(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 104580135 A
(43)申请公布日 2015.04.29

(21)申请号 201410457596.8

(22)申请日 2014.09.10

(71)申请人 中电科技（北京）有限公司
地址 100083 北京市海淀区卧虎桥甲 6 号工作区（南）太极大厦 13 层北侧

(72)发明人 陈小春 孙亮 张超 朱立森

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
G06F 9/445(2006.01)
G06F 9/44(2006.01)
G06F 21/57(2013.01)
G06F 11/30(2006.01)

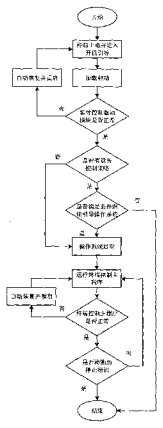
权利要求书1页 说明书4页 附图3页

(54)发明名称

一种基于UEFI的终端实时控制系统和方法

(57)摘要

本发明公开了一种基于UEFI的终端实时控制系统和方法，属于计算机安全技术领域。系统包括终端实时控制驱动模块、终端控制主程序和终端实时控制系统服务端；终端实时控制驱动模块包括自我恢复子模块、控制指令解析子模块、控制指令执行子模块和操作系统及网络接口子模块；终端控制主程序包括运行状态交互接口子模块、终端控制策略执行子模块、通信接口子模块、定时子模块；终端实时控制系统服务端包括终端控制服务、策略管理服务和终端信息展示服务。本发明能解决在开机引导过程中和操作系统启动后，无法在固件层对终端进行实时控制的问题。



CN 104580135 A

1. 一种基于 UEFI 的终端实时控制系统，其特征在于，所述系统包括终端实时控制驱动模块、终端控制主程序和终端实时控制系统服务端；

所述终端实时控制驱动模块是在固件层控制终端的驱动模块，包括自我恢复子模块、控制指令解析子模块、控制指令执行子模块、操作系统及网络接口子模块四个部分；其中，自动恢复子模块用于对实时终端控制驱动模块和终端控制主程序进行恢复，控制策略解析用于对接收到的控制指令进行辨析，明确需要执行哪些终端控制指令；控制指令执行模块用于执行相应的控制指令；操作系统及网络接口子模块用于提供终端实时控制系统驱动模块与操作系统中终端控制主程序的数据交互接口，以及终端控制主程序与服务端的数据交互接口；终端实时控制驱动模块可以通过操作系统中的终端控制主程序进行控制，也可以通过系统中断自动调用；

所述终端控制主程序运行于操作系统，接收和执行服务端指令；终端控制主程序包括运行状态交互接口子模块、终端控制策略执行子模块、通信接口子模块、定时子模块；运行状态交互接口子模块用于终端控制主程序与终端实时控制驱动模块进行状态交互；通信接口子模块用于终端控制主程序与服务器进行网络通信；终端控制策略执行子模块用于执行从服务器接收到的指令；定时子模块用于在指定的时间间隔内，调用终端实时控制系统驱动模块；

所述终端实时控制系统服务端包括终端控制服务、策略管理服务和终端信息展示服务；其中，终端控制服务用于向客户端发送相应的控制指令；策略管理服务用于制定终端控制策略；终端信息展示用于展示当前接入终端的状态。

2. 如权利要求 1 所述的基于 UEFI 的终端实时控制系统，其特征在于，系统的实现过程如下：

步骤一、计算机终端开机上电后，开始进入 UEFI 的开机引导过程，操作系统启动；

步骤二、在固件层加载所需的驱动；

步骤三、在固件层检测实时驱动模块是否正常；如果正常则进入步骤四；如果驱动模块出现异常，则自动进行恢复和重启；

步骤四、检测是否已有对终端进行控制的策略；如果已有既定控制策略，则转入步骤五；否则直接启动操作系统；

步骤五、执行既定的终端控制策略；

步骤六、启动操作系统；

步骤七、终端控制主程序自动运行；

步骤八、检测终端控制主程序运行状态是否正确；如果正常转入步骤九，否则自动恢复并重启；

步骤九、如果未检测到停止标识，则继续执行；如果检测到停止标识，则终端实时控制流程结束。

一种基于 UEFI 的终端实时控制系统和方法

技术领域

[0001] 本发明属于计算机安全技术领域，涉及一种基 UEFI 固件，在开机引导过程中和操作系统启动后，对终端进行实时控制的系统和方法。

背景技术

[0002] 目前，在计算机安全和通信领域，对计算机终端的控制主要通过服务器远程发布控制指令，由运行于客户端操作系统上的特定程序进行接收和执行，也有直接通过简单控制电路对终端进行控制。在操作系统层对应用程序进行实时保护，特别是对关键终端控制程序进行保护，有着以下的不足，主要包括：

[0003] 在计算机终端更换硬盘、Flash 等存储被保护程序的装置后，将不能自动地恢复终端控制程序，对终端进行监控。

[0004] 在对硬盘、Flash 等被保护程序的存储空间进行重新分区后，计算机终端将不能自动地恢复终端控制程序，对终端进行监控。

[0005] 在对硬盘、Flash 等被保护程序的存储空间进行格式化后，计算机终端将不能自动地恢复终端控制程序，对终端进行监控。

[0006] 当被保护可执行程序文件不属于操作系统自带软件的情况下，在计算机终端重新安装操作系统后，将不能自动地恢复终端控制程序，对计算机终端进行监控。

[0007] 当终端的操作系统中的特定终端控制软件被病毒或木马篡改和删除后，将不能自动地进行恢复，此外，在操作系统中运行的终端控制软件有可能被终端用户非授权地中止。

发明内容

[0008] 有本发明的目的是为了克服已有技术的缺陷，为了解决在开机引导过程中和操作系统启动后，无法在固件层对终端进行实时控制的问题，提出一种基于 UEFI 的终端实时控制系统和方法。

[0009] 一种基于 UEFI 的终端实时控制系统，包括终端实时控制驱动模块、终端控制主程序和终端实时控制系统服务端；

[0010] 所述终端实时控制系统的终端实时控制驱动模块是在固件层控制终端的驱动模块，主要包括自我恢复子模块、控制指令解析子模块、控制指令执行子模块、操作系统及网络接口子模块四个部分；其中，自动恢复子模块用于对实时终端控制驱动模块和终端控制主程序进行恢复，控制策略解析用于对接收到的控制指令进行辨析，明确需要执行哪些终端控制指令；控制指令执行模块用于执行相应的控制指令；操作系统及网络接口子模块用于提供终端实时控制系统驱动模块与操作系统中终端控制主程序的数据交互接口，以及终端控制主程序与服务端的数据交互接口；终端实时控制驱动模块可以通过操作系统中的终端控制主程序进行控制，也可以通过系统中断自动调用；

[0011] 所述终端实时控制系统的终端控制主程序，终端控制主程序运行于操作系统，接收和执行服务端指令；终端控制主程序包括运行状态交互接口子模块、终端控制策略执行

子模块、通信接口子模块、定时子模块；运行状态交互接口子模块用于终端控制主程序与终端实时控制驱动模块进行状态交互；通信接口子模块用于终端控制主程序与服务器进行网络通信；终端控制策略执行子模块用于执行从服务器接收到的指令；定时子模块用于在指定的时间间隔内，调用终端实时控制系统驱动模块；

[0012] 所述终端实时控制系统的终端实时控制系统服务端包括终端控制服务、策略管理服务和终端信息展示服务；其中，终端控制服务用于向客户端发送相应的控制指令；策略管理服务用于制定终端控制策略；终端信息展示用于展示当前接入终端的状态。

[0013] 所述一种基于 UEFI 的终端实时控制系统的实现过程如下：

[0014] 步骤一、计算机终端开机上电后，开始进入 UEFI 的开机引导过程，操作系统启动；

[0015] 步骤二、在固件层加载所需的驱动；

[0016] 步骤三、在固件层检测实时驱动模块是否正常；如果正常则进入步骤四；如果驱动模块出现异常，则自动进行恢复和重启；

[0017] 步骤四、检测是否已有对终端进行控制的策略；如果已有既定控制策略，则转入步骤五；否则直接启动操作系统；

[0018] 步骤五、执行既定的终端控制策略；

[0019] 步骤六、启动操作系统；

[0020] 步骤七、终端控制主程序自动运行；

[0021] 步骤八、检测终端控制主程序运行状态是否正确；如果正常转入步骤九，否则自动恢复并重启；

[0022] 步骤九、如果未检测到停止标识，则继续执行；如果检测到停止标识，则终端实时控制流程结束。

[0023] 有益效果：

[0024] 1、本发明在计算机终端更换硬盘、Flash 等存储被保护程序的装置后，能够自动地重新恢复终端控制程序，对终端进行实时监控。

[0025] 2、在对硬盘、Flash 等被保护程序的存储空间进行重新分区后，计算机终端将能够自动地恢复终端控制程序，对终端进行实时监控。

[0026] 3、在对硬盘、Flash 等被保护程序的存储空间进行格式化后，计算机终端将能够自动地重新恢复终端控制程序，对终端进行实时监控。

[0027] 4、在计算机终端重新安装操作系统后，能够自动地重新恢复终端控制程序，对终端进行实时监控。当终端控制软件被病毒或木马篡改和删除后，能够自动地进行恢复。在用户卸载终端控制软件后，将能够自动恢复终端控制软件，并对终端进行实时监控。

附图说明

[0028] 图 1 为基于 UEFI 的终端实时控制总体框架图。

[0029] 图 2 为终端实时控制系统框架图。

[0030] 图 3 为终端实时控制流程图。

具体实施方式

[0031] 下面结合附图并举实施例，对本发明进行详细描述。

[0032] 如附图 1 所示，本发明的一种基于 UEFI 的终端实时控制系统，包括终端实时控制驱动模块、终端控制主程序和终端实时控制系统服务端；

[0033] 如附图 2 所示，所述终端实时控制系统的终端实时控制驱动模块是在固件层控制终端的驱动模块，主要包括自我恢复子模块、控制指令解析子模块、控制指令执行子模块、操作系统及网络接口子模块四个部分；其中，自动恢复子模块用于对实时终端控制驱动模块和终端控制主程序进行恢复，控制策略解析用于对接收到的控制指令进行辨析，明确需要执行哪些终端控制指令；控制指令执行模块用于执行相应的控制指令；操作系统及网络接口子模块用于提供终端实时控制系统驱动模块与操作系统中终端控制主程序的数据交互接口，以及终端控制主程序与服务端的数据交互接口；终端实时控制驱动模块可以通过操作系统中的终端控制主程序进行控制，也可以通过系统中断自动调用；

[0034] 所述终端实时控制系统的终端控制主程序，终端控制主程序运行于操作系统，接收和执行服务端指令；终端控制主程序包括运行状态交互接口子模块、终端控制策略执行子模块、通信接口子模块、定时子模块；运行状态交互接口子模块用于终端控制主程序与终端实时控制驱动模块进行状态交互；通信接口子模块用于终端控制主程序与服务器进行网络通信；终端控制策略执行子模块用于执行从服务器接收到的指令；定时子模块用于在指定的时间间隔内，调用终端实时控制系统驱动模块；

[0035] 所述终端实时控制系统的终端实时控制系统服务端包括终端控制服务、策略管理服务和终端信息展示服务；其中，终端控制服务用于向客户端发送相应的控制指令；策略管理服务用于制定终端控制策略；终端信息展示用于展示当前接入终端的状态。

[0036] 本发明在应用前，需要在计算机终端先行部署，可以选用的方法包括：

[0037] (1) 在 UEFI 核心镜像中添加驱动模块。

[0038] (2) 在 UEFI 核心镜像中挂载 Option ROM 模块。

[0039] (3) 在可信卡等其他外围设备中挂载驱动模块。

[0040] 如附图 3 所示，本发明的一种基于 UEFI 的终端实时控制系统的实现过程如下：

[0041] 步骤一、计算机终端开机上电后，开始进入 UEFI 的开机引导过程，操作系统启动；

[0042] 步骤二、在固件层加载所需的驱动；

[0043] 步骤三、在固件层检测实时驱动模块是否正常；如果正常则进入步骤四；如果驱动模块出现异常，则自动进行恢复和重启；

[0044] 步骤四、检测是否已有对终端进行控制的策略；如果已有既定控制策略，则转入步骤五；否则直接启动操作系统；

[0045] 步骤五、执行既定的终端控制策略；

[0046] 步骤六、启动操作系统；

[0047] 步骤七、终端控制主程序自动运行；

[0048] 步骤八、检测终端控制主程序运行状态是否正确；如果正常转入步骤九，否则自动恢复并重启；

[0049] 步骤九、如果未检测到停止标识，则继续执行；如果检测到停止标识，则终端实时控制流程结束。

[0050] 综上所述，以上仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。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。

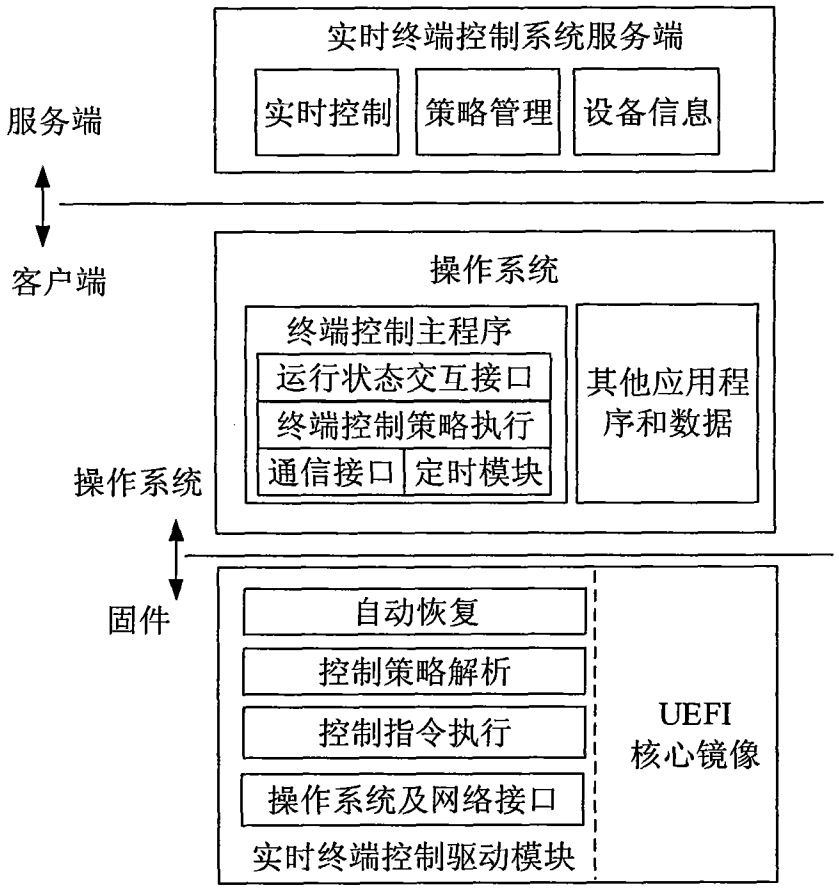

实时终端控制系统服务端
实时控制
策略管理
设备信息
服务端
客户端
操作系统
终端控制主程序
运行状态交互接口
终端控制策略执行
通信接口
定时模块
其他应用程序和数据
操作系统
固件
自动恢复
控制策略解析
控制指令执行
操作系统及网络接口
实时终端控制驱动模块
UEFI
核心镜像

图 1

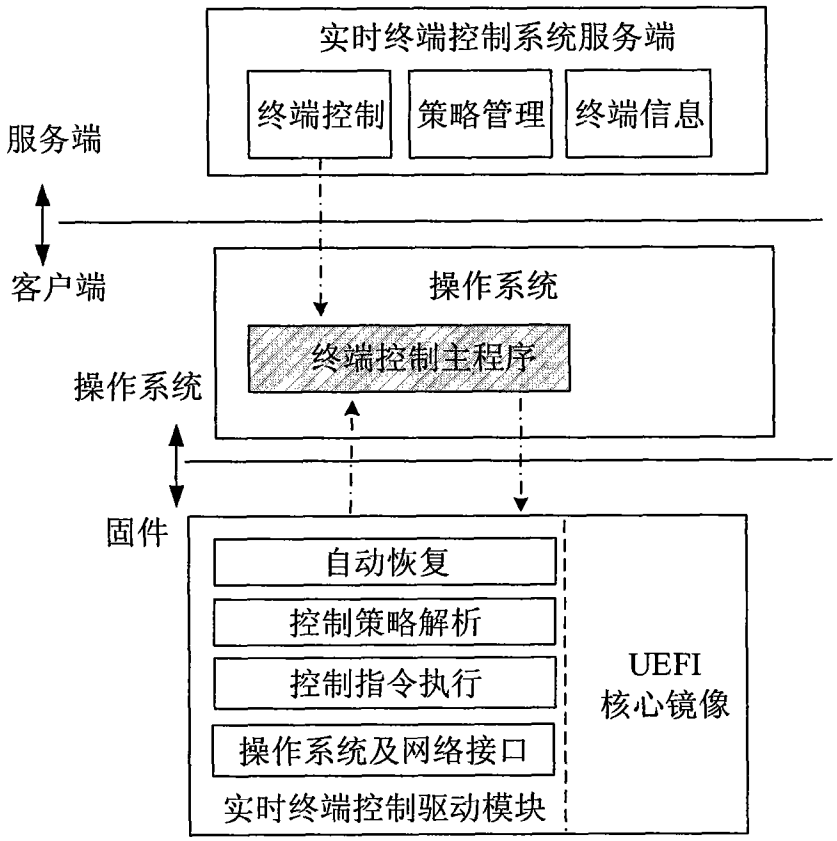

实时终端控制系统服务端
终端控制
策略管理
终端信息
服务端
客户端
操作系统
终端控制主程序
操作系统
固件
自动恢复
控制策略解析
控制指令执行
操作系统及网络接口
实时终端控制驱动模块
UEFI
核心镜像

图 2

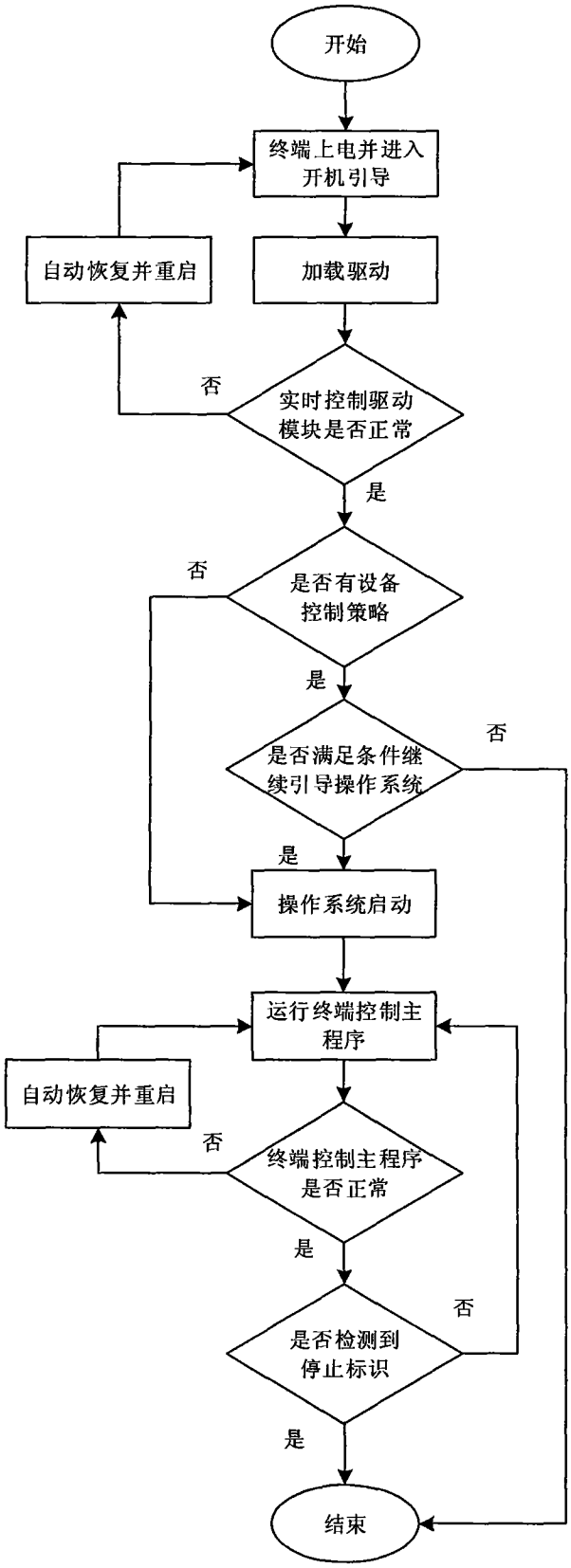

开始
终端上电并进入开机引导
加载驱动
实时控制驱动模块是否正常
否
自动恢复并重启
是
是否有设备控制策略
否
是
是否满足条件继续引导操作系统
否
是
操作系统启动
运行终端控制主程序
自动恢复并重启
终端控制主程序是否正常
否
是
是否检测到停止标识
否
是
结束

图 3