，若用户在该设定时间内未选择安全关机，则可根据默认设置自动选择安全关机方式。如图3所示，可自动选择全盘查杀病毒木马和清除痕迹后，对终端进行全盘查杀病毒木马和清除痕迹后再关闭终端。
- [48] 在一个实施例中，也可根据默认设置自动为用户选择安全关机方式，由用户确认是否按照默认设置自动选择的安全关机方式进行关机。
- [49] 具体的，可在安全关机操作界面中设置默认设置的设置界面，用户可通过该设置界面设置默认的安全关机方式，当检测到在设定时间内未获取到用户选择的安全关机方式时，则可按照默认设置中的安全关机方式对安全隐患进行处理，并在处理结束后关闭终端。
- [50] 在一个实施例中，还可在安全关机操作界面中设置始终按推荐安全关机方式关机的选项。如图3所示，当用户选择“不再提醒，安全关机均按此执行”的选项时，则在以后终端拦截到关机操作后，则无需用户再参与选择，终端会根据安全检测结果自动为用户选择对应的安全关机方式。本实施例可以自动对终端进行安全检测并对安全隐患进行处理，无需用户主动发起安全检测，节省了用户操作成本和操作时间。
- [51] 如图5所示，在一个实施例中，一种控制终端关闭的系统，包括拦截模块100、安全检测模块200和安全关机模块300，其中：
- [52] 拦截模块100用于拦截关机操作。
- [53] 进一步的，在一个实施例中，拦截模块100当触发关机操作时截取关机进程。通过安全检测模块200调用安全检测进程，通过安全检测进程执行安全检测，待安全检测完成并对终端中的安全隐患进行对应处理后，安全关机模块300再激活关机进程，从而关闭终端。
- [54] 在一个实施例中，拦截模块100用于当监测到关机指令时则拦截关机操作。该

方式为自动拦截方式，即当用户一触发关机则拦截关机操作。

- [55] 在另一个实施例中，拦截模块100用于当监测到关机指令时进入安全关机选择界面，通过所述安全关机选择界面获取安全关机指令，拦截关机操作。具体的，安全关机指令可以是通过安全关机选择界面选择的安全关机下拉列表项或安全关机按钮或安全关机扩展菜单项所生成的指令。该方式为用户触发拦截方式，即当用户触发关机后需选择预设的安全关机下拉列表项或安全关机按钮或安全关机扩展菜单项才拦截关机操作。
- [56] 安全检测模块200用于根据预设的安全检测项执行对应的安全检测。
- [57] 在一个实施例中，安全检测项包括木马查杀、清理垃圾、清除痕迹、修复漏洞、安全体检和软件升级中的至少一种。
- [58] 不同的安全检测项对应设置了不同的安全检测。进一步的，在一个实施例中，安全检测模块200用于根据预设的安全检测项读取和/或扫描注册表；和/或根据预设的安全检测项扫描终端关键位置。
- [59] 安全关机模块300用于对安全隐患进行对应处理，并在处理结束后关闭终端。
- [60] 在一个实施例中，如图6所示，安全关机模块300包括安全关机方式获取模块310、安全关机方式展示模块320和第一终端关闭控制模块330，其中：
- [61] 安全关机方式获取模块310用于根据预设的安全检测结果与安全关机方式的对应关系获取与安全检测得到的结果对应的安全关机方式。
- [62] 安全关机方式展示模块320用于通过安全关机操作界面展示安全关机方式。
- [63] 第一终端关机控制模块330用于获取通过所述安全关机操作界面选择的安全关机方式，根据选择的安全关机方式对安全隐患进行处理，并在处理结束后关闭终端。
- [64] 在另一个实施例中，如图7所示，安全关机模块300包括上述安全关机方式获取模块310和安全关机方式展示模块320外，还包括第二终端关闭控制模块340，其中：
- [65] 第二终端关闭控制模块430用于若检测到在设定时间内未获取到选择的安全关机方式，则在设定时间后自动选择安全关机方式，根据该选择的安全关机方式对安全隐患进行处理，并在处理结束后关闭终端。

- [66] 在其他实施例中，安全关机模块300还可同时包括上述安全关机方式获取模块310、安全关机方式展示模块320、第一终端关闭控制模块330和第二终端关闭控制模块340。
- [67] 在一个实施例中，还可在安全关机操作界面中设置始终按推荐安全关机方式关机的选项。则在以后终端拦截到关机操作后，无需用户再参与选择，终端会根据安全检测结果自动为用户选择对应的安全关机方式。本实施例可以自动对终端进行安全检测并对安全隐患进行处理，无需用户主动发起安全检测，节省了用户操作成本和操作时间。
- [68] 上述控制终端关闭的方法和系统，由于在终端关闭前处理了终端可能存在的一些安全隐患，能够提高终端的安全性，使得终端在下一次运行时处于更加安全的环境中，也改善了终端下一次的启动速度、运行速度等。
- [69] 此外，在终端关闭前处理安全隐患，安全隐患处理结束后自动关闭终端，相对于传统的在发现终端有安全隐患时用户再主动发起安全检测的方式，由于安全隐患的处理需要花费一定时间，在终端关闭时进行处理不会影响终端的其他应用程序的运行，更加节省时间成本。
- [70] 对于不同的操作系统，可在安全关机选择界面中设置安全关机下拉列表项或安全关机按钮或安全关机扩展菜单项实现拦截关闭操作，因此上述控制终端关闭的方法和系统适用于各种终端（如个人计算机、手机、平板电脑等）上运行的各种操作系统（如Windows、andriod、Mac OS等）。
- [71] 另外，通过设置安全关机选择界面和安全关机操作界面，提高了易用性，用户可以通过安全关机操作界面选择多种安全关机方式，也可以设置后续的终端关闭时的安全检测无需用户参与选择，节省了用户的操作成本和时间，提高了用户的体验需求。
- [72] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory, ROM）或随机存储记忆体（Random Access Memory, RAM）等。

[73] 以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对本发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明的保护范围应以所附权利要求为准。

## 权利要求书

- [权利要求 1] 一种控制终端关闭的方法，应用于终端，所述方法包括以下步骤：
- 拦截关机操作；
- 根据预设的安全检测项执行对应的安全检测；
- 对安全隐患进行对应处理，并在处理结束后关闭终端。
- [权利要求 2] 根据权利要求1所述的控制终端关闭的方法，其特征在于，所述拦截关机操作的步骤为：当监测到关机指令时则拦截关机操作。
- [权利要求 3] 根据权利要求1所述的控制终端关闭的方法，其特征在于，所述拦截关机操作的步骤为：当监测到关机指令时进入安全关机选择界面，通过所述安全关机选择界面获取安全关机指令，拦截关机操作。
- [权利要求 4] 根据权利要求1所述的控制终端关闭的方法，其特征在于，所述预设的安全检测项包括木马查杀、清理垃圾、清除痕迹、修复漏洞、安全体检和软件升级中的至少一种。
- [权利要求 5] 根据权利要求4所述的控制终端关闭的方法，其特征在于，所述根据预设的安全检测项执行对应的安全检测的步骤为：
- 根据预设的安全检测项读取和/或扫描注册表；和/或
- 根据预设的安全检测项扫描终端关键位置。
- [权利要求 6] 根据权利要求1所述的控制终端关闭的方法，其特征在于，所述对安全隐患进行对应处理，并在处理结束后关闭终端的步骤包括：
- 根据预设的安全检测结果与安全关机方式的对应关系获取与所述安全检测得到的结果对应的安全关机方式；
- 通过安全关机操作界面展示所述安全关机方式。
- [权利要求 7] 根据权利要求6所述的控制终端关闭的方法，其特征在于，所述根据安全检测结果对安全隐患进行处理，并在处理结束后关闭终端的步骤还包括：
- 获取通过所述安全关机操作界面选择的安全关机方式，根据所述

选择的安全关机方式对安全隐患进行处理，并在处理结束后关闭终端。

[权利要求 8] 根据权利要求6所述的控制终端关闭的方法，其特征在于，所述对安全隐患进行对应处理，并在处理结束后关闭终端的步骤还包括：

若检测到在设定时间内未获取到选择的安全关机方式，则在所述设定时间后自动选择安全关机方式，根据所述选择的安全关机方式对安全隐患进行处理，并在处理结束后关闭终端。

[权利要求 9] 一种控制终端关闭的系统，运行于终端，其特征在于，所述系统包括：

拦截模块，用于拦截关机操作；

安全检测模块，用于根据预设的安全检测项执行对应的安全检测；

安全关机模块，用于对安全隐患进行对应处理，并在处理结束后关闭终端。

[权利要求 10] 根据权利要求9所述的控制终端关闭的系统，其特征在于，所述拦截模块用于当监测到关机指令时则拦截关机操作。

[权利要求 11] 根据权利要求9所述的控制终端关闭的系统，其特征在于，所述拦截模块用于当监测到关机指令时进入安全关机选择界面，通过所述安全关机选择界面获取安全关机指令，拦截关机操作。

[权利要求 12] 根据权利要求9所述的控制终端关闭的系统，其特征在于，所述预设的安全检测项包括木马查杀、清理垃圾、清除痕迹、修复漏洞、安全体检和软件升级中的至少一种。

[权利要求 13] 根据权利要求12所述的控制终端关闭的系统，其特征在于，所述安全检测模块用于根据预设的安全检测项读取和/或扫描注册表；和/或根据预设的安全检测项扫描终端关键位置。

[权利要求 14] 根据权利要求9所述的控制终端关闭的系统，其特征在于，所述安全关机模块包括：

安全关机方式获取模块，用于根据预设的安全检测结果与安全关机方式的对应关系获取与所述安全检测得到的结果对应的安全关机方式；

安全关机方式展示模块，用于通过安全关机操作界面展示所述安全关机方式。

[权利要求 15] 根据权利要求14所述的控制终端关闭的系统，其特征在于，所述安全关机模块还包括：

第一终端关闭控制模块，用于获取通过所述安全关机操作界面选择的安全关机方式，根据所述选择的安全关机方式对安全隐患进行处理，并在处理结束后关闭终端。

[权利要求 16] 根据权利要求14所述的控制终端关闭的系统，其特征在于，所述安全关机模块还包括：

第二终端关闭控制模块，用于若检测到在设定时间内未获取到选择的安全关机方式，则在所述设定时间后自动选择安全关机方式，根据所述选择的安全关机方式对安全隐患进行处理，并在处理结束后关闭终端。

[权利要求 17] 一个或多个包含计算机可执行指令的计算机存储介质，所述计算机可执行指令用于执行一种控制终端关闭的方法，其特征在于，所述方法包括以下步骤：

拦截关机操作；

根据预设的安全检测项执行对应的安全检测；

对安全隐患进行对应处理，并在处理结束后关闭终端。

[权利要求 18] 根据权利要求17所述的计算机存储介质，其特征在于，所述拦截关机操作的步骤为：当监测到关机指令时则拦截关机操作。

[权利要求 19] 根据权利要求17所述的计算机存储介质，其特征在于，所述拦截关机操作的步骤为：当监测到关机指令时进入安全关机选择界面，通过所述安全关机选择界面获取安全关机指令，拦截关机操作。

- [权利要求 20] 根据权利要求17所述的计算机存储介质，其特征在于，所述预设的安全检测项包括木马查杀、清理垃圾、清除痕迹、修复漏洞、安全体检和软件升级中的至少一种。
- [权利要求 21] 根据权利要求20所述的计算机存储介质，其特征在于，所述根据预设的安全检测项执行对应的安全检测的步骤为：  
根据预设的安全检测项读取和/或扫描注册表；和/或  
根据预设的安全检测项扫描终端关键位置。
- [权利要求 22] 根据权利要求17所述的计算机存储介质，其特征在于，所述对安全隐患进行对应处理，并在处理结束后关闭终端的步骤包括：  
根据预设的安全检测结果与安全关机方式的对应关系获取与所述安全检测得到的结果对应的安全关机方式；  
通过安全关机操作界面展示所述安全关机方式。
- [权利要求 23] 根据权利要求22所述的计算机存储介质，其特征在于，所述根据安全检测结果对安全隐患进行处理，并在处理结束后关闭终端的步骤还包括：  
获取通过所述安全关机操作界面选择的安全关机方式，根据所述选择的安全关机方式对安全隐患进行处理，并在处理结束后关闭终端。
- [权利要求 24] 根据权利要求22所述的计算机存储介质，其特征在于，所述对安全隐患进行对应处理，并在处理结束后关闭终端的步骤还包括：  
若检测到在设定时间内未获取到选择的安全关机方式，则在所述设定时间后自动选择安全关机方式，根据所述选择的安全关机方式对安全隐患进行处理，并在处理结束后关闭终端。