(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 103413089 A
(43)申请公布日 2013.11.27

(21)申请号 201310382336.4

(22)申请日 2013.08.28

(71)申请人 天翼电信终端有限公司
地址 100033 北京市西城区金融大街31号2层

(72)发明人 马道杰 李海强 李霞

(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 王莹

(51)Int.Cl.
G06F 21/53(2013.01)
G06F 21/74(2013.01)

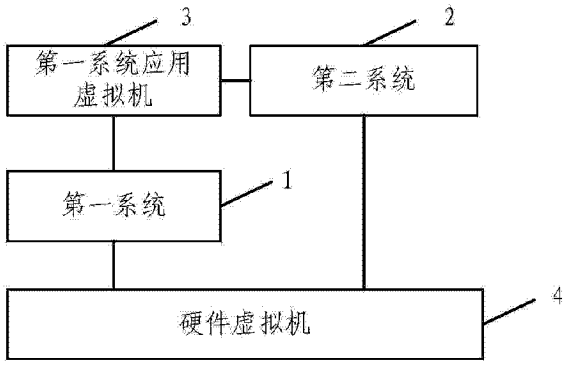
权利要求书1页 说明书4页 附图2页

(54)发明名称

移动终端及其实现双系统的方法

(57)摘要

本发明提供一种移动终端及其实现双系统的方法，该移动终端包括：第一系统，用于私密应用的运行和管理；第二系统，用于非私密应用的运行和管理；第一系统应用虚拟机，用于将该私密应用虚拟为该第二系统应用，以便该第二系统的应用加载器对该私密应用进行调用和管理；硬件虚拟机，用于在该移动终端的物理硬件层上分别为该第一系统和第二系统模拟独立的硬件资源访问和控制。本发明能够提高用户数据的安全性。



CN 103413089 A

1. 一种移动终端，其特征在于，包括：

第一系统，用于私密应用的运行和管理；

第二系统，用于非私密应用的运行和管理；

第一系统应用虚拟机，用于将所述私密应用虚拟为所述第二系统应用，以便所述第二系统的应用加载器对所述私密应用进行调用和管理；

硬件虚拟机，用于在所述移动终端的物理硬件层上分别为所述第一系统和第二系统模拟独立的硬件资源访问和控制。

2. 根据权利要求 1 所述的移动终端，其特征在于，所述私密应用包括电话、短信、联系人和记事本中的一个或多个应用。

3. 根据权利要求 2 所述的移动终端，其特征在于，所述第一系统为 RTOS 系统，所述第二系统为 Android 操作系统。

4. 根据权利要求 3 所述的移动终端，其特征在于，所述私密应用和所述非私密应用具有一致的界面风格。

5. 根据权利要求 3 所述的移动终端，其特征在于，所述 RTOS 系统应用虚拟机还用于为所述 RTOS 系统实现虚拟访问，以便在 RTOS 系统应用和 Android 操作系统应用之间协调屏幕资源。

6. 根据权利要求 1 所述的移动终端，其特征在于，还包括：

获取模块，用于获取用户点击应用的 ID，以便所述应用加载器根据所述 ID 调用所述 ID 对应的应用。

7. 一种权利要求 1-6 任意一项所述的移动终端实现双系统的方法，其特征在于，包括：

判断用户点击的应用是否为私密应用，若是，则调用所述用户点击的应用和所述第一系统，将所述用户点击的应用通过所述第一系统运行；否则，调用所述用户点击的应用和所述第二系统，将所述用户点击的应用通过所述第二系统运行。

8. 根据权利要求 7 所述的移动终端实现双系统的方法，其特征在于，判断用户点击的应用是否为私密应用包括：

获取用户点击的应用的 ID；

根据所述 ID 判断所述用户点击的应用是否为私密应用。

移动终端及其实现双系统的方法

技术领域

[0001] 本发明涉及数据安全领域，尤其涉及一种移动终端及其实现双系统的方法。

背景技术

[0002] 目前的智能终端都拥有上网和自由下载安装第三方应用的功能，导致的一个严重问题便是终端用户个人隐私数据的泄露以及遭遇恶意木马病毒的攻击。

[0003] 现有的移动终端用户数据安全保护相关方案均是基于一个开放操作系统(如Android 系统)的二次开发，由于原生操作系统的开放性和开源性，使得二次开发的安全方案都极容易被破解或规避，导致现有的安全方案失去其原本的安全功能。

发明内容

[0004] (一)要解决的技术问题

[0005] 本发明要解决的技术问题是：如何提高用户数据的安全性。

[0006] (二)技术方案

[0007] 为解决上述技术问题，本发明提供了一种移动终端，包括：

[0008] 第一系统，用于私密应用的运行和管理；

[0009] 第二系统，用于非私密应用的运行和管理；

[0010] 第一系统应用虚拟机，用于将所述私密应用虚拟为所述第二系统应用，以便所述第二系统的应用加载器对所述私密应用进行调用和管理；

[0011] 硬件虚拟机，用于在所述移动终端的物理硬件层上分别为所述第一系统和第二系统模拟独立的硬件资源访问和控制。

[0012] 进一步地，所述私密应用包括电话、短信、联系人和记事本中的一个或多个应用。

[0013] 进一步地，所述第一系统为 RTOS 系统，所述第二系统为 Android 操作系统。

[0014] 进一步地，所述私密应用和所述非私密应用具有一致的界面风格。

[0015] 进一步地，所述 RTOS 系统应用虚拟机还用于为所述 RTOS 系统实现虚拟访问，以便在 RTOS 系统应用和 Android 操作系统应用之间协调屏幕资源。

[0016] 进一步地，还包括：

[0017] 获取模块，用于获取用户点击应用的 ID，以便所述应用加载器根据所述 ID 调用所述 ID 对应的应用。

[0018] 为解决上述问题，本发明还提供了上述的移动终端实现双系统的方法，包括：

[0019] 判断用户点击的应用是否为私密应用，若是，则调用所述用户点击的应用和所述第一系统，将所述用户点击的应用通过所述第一系统运行；否则，调用所述用户点击的应用和所述第二系统，将所述用户点击的应用通过所述第二系统运行。

[0020] 进一步地，判断用户点击的应用是否为私密应用包括：

[0021] 获取用户点击的应用的 ID；

[0022] 根据所述 ID 判断所述用户点击的应用是否为私密应用。

[0023] (三)有益效果

[0024] 本发明为移动终端设置双系统,其中,第一系统用于隐私数据相关应用(私密应用)的运行和管理,保证用户的私密数据只被第一系统访问和管理,确保这些数据不会被其它操作系统上的应用所影响或窃取,第二系统用于非隐私数据相关应用(非私密应用)的运行和管理,两个系统独立且配合运行,从而彻底隔绝一切可能导致用户隐私数据泄露的外在源头,提高了用户数据的安全性。

附图说明

[0025] 图 1 为本发明一种实施方式提供的移动终端的结构图 ;

[0026] 图 2 是本发明另一种实施方式提供的移动终端的示意图 ;

[0027] 图 3 是本发明一种实施方式提供的移动终端实现双系统的方法的流程图 ;

[0028] 图 4 是本发明另一种实施方式提供的移动终端实现双系统的方法的流程图。

具体实施方式

[0029] 本发明的核心思想为 :为移动终端设置双系统,其中,第一系统用于隐私数据相关应用(私密应用)的运行和管理,保证用户的私密数据只被第一系统访问和管理,确保这些数据不会被其它操作系统上的应用所影响或窃取,第二系统用于非隐私数据相关应用(非私密应用)的运行和管理,两个系统独立且配合运行,从而彻底隔绝一切可能导致用户隐私数据泄露的外在源头,提高了用户数据的安全性。

[0030] 图 1 为本发明实施方式提供的移动终端的结构图,该移动终端包括 :

[0031] 第一系统 1,用于私密应用的运行和管理 ;

[0032] 该私密应用包含所有用户在意的私密数据相关的应用,只允许在第一系统上运行,其相关数据不会被其它系统访问。

[0033] 第二系统 2,用于非私密应用的运行和管理 ;

[0034] 该非私密应用为除私密应用之外的应用,只允许在该第二系统上运行 ;该第二系统可以为智能操作系统,以便为用户提供丰富的应用程序。

[0035] 第一系统应用虚拟机 3,用于将所述私密应用虚拟为所述第二系统应用,以便所述第二系统的应用加载器对所述私密应用进行调用和管理 ;

[0036] 该第一系统应用虚拟机将私密应用的应用入口封装为第二系统的应用加载器所能识别的文件格式,以便该第二系统的应用加载器对所述私密应用进行调用和管理。

[0037] 硬件虚拟机 4,用于在所述移动终端的物理硬件层上分别为所述第一系统和第二系统模拟独立的硬件资源访问和控制。

[0038] 该硬件虚拟机负责为两套系统虚拟出各自的硬件资源访问,以便实现在每个系统看来自己都拥有独立的一套硬件资源的自由访问。

[0039] 本实施方式提供的移动终端包含双系统,第一系统用于隐私数据相关应用(私密应用)的运行和管理,保证用户的私密数据只被第一系统访问和管理,确保这些数据不会被其它操作系统上的应用所影响或窃取,第二系统用于非隐私数据相关应用(非私密应用)的运行和管理,两个系统独立且配合运行,从而彻底隔绝一切可能导致用户隐私数据泄露的外在源头,保证了用户的数据安全。

[0040] 优选地，所述私密应用包括电话、短信、联系人和记事本中的一个或多个应用。

[0041] 优选地，所述第一系统为 RTOS 系统，所述第二系统为 Android 操作系统。

[0042] 优选地，所述 RTOS 系统的私密应用和所述 Android 操作系统的非私密应用具有一致的界面风格。

[0043] 优选地，所述 RTOS 系统应用虚拟机还用于为所述 RTOS 系统实现虚拟访问，以便在 RTOS 系统应用和 Android 操作系统应用之间协调屏幕资源。

[0044] 参见图 2，图 2 是本发明另一种实施方式提供的移动终端，该移动终端包括 RTOS（Real Time Operating System，实时操作系统）、Android 操作系统核心 Linux Kernel、Android 操作系统 Lancher（应用加载器）、RTOS-VM（RTOS 应用虚拟机）、私密应用、非私密应用、HVM（硬件虚拟机），其中，各个模块的功能如下：

[0045] Android 操作系统 Lancher（应用加载器）：负责调用和管理双系统的各类应用，包括基于 RTOS 的私密应用和基于 Android 操作系统的非私密应用。

[0046] RTOS-VM（RTOS 应用虚拟机）：将 RTOS 应用虚拟成 Android 操作系统应用，便于 Lancher 调用和管理，同时为 RTOS 实现虚拟的 frame buffer、key、touch 的访问，便于在 RTOS 应用和 Android 操作系统应用之间协调屏幕相关的资源。

[0047] 私密应用：包含所有用户在意的私密数据相关的应用，只允许在 RTOS 系统上运行，其相关数据不会被 Android 操作系统访问。

[0048] 非私密应用：除私密应用之外的应用，只允许在 Android 操作系统上运行。

[0049] RTOS：实时操作系统层，RTOS 系统上的私密应用只能调用 RTOS 系统的接口，与 Android 操作系统完全隔绝。

[0050] Linux Kernel：Android 操作系统核心层，Android 操作系统上的非私密应用只能调用该层，与 RTOS 系统完全隔绝。

[0051] HVM（硬件虚拟机）：负责在移动终端的 HW（物理硬件层）上为两套系统虚拟出各自的硬件资源访问，以便实现在每个系统看来自己都拥有独立的一套硬件资源的自由访问。

[0052] 优选地，该移动终端还包括：

[0053] 获取模块，用于获取用户点击应用的 ID，以便所述应用加载器根据所述 ID 调用所述 ID 对应的应用。

[0054] 图 3 是上述移动终端实现双系统的方法的流程图，包括：

[0055] 步骤 S1：判断用户点击的应用是否为私密应用，若是，执行步骤 S2，否则，执行步骤 S3；

[0056] 步骤 S2：调用所述用户点击的应用和所述第一系统，将所述用户点击的应用通过所述第一系统运行；

[0057] 步骤 S3：调用所述用户点击的应用和所述第二系统，将所述用户点击的应用通过所述第二系统运行。

[0058] 优选地，步骤 S1 具体包括：获取用户点击的应用的 ID；根据所述 ID 判断所述用户点击的应用是否为私密应用。

[0059] 具体地，本发明实施方式提供的移动终端首先将电话、短信、联系人、记事本等应用设为需要在 RTOS 上运行的私密应用，并基于 RTOS 的系统接口调用和 Android 的 GUI 实现这些应用，同时 disable 掉 Android 系统上的同类应用；通过 RTOS-VM 将电话、短信、联系

人、记事本等私密应用的应用入口封装为 Android Lancher 所能识别的 apk 形式，同时，将 RTOS 应用中的关于 frame buffer、key、touch 的访问接口的封装使用 Android 的相关接口来实现；修改 Android 的 lancher，如果被调用的应用为电话、短信、联系人、记事本等私密应用，则向下调用 RTOS 系统的电话、短信、联系人、记事本；参见图 4，当用户点击移动终端的应用，通过该应用的 ID 判断用户点击的应用是否为私密应用，若是，则调用用户点击的应用和 RTOS 系统，将所述用户点击的应用通过 RTOS 系统运行；否则，调用用户点击的应用和 Android 操作系统核心层，将用户点击的应用通过 Android 操作系统运行。

[0060] 本实施方式将用户在意的私密应用与其它应用（主要指涉及网络访问的相关应用）隔绝，从根本上确保私密数据不会被外泄，实现了真正的数据安全，其次，双系统中的智能操作系统（Android 操作系统）可以为用户提供丰富的应用下载和使用，保证了移动终端应用的丰富性和多样性。

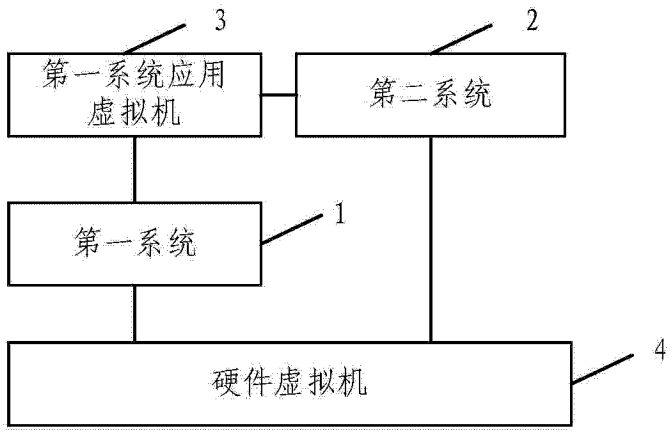

3
2
第一系统应用虚拟机
第二系统
1
第一系统
4
硬件虚拟机

图 1

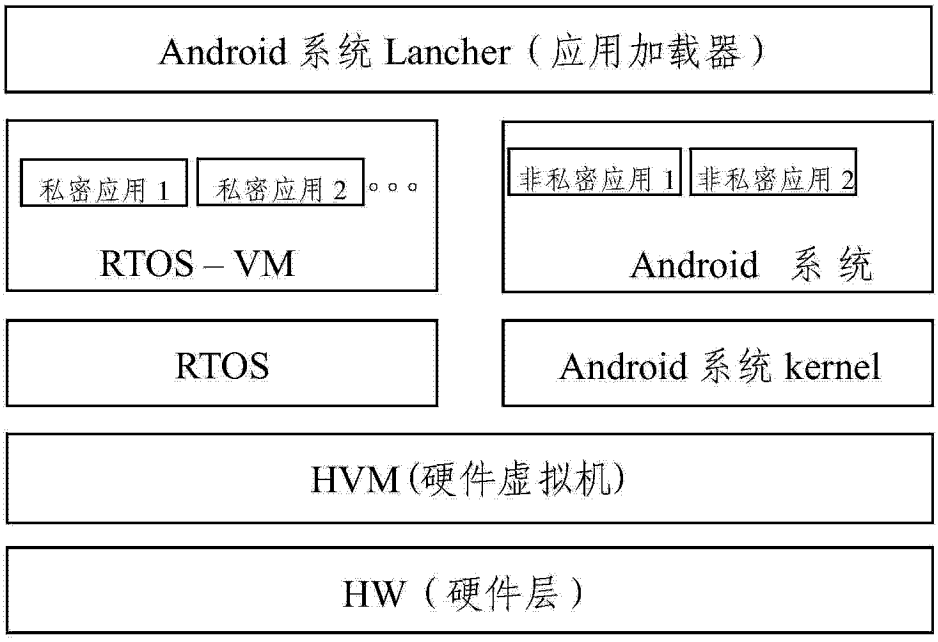

Android 系统 Lancher（应用加载器）
私密应用 1
私密应用 2
。。。
RTOS – VM
非私密应用 1
非私密应用 2
Android 系统
RTOS
Android 系统 kernel
HVM(硬件虚拟机)
HW（硬件层）

图 2

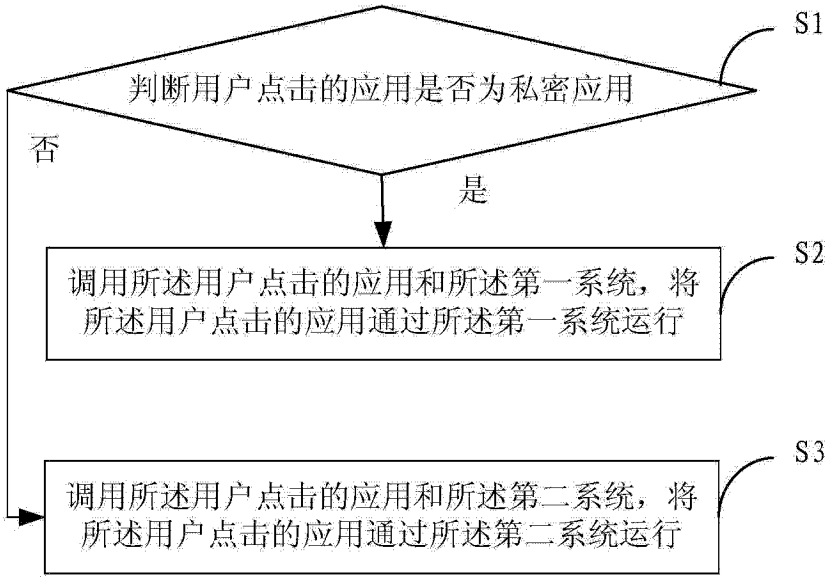

S1
判断用户点击的应用是否为私密应用
否
是
S2
调用所述用户点击的应用和所述第一系统，将所述用户点击的应用通过所述第一系统运行
S3
调用所述用户点击的应用和所述第二系统，将所述用户点击的应用通过所述第二系统运行

图 3

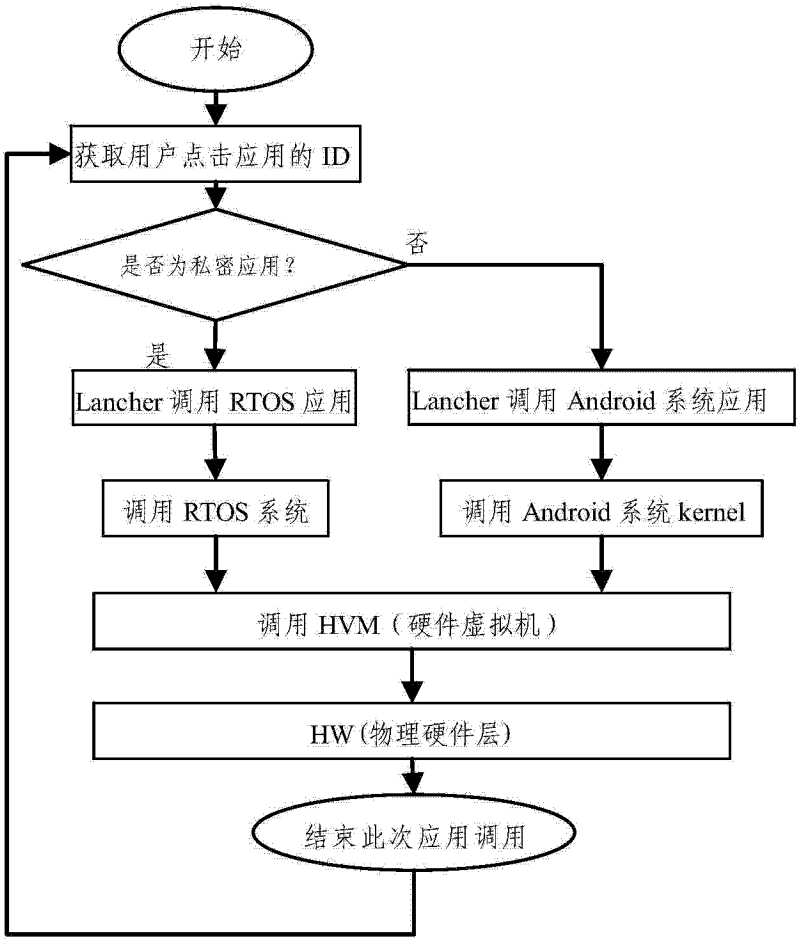

开始
获取用户点击应用的 ID
是否为私密应用？
否
是
Lancher 调用 RTOS 应用
Lancher 调用 Android 系统应用
调用 RTOS 系统
调用 Android 系统 kernel
调用 HVM（硬件虚拟机）
HW(物理硬件层)
结束此次应用调用

图 4