(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 103971057 B
(45)授权公告日 2017.12.19

(21)申请号 201410155911.1

(22)申请日 2014.04.17

(65)同一申请的已公布的文献号
申请公布号 CN 103971057 A

(43)申请公布日 2014.08.06

(73)专利权人 兴唐通信科技有限公司
地址 100191 北京市海淀区学院路40号

(72)发明人 王永利 高文博 夏捷 邱毅 刘国庆

(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 李迪

(51)Int.Cl.
G06F 21/57(2013.01)

(56)对比文件
CN 1702592 A,2005.11.30,说明书第2页倒数第2段,第3页第3-6段,图2.
CN 101154256 A,2008.04.02,说明书第0012-0013段.
CN 103164644 A,2013.06.19,全文.

审查员 张莹

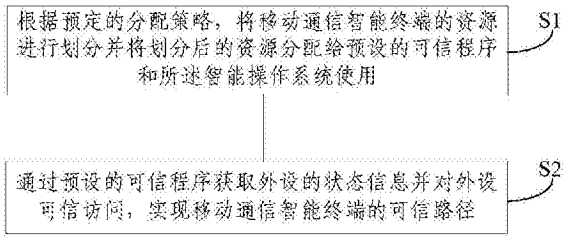
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种移动通信智能终端的可信路径实现方法及系统

(57)摘要

本发明公开一种移动通信智能终端的可信路径实现方法及系统,该方法包括:S1.根据预定的分配策略,将移动通信智能终端的资源进行划分并将划分后的资源分配给预设的可信程序和所述智能操作系统使用,实现移动通信智能终端的资源隔离;S2.通过预设的可信程序获取外设的状态信息并对外设可信访问,实现移动通信智能终端的可信路径。



1.一种移动通信智能终端的可信路径实现方法，其特征在于，该方法包括：

S1.根据预定的分配策略，将移动通信智能终端的资源进行划分并将划分后的资源分别分配给预设的可信程序和智能操作系统使用；其中，所述预设的可信程序和所述智能操作系统只能访问被分配到各自的资源；

S2.通过预设的可信程序获取外设的状态信息并对外设可信访问，实现移动通信智能终端的可信路径；

该方法进一步包括：

S3.通过预设的可信程序对用户口令及移动通信智能终端的智能操作系统进行认证，并根据认证情况判断是否启动移动通信智能终端的智能操作系统，其中，所述用户口令是通过分配给所述预设的可信程序的外设输入的。

2.根据权利要求1所述的方法，其特征在于，所述资源包括：CPU、内存、显示触摸屏、硬盘、按键、蓝牙、声音接口、串口、USB、网口、麦克风、扬声器、听筒及红外。

3.根据权利要求1或2所述的方法，其特征在于，所述步骤S2包括：

通过进程间通信IPC机制，由所述预设的可信程序获取外设的状态信息，所述状态信息由分配给所述预设的可信程序的显示触摸屏区域显示。

4.根据权利要求 1所述的方法，其特征在于，所述步骤S3包括：

S31.通过预设的可信程序对用户口令进行身份认证及移动通信智能终端的智能操作系统进行完整性认证；

S32.如果认证成功，则启动移动通信智能终端的智能操作系统，否则不启动移动通信智能终端的智能操作系统。

5.根据权利要求4所述的方法，其特征还在于，所述步骤S3进一步包括：

S33.通过进程间通信IPC机制，所述预设的可信程序启动移动通信智能终端的智能操作系统上的预设的可信软件。

6.一种移动通信智能终端的可信路径实现系统，其特征在于，该系统包括：

资源划分与分配模块，用于根据预定的分配策略，将移动通信智能终端的资源进行划分并将划分后的资源分别分配给预设的可信程序和智能操作系统使用；其中，所述预设的可信程序和所述智能操作系统只能访问被分配到各自的资源；

可信路径实现模块，用于通过预设的可信程序获取外设的状态信息并对外设可信访问，实现移动通信智能终端的可信路径；

认证与判断模块，用于通过预设的可信程序对用户口令及移动通信智能终端的智能操作系统进行认证，并根据认证情况判断是否启动移动通信智能终端的智能操作系统，其中，所述用户口令是通过分配给所述预设的可信程序的外设输入的。

7.根据权利要求6所述的系统，其特征在于，所述可信路径实现模块通过进程间通信IPC机制，由所述预设的可信程序获取外设的状态信息，所述状态信息由分配给所述预设的可信程序的显示触摸屏区域显示。

8.根据权利要求6所述的系统，其特征在于，所述认证与判断模块通过预设的可信程序对用户口令进行身份认证及移动通信智能终端的智能操作系统进行完整性认证；如果认证成功，则启动移动通信智能终端的智能操作系统，否则不启动移动通信智能终端的智能操作系统；通过进程间通信IPC机制，所述预设的可信程序启动移动通信智能终端的智能操作

系统上的预设的可信软件。

一种移动通信智能终端的可信路径实现方法及系统

技术领域

[0001] 本发明涉及移动通信领域，具体涉及一种移动通信智能终端的可信路径实现方法及系统。

背景技术

[0002] 随着移动通信技术的发展，移动通信智能终端得到了巨大的普及，移动通信智能终端采用了智能操作系统，智能操作系统的使用给移动通信用户带来了巨大的便利，用户可以随时连接网络查看信息，并可以安装各种功能丰富的应用。但是随之带来的安全隐患也越来越成为人们关注的重点。移动通信智能终端的用户在上网或安装恶意应用时，容易感染病毒、木马程序，用户的信息如账号密码等，容易被病毒、木马截获，造成用户的信息泄露。

[0003] 针对移动通信智能终端存在的安全问题，需要在移动通信智能终端建立可信路径，保证用户通过它可以与TCB进行直接通信，并且这种通信不可以被攻击者截获或修改，从而保护用户账号和密码等信息。现有的主流的操作系统都在一定程度上提供了可信路径机制，这些操作系统的可信路径一般都是通过安全注意键(Secure Attention Key，SAK)的方式来实现的。

[0004] Windows系列操作系统所默认的SAK序列为“Ctrl+Alt+Del”，当系统内核检测到上述三键被同时按下时，由Winlogon进程将当前桌面切换到Winlogon桌面，而只有Winlogon进程可以访问Winlogon桌面，从而保证没有别的恶意程序可以监控登录过程。

[0005] Linux系统默认的SAK序列是“Alt+SysRq+K”，当用户在某一虚拟终端使用SAK时，系统将终止那些打开虚拟终端的进程，重新由Init程序启动新的虚拟终端，并进一步完成登录过程。

[0006] 目前，Windows系列操作系统通过隔离桌面作用于发起访问的对象、Linux系统通过统一的资源保护作用于被保护的对象实现的可信路径，并没有完全消除潜在的安全威胁。

[0007] 在Windows系列操作系统下GINA木马可以伪造桌面；在Linux系统下某些木马程序可以躲避被杀掉的风险。

[0008] 通过SAK方式实现的可信路径只能保护用户的登录过程，并不能保护用户的其他输入操作。

[0009] 因此，在移动通信智能终端上采用SAK方式实现的可信路径，并不能全面保护用户的账号和密码等信息不被泄露。同时，目前的主流的移动通信智能终端都是采用触摸屏进行输入，物理按键较少，如果在移动通信智能终端采用SAK方式实现可信路径，用户体验较差。

发明内容

[0010] 本发明所要解决的技术问题是现有的移动通信智能终端的可信路径实现方式，并

不能全面保护用户的账号和密码等信息不被泄露，同时，目前的主流的移动通信智能终端都是采用触摸屏进行输入，物理按键较少，如果在移动通信智能终端采用SAK方式实现可信路径，用户体验较差。

[0011] 为此目的，本发明提出一种移动通信智能终端的可信路径实现方法，该方法包括：

[0012] S1.根据预定的分配策略，将移动通信智能终端的资源进行划分并将划分后的资源分配给预设的可信程序和所述智能操作系统使用；

[0013] S2.通过预设的可信程序获取外设的状态信息并对外设可信访问，实现移动通信智能终端的可信路径。

[0014] 较佳的，该方法进一步包括：

[0015] S3.通过预设的可信程序对用户口令及移动通信智能终端的智能操作系统进行认证，并根据认证情况判断是否启动移动通信智能终端的智能操作系统。

[0016] 其中，所述资源包括：CPU、内存、显示触摸屏、硬盘、按键、蓝牙、声音接口、串口、USB、网口、麦克风、扬声器、听筒及红外。

[0017] 其中于，所述步骤S2包括：

[0018] 通过进程间通信IPC机制，由所述预设的可信程序获取外设的状态信息，所述状态信息由分配给所述预设的可信程序的显示触摸屏区域显示。

[0019] 其中，所述步骤S3包括：

[0020] S31.通过预设的可信程序对用户口令进行身份认证及移动通信智能终端的智能操作系统进行完整性认证；

[0021] S32.如果认证成功，则启动移动通信智能终端的智能操作系统，否则不启动移动通信智能终端的智能操作系统。

[0022] 较佳的，所述步骤S3进一步包括：

[0023] S33.通过进程间通信IPC机制，所述预设的可信程序启动移动通信智能终端的智能操作系统上的预设的可信软件。

[0024] 本发明还提出一种移动通信智能终端的可信路径实现系统，该系统包括：

[0025] 资源划分与分配模块，用于根据预定的分配策略，将移动通信智能终端的资源进行划分并将划分后的资源分配给预设的可信程序和所述智能操作系统使用；

[0026] 可信路径实现模块，用于通过预设的可信程序获取外设的状态信息并对外设可信访问，实现移动通信智能终端的可信路径。

[0027] 较佳的，该系统进一步包括：认证与判断模块，用于通过预设的可信程序对用户口令及移动通信智能终端的智能操作系统进行认证，并根据认证情况判断是否启动移动通信智能终端的智能操作系统。

[0028] 其中，所述可信路径实现模块通过进程间通信IPC机制，由所述预设的可信程序获取外设的状态信息，所述状态信息由分配给所述预设的可信程序的显示触摸屏区域显示。

[0029] 其中，所述认证与判断模块通过预设的可信程序对用户口令进行身份认证及移动通信智能终端的智能操作系统进行完整性认证；如果认证成功，则启动移动通信智能终端的智能操作系统，否则不启动移动通信智能终端的智能操作系统；通过进程间通信IPC机制，所述预设的可信程序启动移动通信智能终端的智能操作系统上的预设的可信软件。

[0030] 相比于现有技术，本发明提供的方法的有益效果是：根据预设策略分配系统资源

给移动通信智能终端安装的智能操作系统和可信程序，将系统的其它资源同智能操作系统隔离开来，该智能操作系统只能访问分配给其的特定资源，无法访问其它的系统资源。利用与智能操作系统隔离的其他资源运行可信程序，通过可信程序提供密码服务、存储私密信息、监视系统运行等功能，用户与可信程序之间的交互都是处于可信路径当中，从而实现保护用户信息。可信程序同外设之间的交互也是处于可信路径当中，方便用户准确掌握关键外设的状态，达到监控移动通信智能终端的系统状态的目的。

附图说明

[0031] 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一简单地介绍，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。

[0032] 图1示出了一种移动通信智能终端的可信路径实现方法流程图；

[0033] 图2示出了一种移动通信智能终端的显示触摸屏资源隔离示意图；

[0034] 图3示出了一种移动通信智能终端的操作系统启动流程图；

[0035] 图4示出了一种移动通信智能终端的可信路径实现系统结构图。

具体实施方式

[0036] 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。

[0037] 实施例1：

[0038] 本实施例公开一种移动通信智能终端的可信路径实现方法，如图1所示，该方法包括：

[0039] S1.根据预定的分配策略，将移动通信智能终端的资源进行划分并将划分后的资源分配给预设的可信程序和所述智能操作系统使用，实现移动通信智能终端的资源隔离；可信程序与智能操作系统的资源之间是分离的，二者无法互相访问；

[0040] S2.通过预设的可信程序获取外设的状态信息并对外设可信访问，实现移动通信智能终端的可信路径。

[0041] 较佳的，该方法进一步包括：

[0042] S3.通过预设的可信程序对用户口令及移动通信智能终端的智能操作系统进行认证，并根据认证情况判断是否启动移动通信智能终端的智能操作系统。

[0043] 其中，所述资源包括：CPU、内存、显示触摸屏、硬盘、按键、蓝牙、声音接口、串口、USB、网口、麦克风、扬声器、听筒及红外。

[0044] 其中于，所述步骤S2包括：

[0045] 通过进程间通信IPC机制，由所述预设的可信程序获取外设的状态信息，所述状态信息由分配给所述预设的可信程序的显示触摸屏区域显示。

[0046] 其中，所述步骤S3包括：

[0047] S31.通过预设的可信程序对用户口令进行身份认证及移动通信智能终端的智能操作系统进行完整性认证；

[0048] S32.如果认证成功，则启动移动通信智能终端的智能操作系统，否则不启动移动通信智能终端的智能操作系统。

[0049] 较佳的，所述步骤S3进一步包括：

[0050] S33.通过进程间通信IPC机制，所述预设的可信程序启动移动通信智能终端的智能操作系统上的预设的可信软件。

[0051] 实施例2：

[0052] 本实施例公开一种移动通信智能终端的可信路径实现方法，该方法包括：

[0053] S1.根据预定的分配策略，将智能终端的显示触摸屏进行区域划分，得到显示触摸屏的不同区域并将划分后的显示触摸屏的不同区域分配给预设的可信程序和所述智能操作系统使用，如图2所示。可信程序和Android智能操作系统只能访问资源管理框架为其分配的特定屏幕资源，并接收用户在相应触摸屏区域输入的信息。可信程序和Android智能操作系统都无法直接访问对方的屏幕资源，也无法获得用户在对方区域进行的输入信息。

[0054] S2.通过预设的可信程序获取外设的状态信息并对外设可信访问，实现移动通信智能终端的可信路径。本实施例中，通过进程间通信IPC机制，由所述预设的可信程序获取外设的状态信息，所述状态信息由分配给所述预设的可信程序的显示触摸屏区域显示。

[0055] S3.通过预设的可信程序对用户口令及移动通信智能终端的智能操作系统进行认证，并根据认证情况判断是否启动移动通信智能终端的智能操作系统。如图3所示，具体包括：

[0056] 通过预设的可信程序对用户口令进行身份认证及移动通信智能终端的智能操作系统进行完整性认证；

[0057] 如果认证成功，则启动移动通信智能终端的智能操作系统，否则不启动移动通信智能终端的智能操作系统；

[0058] 通过进程间通信IPC机制，所述预设的可信程序启动移动通信智能终端的智能操作系统上的预设的可信软件。

[0059] 本实施例中，可信程序通过接收用户的控制指令、提供密码服务、存储用户的保密信息、显示外设状态等功能，达到保护用户信息、监控系统运行状态的目的。

[0060] 本实施例中，系统上电后，可信程序首先启动，并显示在可信程序的显示区域。可信程序通过可信路径对Android智能操作系统进行身份认证或完整性验证来，只有通过验证后，移动通信智能终端的Android智能操作系统才可以启动，并显示在操作系统显示区域。

[0061] 本实施例中，所说的可信程序是在移动智能通信终端的隔离资源基础上的、通过可信路径实现的程序。可信程序接收分配给其的显示和触摸屏资源，并同用户进行交互的程序。可信程序所能访问的系统资源同智能操作系统进行隔离。

[0062] 本实施例中，可信程序通过可信路径接收用户的输入(如点击按钮)，通过可信路径利用IPC机制启动移动通信智能终端的Android操作系统上的可信软件。

[0063] 实施例3：

[0064] 本实施例公开一种移动通信智能终端的可信路径实现系统，如图4所示，该系统包

括：

[0065] 资源划分与分配模块，用于根据预定的分配策略，将移动通信智能终端的资源进行划分并将划分后的资源分配给预设的可信程序和所述智能操作系统使用；

[0066] 认证与判断模块，用于通过预设的可信程序对用户口令及移动通信智能终端的智能操作系统进行认证，并根据认证情况判断是否启动移动通信智能终端的智能操作系统；

[0067] 可信路径实现模块，用于通过预设的可信程序获取外设的状态信息并对外设可信访问，实现移动通信智能终端的可信路径。

[0068] 其中，所述认证与判断模块通过预设的可信程序对用户口令进行身份认证及移动通信智能终端的智能操作系统进行完整性认证；如果认证成功，则启动移动通信智能终端的智能操作系统，否则不启动移动通信智能终端的智能操作系统；通过进程间通信IPC机制，所述预设的可信程序启动移动通信智能终端的智能操作系统上的预设的可信软件。

[0069] 其中，所述可信路径实现模块通过进程间通信IPC机制，由所述预设的可信程序获取外设的状态信息，所述状态信息由分配给所述预设的可信程序的显示触摸屏区域显示。

[0070] 上述实施例通过资源隔离实现移动通信智能终端的可信路径的方法及系统的有益效果是：可应用于安装有智能操作系统下的移动通信智能终端，通过专门设计的系统操作移动通信智能终端硬件，在底层控制整个终端的资源，对资源进行分配、管理和回收。根据预设策略分配系统资源给移动通信智能终端安装的智能操作系统和可信程序，将系统的其它资源同智能操作系统隔离开来，该智能操作系统只能访问分配给其的特定资源，无法访问其它的系统资源。利用与智能操作系统隔离的其他资源运行可信程序，通过可信程序提供密码服务、存储私密信息、监视系统运行等功能，用户与可信程序之间的交互都是处于可信路径当中，从而实现保护用户信息。可信程序同外设之间的交互也是处于可信路径当中，方便用户准确掌握关键外设的状态，达到监控移动通信智能终端的系统状态的目的。

[0071] 虽然结合附图描述了本发明的实施方式，但是本领域技术人员可以在不脱离本发明的精神和范围的情况下做出各种修改和变型，这样的修改和变型均落入由所附权利要求所限定的范围之内。

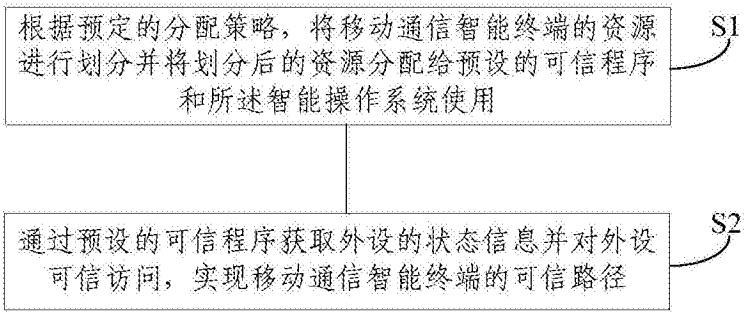

根据预定的分配策略，将移动通信智能终端的资源进行划分并将划分后的资源分配给预设的可信程序和所述智能操作系统使用
S1
通过预设的可信程序获取外设的状态信息并对外设可信访问，实现移动通信智能终端的可信路径
S2

图1


可信程序显示区域
操作系统显示区域
（Android、Windows Phone、Linux）

图2

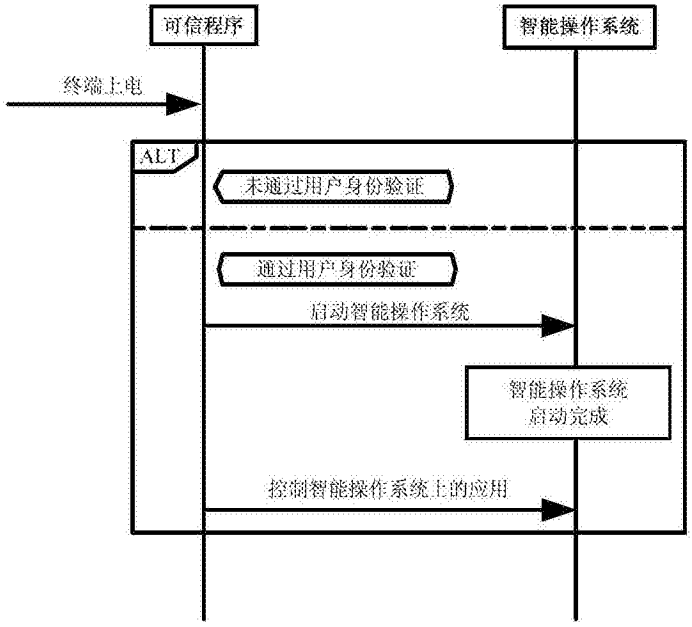

可信程序
智能操作系统
终端上电
ALT
未通过用户身份验证
通过用户身份验证
启动智能操作系统
智能操作系统启动完成
控制智能操作系统上的应用

图3

图4