(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 102693395 B
(45)授权公告日 2015.02.11

(21)申请号 201210187455.X

(22)申请日 2012.06.07

(73)专利权人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
专利权人 奇智软件(北京)有限公司

(72)发明人 丁祎 李元

(74)专利代理机构 北京市中伦律师事务所 11410
代理人 程义贵 王桂玲

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

(56)对比文件

CN 101493873 A,2009.07.29, 权利要求1, 附图1.

CN 101667235 A,2010.03.10, 说明书第6页第2段,附图2.

US 5974549 A,1999.10.26, 全文.

CN 101620660 A,2010.01.06, 全文.

US 7797733 B1,2010.09.14, 全文.

史永林等.Windows API拦截技术.《电脑知识与技术》.2008, 第3卷(第9期), 第1920页, 图1.

审查员 彭明明

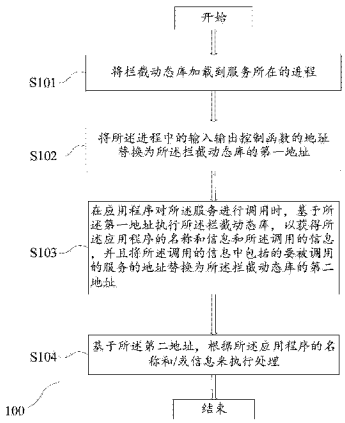
权利要求书3页 说明书9页 附图3页

(54)发明名称

一种用于拦截应用程序对服务的调用的方法和装置

(57)摘要

本发明提供了一种用于拦截电子设备的操作系统中应用程序对服务的调用的方法和装置。所述方法包括:将拦截动态库加载到服务所在的进程;将所述进程中的输入输出控制函数的地址替换为所述拦截动态库的第一地址;在应用程序对所述服务进行调用时,基于所述第一地址执行所述拦截动态库,以获得所述应用程序的名称和信息和所述调用的信息,并且将所述调用的信息中包括的要被调用的服务的地址替换为所述拦截动态库的第二地址;以及基于所述第二地址,根据所述应用程序的名称和/或信息来执行处理。本发明提高了电子设备操作系统的安全性。



CN 102693395 B

1. 一种用于拦截电子设备的操作系统中应用程序对服务的调用的方法 (100)，包括：

将拦截动态库加载到服务所在的进程 (S101)；

将所述进程中的输入输出控制函数的地址替换为所述拦截动态库的第一地址 (S102)；

在应用程序对所述服务进行调用时，基于所述第一地址执行所述拦截动态库，以获得所述应用程序的名称和信息和所述调用的信息，并且将所述调用的信息中包括的要被调用的服务的地址替换为所述拦截动态库的第二地址 (S103)；以及

基于所述第二地址，根据所述应用程序的名称和 / 或信息来执行处理 (S104)。

2. 如权利要求 1 所述的方法，其中根据所述应用程序的名称和 / 或信息来执行处理的步骤包括：通过将所述应用程序的名称和 / 或信息与预先定义的数据库中的信息进行比较，而 (a) 根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果，或者 (b) 向所述应用程序返回预先定义的服务结果。

3. 如权利要求 1 所述的方法，其中根据所述应用程序的名称来执行处理的步骤包括：在所述应用程序的名称包含在预先定义的数据库中的白名单中时，根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者，在所述应用程序的名称包含在预先定义的数据库中的黑名单中时，向所述应用程序返回预先定义的服务结果；或者，在所述应用程序的名称未包含在预先定义的数据库中的白名单和黑名单中时，显示所述应用程序的名称和信息和所述调用的信息，并且根据在电子设备上通过操作系统对于所述调用的选择来执行处理。

4. 如权利要求 1 所述的方法，其中根据所述应用程序的信息来执行处理的步骤包括：在所述应用程序的信息包含预先定义的数据库中的特征数据时，向所述应用程序返回预先定义的服务结果；或者，在所述应用程序的信息不包含预先定义的数据库中的特征数据时，显示所述应用程序的名称和信息和所述调用的信息，并且根据在电子设备上通过操作系统对于所述调用的选择来执行处理。

5. 如权利要求 3 或 4 所述的方法，其中根据在电子设备上通过操作系统的选择来执行处理的步骤包括：在选择了允许所述应用程序对所述服务的调用的情况下，根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者在选择了不允许所述应用程序对所述服务的调用的情况下，向所述应用程序返回预先定义的服务结果。

6. 如权利要求 1 至 4 中的任一项所述的方法，还包括在将拦截动态库加载到服务所在的进程 (S101) 的步骤之前暂停所述进程，以及在将所述进程中的输入输出控制函数的地址替换为所述拦截动态库的第一地址 (S102) 的步骤之后恢复所述进程。

7. 如权利要求 1 至 4 中的任一项所述的方法，其中所述调用的信息包括所述调用的接口序号以及要被调用的服务的地址。

8. 如权利要求 1 至 4 中的任一项所述的方法，其中所述操作系统是 Android 系统，所述应用程序通过 Android 系统的 Binder 机制对所述服务进行调用。

9. 如权利要求 8 所述的方法，其中所述输入输出控制函数是 Binder 机制中的 IOCTL 函数。

10. 如权利要求 9 所述的方法，其中在应用程序对所述服务进行调用时，基于所述第一地址执行所述拦截动态库，以通过所述 IOCTL 函数而先于 Android 系统获得所述应用程序

的名称和信息和所述调用的信息。

11. 一种用于拦截电子设备的操作系统中应用程序对服务的调用的装置 (200)，包括：

加载模块 (210)，用于将拦截动态库加载到服务所在的进程；

第一替换模块 (220)，用于将所述进程中的输入输出控制函数的地址替换为所述拦截动态库的第一地址；

第二替换模块 (230)，用于在应用程序对所述服务进行调用时，基于所述第一地址执行所述拦截动态库，以获得所述应用程序的名称和信息和所述调用的信息，并且将所述调用的信息中包括的要被调用的服务的地址替换为所述拦截动态库的第二地址；以及

处理模块 (240)，用于基于所述第二地址，根据所述应用程序的名称和 / 或信息来执行处理。

12. 如权利要求 11 所述的装置，其中所述处理模块 (240) 通过将所述应用程序的名称和 / 或信息与预先定义的数据库中的信息进行比较，而 (a) 根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果，或者 (b) 向所述应用程序返回预先定义的服务结果。

13. 如权利要求 11 所述的装置，其中在所述应用程序的名称包含在预先定义的数据库中的白名单中时，所述处理模块 (240) 根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者，在所述应用程序的名称包含在预先定义的数据库中的黑名单中时，所述处理模块 (240) 向所述应用程序返回预先定义的服务结果；或者，在所述应用程序的名称未包含在预先定义的数据库中的白名单和黑名单中时，所述处理模块 (240) 显示所述应用程序的名称和信息和所述调用的信息，并且根据在电子设备上通过操作系统对于所述调用的选择来执行处理。

14. 如权利要求 11 所述的装置，在所述应用程序的信息包含预先定义的数据库中的特征数据时，所述处理模块 (240) 向所述应用程序返回预先定义的服务结果；或者，在所述应用程序的信息不包含预先定义的数据库中的特征数据时，所述处理模块 (240) 显示所述应用程序的名称和信息和所述调用的信息，并且根据在电子设备上通过操作系统对于所述调用的选择来执行处理。

15. 如权利要求 13 或 14 所述的装置，其中在所述应用程序对所述服务的调用被选择为允许的情况下，所述处理模块 (240) 根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者在所述应用程序对所述服务的调用被选择为不允许的情况下，所述处理模块 (240) 向所述应用程序返回预先定义的服务结果。

16. 如权利要求 11 至 14 中的任一项所述的装置，还包括用于在所述加载模块 (210) 将拦截动态库加载到服务所在的进程之前暂停所述进程的暂停模块、以及用于在所述第一替换模块 (220) 将所述进程中的输入输出控制函数的地址替换为所述拦截动态库的第一地址之后恢复所述进程的恢复模块。

17. 如权利要求 11 至 14 中的任一项所述的装置，其中所述调用的信息包括所述调用的接口序号以及要被调用的服务的地址。

18. 如权利要求 11 至 14 中的任一项所述的装置，其中所述操作系统是 Android 系统，所述应用程序通过 Android 系统的 Binder 机制对所述服务进行调用。

19. 如权利要求 18 所述的装置，其中所述输入输出控制函数是 Binder 机制中的 IOCTL

函数。

20. 如权利要求 19 所述的装置，其中在应用程序对所述服务进行调用时，所述第二替换模块 (230) 基于所述第一地址执行所述拦截动态库，以通过所述 IOCTL 函数而先于 Android 系统获得所述应用程序的名称和信息和所述调用的信息。

一种用于拦截应用程序对服务的调用的方法和装置

技术领域

[0001] 本发明涉及电子设备操作系统的系统安全，特别涉及一种用于拦截电子设备的操作系统中应用程序对服务的调用的方法和装置。

背景技术

[0002] 近年来，安装有操作系统的电子设备、特别是便携式电子设备（例如，移动电话、平板电脑等）变得越来越普及。与之相应地，运行在这些电子设备的操作系统上的应用程序的数量也有了呈几何级数的爆炸式增长。以 iOS 系统和 Android 系统为例，目前这两个系统上的应用程序分别超过了 60 万个和 40 万个。

[0003] 尽管海量的应用程序给用户带来了更多的选择，但随之而来的安全性问题也值得关注。以 Android 系统为例，系统的部分重要功能通过服务接口的形式提供，譬如读取联系人信息是通过数据源服务（即系统的一个进程，该进程加载了数据源服务对象，并且提供接口）来进行的，任何需要读取联系人信息的程序都需要通过接口来向该服务申请读取联系人信息。

[0004] 这种服务的接口基于 Binder 通讯机制，调用接口的流程如下：应用程序发出对某个服务的接口请求，发送服务名称和接口序号 -> 服务的总路由查询服务，并登记调用者，让其等待 -> 服务的总路由分配客户的请求到具体服务 -> 具体服务执行对自己接口的调用 -> 具体服务返回接口调用的结果 -> 服务的总路由拿到结果，并返回给登记过的应用程序 -> 客户程序拿到接口请求的结果。

[0005] 目前，Android 系统本身不具备拦截的机制，只是在恶意程序安装之前告知系统用户此程序可能会访问某些服务，但是对于应用程序是否是恶意程序不做判断。目前，存在一些针对恶意程序进行拦截的方案。例如，通过向系统注册假服务的方式实现拦截，但是这种方式会在进行拦截的系统中留下明显的假服务名称，很容易被恶意程序发现，进而使拦截失效。

发明内容

[0006] 为了至少解决上述技术问题，本发明提供了一种用于拦截电子设备的操作系统中应用程序对服务的调用的方法和装置。

[0007] 根据本发明第一方面，提供了一种用于拦截电子设备的操作系统中应用程序对服务的调用的方法，包括：

[0008] 将拦截动态库加载到服务所在的进程；

[0009] 将所述进程中的输入输出控制函数的地址替换为所述拦截动态库的第一地址；

[0010] 在应用程序对所述服务进行调用时，基于所述第一地址执行所述拦截动态库，以获得所述应用程序的名称和信息和所述调用的信息，并且将所述调用的信息中包括的要被调用的服务的地址替换为所述拦截动态库的第二地址；以及

[0011] 基于所述第二地址，根据所述应用程序的名称和 / 或信息来执行处理。

[0012] 优选地，根据所述应用程序的名称和 / 或信息来执行处理的步骤包括：通过将所述应用程序的名称和 / 或信息与预先定义的数据库中的信息进行比较，而 (a) 根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果，或者 (b) 向所述应用程序返回预先定义的服务结果。

[0013] 优选地，根据所述应用程序的名称来执行处理的步骤包括：在所述应用程序的名称包含在预先定义的数据库中的白名单中时，根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者，在所述应用程序的名称包含在预先定义的数据库中的黑名单中时，向所述应用程序返回预先定义的服务结果；或者，在所述应用程序的名称未包含在预先定义的数据库中的白名单和黑名单中时，显示所述应用程序的名称和信息和所述调用的信息，并且根据在电子设备上通过操作系统对于所述调用的选择来执行处理。

[0014] 优选地，根据所述应用程序的信息来执行处理的步骤包括：在所述应用程序的信息包含预先定义的数据库中的特征数据时，向所述应用程序返回预先定义的服务结果；或者，在所述应用程序的信息不包含预先定义的数据库中的特征数据时，显示所述应用程序的名称和信息和所述调用的信息，并且根据在电子设备上通过操作系统对于所述调用的选择来执行处理。

[0015] 优选地，根据在电子设备上通过操作系统的选择来执行处理的步骤包括：在选择了允许所述应用程序对所述服务的调用的情况下，根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者在选择了不允许所述应用程序对所述服务的调用的情况下，向所述应用程序返回预先定义的服务结果。

[0016] 优选地，所述方法还包括在将拦截动态库加载到服务所在的进程的步骤之前暂停所述进程，以及在将所述进程中的输入输出控制函数的地址替换为所述拦截动态库的第一地址的步骤之后恢复所述进程。

[0017] 优选地，所述调用的信息包括所述调用的接口序号以及要被调用的服务的地址。

[0018] 优选地，所述操作系统是 Android 系统，所述应用程序通过 Android 系统的 Binder 机制对所述服务进行调用。

[0019] 优选地，所述输入输出控制函数是 Binder 机制中的 IOCTL 函数。

[0020] 优选地，在应用程序对所述服务进行调用时，基于所述第一地址执行所述拦截动态库，以通过所述 IOCTL 函数而先于 Android 系统获得所述应用程序的名称和信息和所述调用的信息。

[0021] 根据本发明第二方面，提供了一种用于拦截电子设备的操作系统中应用程序对服务的调用的装置，包括：

[0022] 加载模块，用于将拦截动态库加载到服务所在的进程；

[0023] 第一替换模块，用于将所述进程中的输入输出控制函数的地址替换为所述拦截动态库的第一地址；

[0024] 第二替换模块，用于在应用程序对所述服务进行调用时，基于所述第一地址执行所述拦截动态库，以获得所述应用程序的名称和信息和所述调用的信息，并且将所述调用的信息中包括的要被调用的服务的地址替换为所述拦截动态库的第二地址；以及

[0025] 处理模块，用于基于所述第二地址，根据所述应用程序的名称和 / 或信息来执行处理。

[0026] 优选地，所述处理模块通过将所述应用程序的名称和 / 或信息与预先定义的数据库中的信息进行比较，而 (a) 根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果，或者 (b) 向所述应用程序返回预先定义的服务结果。

[0027] 优选地，在所述应用程序的名称包含在预先定义的数据库中的白名单中时，所述处理模块根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者，在所述应用程序的名称包含在预先定义的数据库中的黑名单中时，所述处理模块向所述应用程序返回预先定义的服务结果；或者，在所述应用程序的名称未包含在预先定义的数据库中的白名单和黑名单中时，所述处理模块显示所述应用程序的名称和信息和所述调用的信息，并且根据在电子设备上通过操作系统对于所述调用的选择来执行处理。

[0028] 优选地，在所述应用程序的信息包含预先定义的数据库中的特征数据时，所述处理模块向所述应用程序返回预先定义的服务结果；或者，在所述应用程序的信息不包含预先定义的数据库中的特征数据时，所述处理模块显示所述应用程序的名称和信息和所述调用的信息，并且根据在电子设备上通过操作系统对于所述调用的选择来执行处理。

[0029] 优选地，在所述应用程序对所述服务的调用被选择为允许的情况下，所述处理模块根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者在所述应用程序对所述服务的调用被选择为不允许的情况下，所述处理模块向所述应用程序返回预先定义的服务结果。

[0030] 优选地，所述装置还包括用于在所述加载模块将拦截动态库加载到服务所在的进程之前暂停所述进程的暂停模块、以及用于在所述第一替换模块将所述进程中的输入输出控制函数的地址替换为所述拦截动态库的第一地址之后恢复所述进程的恢复模块。

[0031] 优选地，所述调用的信息包括所述调用的接口序号以及要被调用的服务的地址。

[0032] 优选地，所述操作系统是 Android 系统，所述应用程序通过 Android 系统的 Binder 机制对所述服务进行调用。

[0033] 优选地，所述输入输出控制函数是 Binder 机制中的 IOCTL 函数。

[0034] 优选地，在应用程序对所述服务进行调用时，所述第二替换模块基于所述第一地址执行所述拦截动态库，以通过所述 IOCTL 函数而先于 Android 系统获得所述应用程序的名称和信息和所述调用的信息。

[0035] 本发明提供了一种用于拦截电子设备的操作系统中应用程序对服务的调用的方法和装置。本发明能够在应用程序对服务进行调用时，对于调用进行拦截，并利用预先定义的数据库中的白名单、黑名单、以及特征数据来判断该应用程序是受信任的应用程序还是恶意应用程序。在应用程序和调用的信息与上述数据库中的信息均不吻合的情况下，还可以显示应用程序的名称和信息和调用的信息，这样就可以根据这些信息来选择是否允许应用程序对服务的调用。在例如恶意应用程序对服务调用的情况下，就可以直接拒绝该调用或者选择拒绝该调用，并向恶意应用程序返回该调用成功的虚假服务结果，使恶意应用程序无法发现，从而提高了系统的安全性。

附图说明

[0036] 根据以下结合附图的详细描述，本发明的以上和其它目的和特征将变得更加清楚，其中：

[0037] 图 1 是根据本发明的实施例的用于拦截电子设备的操作系统中应用程序对服务的调用的方法的流程图；

[0038] 图 2 是根据本发明的实施例的在电子设备上通过操作系统对于调用进行选择的示例视图；以及

[0039] 图 3 是根据本发明的实施例的用于拦截电子设备的操作系统中应用程序对服务的调用的装置的框图。

具体实施方式

[0040] 在以下的详细描述中，为了说明和示例的目的，描述若干个具体细节，以便提供对于各实施例的全面理解。然而，对于本领域普通技术人员而言，可以在没有这些具体细节的情况下实现这些实施例。在以下描述中使用的部件名称仅仅是为了容易说明，而不是为了进行任何限制。

[0041] 图 1 是根据本发明的实施例的用于拦截电子设备的操作系统中应用程序对服务的调用的方法的流程图。根据本发明，所述电子设备包括但不限于安装有操作系统的以下电子设备：移动电话、平板电脑、笔记本计算机、导航仪、音频和 / 或视频播放器、收音机、移动电视、多功能遥控器等便携式计算设备；台式计算机、大型计算机、打印机、传真机、复印机、多功能一体机、机顶盒、公共信息查询设备、多媒体信息交互设备等固定式计算设备；以及其它安装有操作系统的电子设备。

[0042] 在下文中，以安装有 Android 系统的移动电话为例，对本发明的原理进行示例性描述，然而此描述仅仅是示例性的，本发明的范围并不限于此，本发明的原理也可以适用于安装有其它操作系统（例如 Linux、iOS、Window Phone、Symbian 等）的任何电子设备，例如前面提及的那些电子设备。

[0043] 在用于拦截电子设备的操作系统中应用程序对服务的调用的方法 100 中，以下以应用程序通过 Android 系统的 Binder 机制对服务进行调用为例进行描述，但此描述仅仅是示例性的，本发明也适用于其它通信机制。

[0044] 根据本发明，预先在 Android 系统中找到各个服务所在的进程，在步骤 S101 中，将拦截动态库加载到服务所在的进程。根据本发明的实施例，例如可以通过 Android 系统所基于的 Linux 系统提供的应用程序编程接口 (Application Programming Interface, API) dlopen 来将该拦截动态库加载到所述服务所在的进程。根据本发明的实施例，在步骤 S101 执行之前，可以暂停所述进程，例如可以通过 Linux 系统提供的应用程序编程接口 ptrace 来实现此暂停操作。

[0045] 在上述步骤 S101 之后，执行步骤 S102，其中，将所述进程中的输入输出控制函数的地址替换为所述拦截动态库的第一地址。根据本发明的实施例，所述输入输出控制函数是 Binder 机制中的 IOCTL 函数。所述拦截动态库的第一地址用于执行所述拦截动态库。在步骤 S102 执行之后，可以恢复所述进程。

[0046] 接下来，在步骤 S103 中，在应用程序对所述服务进行调用时，基于所述第一地址执行所述拦截动态库，以获得所述应用程序的名称和信息和所述调用的信息，并且将所述调用的信息中包括的要被调用的服务的地址替换为所述拦截动态库的第二地址。根据本发明的实施例，在所述应用程序通过 Binder 机制来对所述服务进行调用时，将到达所述

IOCTL 函数，由于 IOCTL 函数的地址已经被替换为所述拦截动态库的第一地址，因此就将基于所述第一地址执行所述拦截动态库。此时，所述拦截动态库就可以通过所述 IOCTL 函数而先于 Android 系统获得所述应用程序的名称和信息和所述调用的信息。

[0047] 根据本发明的实施例，所述调用的信息包括所述调用的接口序号以及要被调用的服务的地址。将所述要被调用的服务的地址替换为所述拦截动态库的第二地址，可以基于该第二地址来根据所述应用程序的名称和 / 或信息来执行处理。

[0048] 由于所述要被调用的服务的地址已经被替换为所述拦截动态库的第二地址，因此，在步骤 S104 中，就将基于所述第二地址，根据所述应用程序的名称和 / 或信息来执行处理。

[0049] 根据本发明的实施例，基于所述第二地址，通过将所述应用程序的名称和 / 或信息与预先定义的数据库中的信息进行比较，而 (a) 根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果，或者 (b) 向所述应用程序返回预先定义的服务结果。

[0050] 根据本发明的实施例，所述预先定义的服务结果可以例如是表示所述调用已经成功的服务结果，以便令所述应用程序认为其对于所述服务的调用已经成功，而对于根据本发明的实施例所进行的拦截一无所知。

[0051] 所述预先定义的数据库可以包含应用程序白名单、黑名单、以及特征数据。所述白名单可以包含已知的受信任的应用程序的名称（包括程序的 UID（唯一标识符）和程序的包名），所述黑名单可以包含已知的恶意应用程序的名称（包括程序的 UID（唯一标识符）和程序的包名），所述特征数据可以包含已知的恶意特征（例如广告特征）的数据。

[0052] 根据本发明的实施例，可以分别利用应用程序的名称和信息、或者结合两者来对于所述应用程序的身份进行判断，进而采取相应的处理。

[0053] 具体而言，在利用应用程序的名称来对于所述应用程序的身份进行判断时：在所述应用程序的名称包含在所述预先定义的数据库中的白名单中时，根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者，在所述应用程序的名称包含在预先定义的数据库中的黑名单中时，向所述应用程序返回预先定义的服务结果；或者，在所述应用程序的名称未包含在预先定义的数据库中的白名单和黑名单中时，显示所述应用程序的名称和信息和所述调用的信息，并且根据在电子设备上通过操作系统对于所述调用的选择来执行处理。

[0054] 也就是说，当应用程序的名称包含在白名单中时，判定该应用程序为受信任的应用程序，允许其对于服务的调用，从而根据所述服务的地址执行调用，并向该应用程序返回实际服务结果；当应用程序的名称包含在黑名单中时，判定该应用软件为恶意应用程序，拒绝其对于服务的调用，直接向其返回虚假的服务结果，使其认为调用已经成功；而当应用程序的名称既未包含在白名单、也未包含在黑名单中时，则显示所述应用程序的名称和信息和所述调用的信息，并且根据在电子设备上通过操作系统对于所述调用的选择来执行处理。具体而言，在选择了允许所述应用程序对所述服务的调用的情况下，根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者在选择了不允许所述应用程序对所述服务的调用的情况下，向所述应用程序返回预先定义的服务结果。上述对于调用的选择例如可以是用户在看到显示在电子设备的显示屏上的所述应用程序的名称和信息和所述调用的信息之后，通过电子设备的操作系统来进行选择的。

[0055] 图 2 是根据本发明的实施例的在电子设备上通过操作系统对于调用进行选择的示例视图。参见图 2，将应用程序的名称和信息和调用的信息显示在移动电话的显示屏上，并向用户询问是否允许所述应用程序对所述服务的调用。在用户选择了允许所述应用程序对所述服务的调用的情况下，根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者在用户选择了不允许所述应用程序对所述服务的调用的情况下，向所述应用程序返回预先定义的服务结果。

[0056] 而在利用应用程序的信息来对于所述应用程序的身份进行判断时：在所述应用程序的信息包含所述预先定义的数据库中的特征数据时，向所述应用程序返回预先定义的服务结果；或者，在所述应用程序的信息不包含所述预先定义的数据库中的特征数据时，显示所述应用程序的名称和信息和所述调用的信息，并且根据在电子设备上通过操作系统对于所述调用的选择来执行处理。

[0057] 也就是说，当应用程序的信息（例如程序包配置信息）包含所述特征数据（例如广告特征的数据）时，即判断此应用程序为恶意应用程序，拒绝其对于服务的调用，直接向其返回虚假的服务结果，使其认为调用已经成功；而当应用程序的信息不包含所述特征数据时，执行上述参考图 2 描述的步骤，在用户选择了允许所述应用程序对所述服务的调用的情况下，根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者在用户选择了不允许所述应用程序对所述服务的调用的情况下，直接向所述应用程序返回预先定义的虚假的服务结果。

[0058] 下面以恶意应用程序 A 发起对于向通知栏发送广告消息的请求为例，对于本发明的原理进行描述，但此描述仅仅是示例性的，本发明可应用于拦截任何恶意应用程序。

[0059] 根据本发明的实施例，启动名单控制和显示服务，并预先在 Android 系统中找到各个服务所在的进程（包括通知栏服务所在的进程，假设其名称为进程 S），将拦截动态库加载到各个服务所在的进程（包括进程 S）。恶意应用程序 A 为了向通知栏发送广告消息，需要对于通知栏服务进行调用，其会首先发起对于通知栏接口的访问。

[0060] 根据本发明的实施例，将 Binder 机制中的 IOCTL 函数的地址替换为所述拦截动态库的第一地址。由于恶意应用程序 A 会通过 Binder 机制来实现对通知栏服务的调用，因此其会执行 Binder 机制中的 IOCTL 函数。该 IOCTL 已被替换为所述第一地址，因而将基于第一地址执行所述拦截动态库。此时，所述拦截动态库就可以通过所述 IOCTL 函数而先于 Android 系统获得所述应用程序的名称和信息（恶意应用程序 A 及其描述）和所述调用的信息（调用通知栏服务、所要显示的广告消息的标题和内容）。然后，将所述通知栏服务的地址替换为拦截动态库的第二地址。

[0061] 接下来，由于通知栏服务的地址已被替换为所述第二地址，因此将基于第二地址，通过 Binder 机制与名单控制和显示服务通信，判断所述恶意应用程序 A 的名称是否包含在预先定义的数据库中的白名单或黑名单中，并且 / 或者判断所述恶意应用程序 A 的信息是否包含预先定义的数据库中的特征数据。由于该恶意应用程序 A 的程序包中包含广告特征，因此即使该恶意应用程序 A 的名称未包含在所述黑名单中，也可以将其判断为恶意应用程序，从而拒绝其对于通知栏服务调用，直接向其返回预先定义的服务结果，即表示所述调用已经成功的服务结果，以便令恶意应用程序 A 认为其对于通知栏服务的调用已经成功，而对于根据本发明的实施例所进行的拦截一无所知。

[0062] 在替代实施例中，假设该恶意应用程序 A 的名称未包含在预先定义的数据库中的白名单和黑名单中，该恶意应用程序 A 的信息也不包含所述预先定义的数据库中的特征数据。此时，可以通过名单控制和显示服务在电子设备的显示屏上显示（例如以图 2 的方式显示或者在通知栏中显示）恶意应用程序 A 的名称和信息和所述调用的信息，在用户选择了允许所述恶意应用程序 A 对通知栏服务的调用的情况下，根据通知栏服务的地址执行所述调用，并向所述恶意应用程序 A 返回实际服务结果；或者在用户选择了不允许所述恶意应用程序 A 对通知栏服务的调用的情况下，直接向所述恶意应用程序 A 返回预先定义的虚假的服务结果。或者，在电子设备的显示屏上显示（例如以图 2 的方式显示或者在通知栏中显示）恶意应用程序 A 的名称和信息和所述调用的信息的同时，可以直接在通知栏中显示恶意应用程序 A 要发送的广告消息，用户在看到该广告消息后可以进行设置，从而将该恶意应用程序 A 添加到所述预先定义的数据库中的黑名单中，并将广告消息添加到所述预先定义的数据库中的特征数据中，以在之后的系统操作中直接拦截该恶意应用程序 A。

[0063] 本发明提供了一种用于拦截电子设备的操作系统中应用程序对服务的调用的方法。本发明能够在应用程序对服务进行调用时，对于调用进行拦截，并利用预先定义的数据库中的白名单、黑名单、以及特征数据来判断该应用程序是受信任的应用程序还是恶意应用程序。在应用程序和调用的信息与上述数据库中的信息均不吻合的情况下，还可以显示应用程序的名称和信息和调用的信息，这样就可以根据这些信息来选择是否允许应用程序对服务的调用。在例如恶意应用程序对服务调用的情况下，就可以直接拒绝该调用或者选择拒绝该调用，并向恶意应用程序返回该调用成功的虚假服务结果，使恶意应用程序无法发现，从而提高了系统的安全性。另外，还可以将用户从实际操作中获得的信息添加到该预先定义的数据库中，以完善数据库中的数据，从而在之后的拦截中获得更好的效果。

[0064] 根据本发明，可以拦截恶意应用程序偷窥电子设备用户的隐私信息（包括联系人信息、通话记录、短信、彩信、各种账户及密码等）的行为，防止恶意应用程序拨打扣费电话、发送扣费短信、访问耗费网络流量的网站，防止恶意应用程序安装木马和病毒程序，防止恶意应用程序记录用户的 GPS 或网络定位，拦截恶意应用程序弹出骚扰广告信息等等，可以对于任何恶意应用程序对于服务的调用进行拦截，从而提高了系统的安全性。

[0065] 与上述的方法 100 相对应，本发明还提供了一种用于拦截电子设备的操作系统中应用程序对服务的调用的装置 200，参见图 3，该装置 200 包括：

[0066] 加载模块 210，用于将拦截动态库加载到服务所在的进程，该加载模块 210 可以用于执行上述方法 100 中的步骤 S101；

[0067] 第一替换模块 220，用于将所述进程中的输入输出控制函数的地址替换为所述拦截动态库的第一地址，该第一替换模块 220 可以用于执行上述方法 100 中的步骤 S102；

[0068] 第二替换模块 230，用于在应用程序对所述服务进行调用时，基于所述第一地址执行所述拦截动态库，以获得所述应用程序的名称和信息和所述调用的信息，并且将所述调用的信息中包括的要被调用的服务的地址替换为所述拦截动态库的第二地址，该第二替换模块 230 可以用于执行上述方法 100 中的步骤 S103；以及

[0069] 处理模块 240，用于基于所述第二地址，根据所述应用程序的名称和 / 或信息来执行处理，该处理模块 240 可以用于执行上述方法 100 中的步骤 S104。

[0070] 在本发明的优选实施例中，所述处理模块 240 通过将所述应用程序的名称和 / 或

信息与预先定义的数据库中的信息进行比较，而 (a) 根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果，或者 (b) 向所述应用程序返回预先定义的服务结果。

[0071] 在本发明的优选实施例中，在所述应用程序的名称包含在预先定义的数据库中的白名单中时，所述处理模块 240 根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者，在所述应用程序的名称包含在预先定义的数据库中的黑名单中时，所述处理模块 240 向所述应用程序返回预先定义的服务结果；或者，在所述应用程序的名称未包含在预先定义的数据库中的白名单和黑名单中时，所述处理模块 240 显示所述应用程序的名称和信息和所述调用的信息，并且根据在电子设备上通过操作系统对于所述调用的选择来执行处理。

[0072] 在本发明的优选实施例中，在所述应用程序的信息包含预先定义的数据库中的特征数据时，所述处理模块 240 向所述应用程序返回预先定义的服务结果；或者，在所述应用程序的信息不包含预先定义的数据库中的特征数据时，所述处理模块 240 显示所述应用程序的名称和信息和所述调用的信息，并且根据在电子设备上通过操作系统对于所述调用的选择来执行处理。

[0073] 在本发明的优选实施例中，在所述应用程序对所述服务的调用被选择为允许的情况下，所述处理模块 240 根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者在所述应用程序对所述服务的调用被选择为不允许的情况下，所述处理模块 240 向所述应用程序返回预先定义的服务结果。

[0074] 在本发明的优选实施例中，所述装置 200 还包括用于在所述加载模块 210 将拦截动态库加载到服务所在的进程之前暂停所述进程的暂停模块、以及用于在所述第一替换模块 220 将所述进程中的输入输出控制函数的地址替换为所述拦截动态库的第一地址之后恢复所述进程的恢复模块。

[0075] 在本发明的优选实施例中，所述调用的信息包括所述调用的接口序号以及要被调用的服务的地址。

[0076] 在本发明的优选实施例中，所述操作系统是 Android 系统，所述应用程序通过 Android 系统的 Binder 机制对所述服务进行调用。

[0077] 在本发明的优选实施例中，所述输入输出控制函数是 Binder 机制中的 IOCTL 函数。

[0078] 在本发明的优选实施例中，在应用程序对所述服务进行调用时，所述第二替换模块 230 基于所述第一地址执行所述拦截动态库，以通过所述 IOCTL 函数而先于 Android 系统获得所述应用程序的名称和信息和所述调用的信息。

[0079] 由于上述各装置实施例与前述各方法实施例相对应，因此不再对各装置实施例进行详细描述。

[0080] 本发明可以以任何适当的形式实现，包括硬件、软件、固件或者它们的任意组合。可选地，本发明可以至少部分地实现为运行在一个或多个处理器和 / 或数字信号处理器上的计算机软件。本发明的实施例的装置和模块可以在物理上、功能上和逻辑上以任何适当的方式实现。根据本发明的各个功能可以在单个单元中、在多个单元中或者作为其他功能单元的一部分来实现。同样地，本发明可以在单个单元中实现，或者可以在物理上和功能上

分布在不同单元和处理器之间。

[0081] 尽管已经结合一些实施例描述了本发明，但是本发明并不意在限于本文阐述的特定形式。相反地，本发明的范围仅由所附权利要求书限定。此外，尽管特征可能看起来是结合特定实施例而被描述的，但是本领域普通技术人员应当认识到，依照本发明可以组合所描述的实施例的各种特征。在权利要求书中，措词“包括”并不排除其他模块或步骤的存在。

[0082] 此外，尽管单独被列出，但是多个模块或方法步骤可以由例如单个单元或处理器实现。此外，尽管单独的特征可能包含在不同的权利要求中，但是这些特征可能地可以有利地加以组合，并且包含在不同的权利要求中并不意味着特征的组合是不可行的。此外，特征包含于一种权利要求类别（例如方法权利要求）中并不意味着限于该类别，而是表示该特征同样可适当地应用于其他权利要求类别（例如装置权利要求）。此外，权利要求中特征的顺序并不意味着必须的任何特定顺序。并且，方法权利要求中各步骤的顺序并不意味着这些步骤必须按照该顺序来执行。相反地，这些步骤可以以任何适当的顺序执行。此外，单数形式的表述并没有排除复数。因此，对于“一”、“一个”、“第一”、“第二”等等的引用并没有排除复数。权利要求中的附图标记仅仅是标号，而不应当将其视为对权利要求的范围的限制。

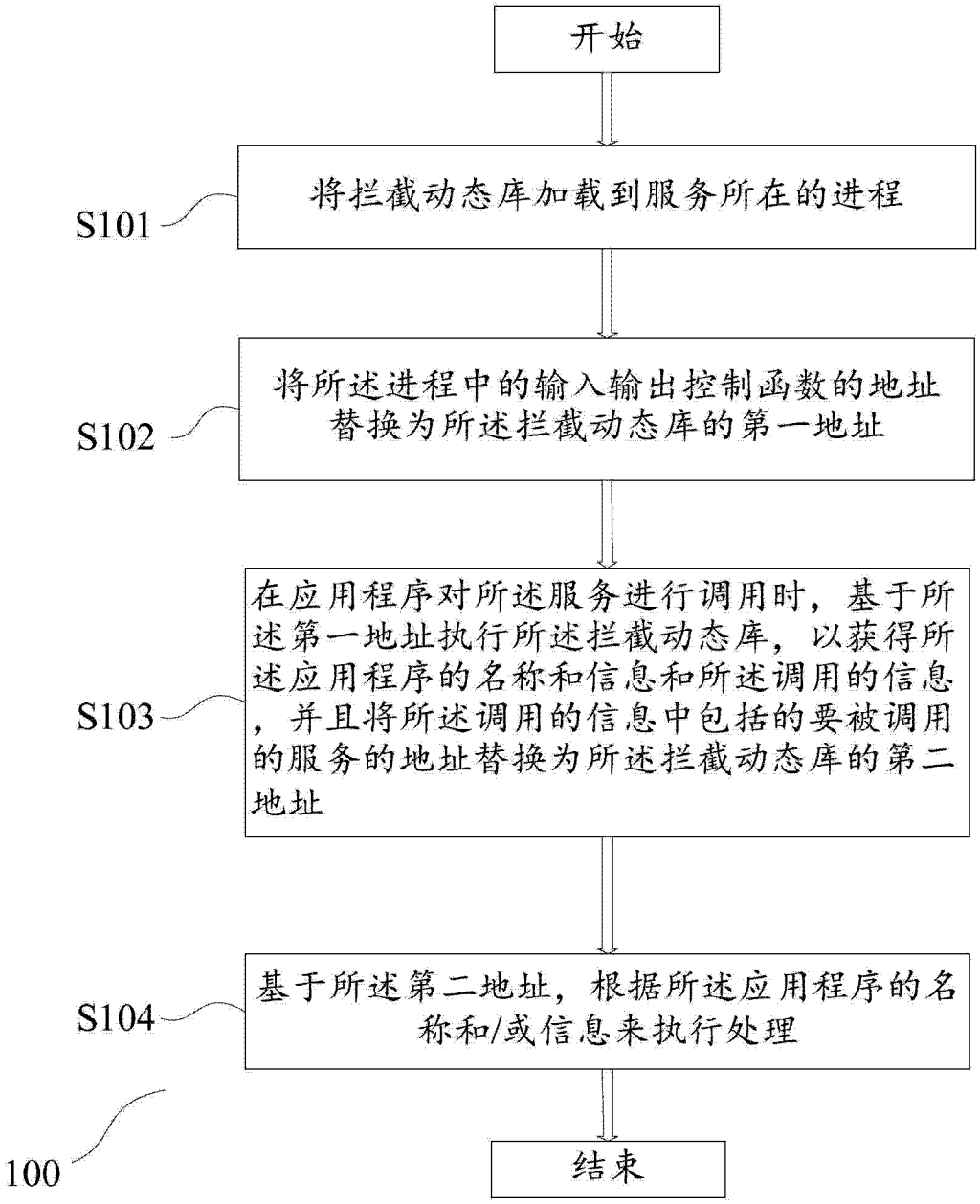

开始
S101
将拦截动态库加载到服务所在的进程
S102
将所述进程中的输入输出控制函数的地址替换为所述拦截动态库的第一地址
S103
在应用程序对所述服务进行调用时，基于所述第一地址执行所述拦截动态库，以获得所述应用程序的名称和信息和所述调用的信息，并且将所述调用的信息中包括的要被调用的服务的地址替换为所述拦截动态库的第二地址
S104
基于所述第二地址，根据所述应用程序的名称和/或信息来执行处理
结束
100

图 1

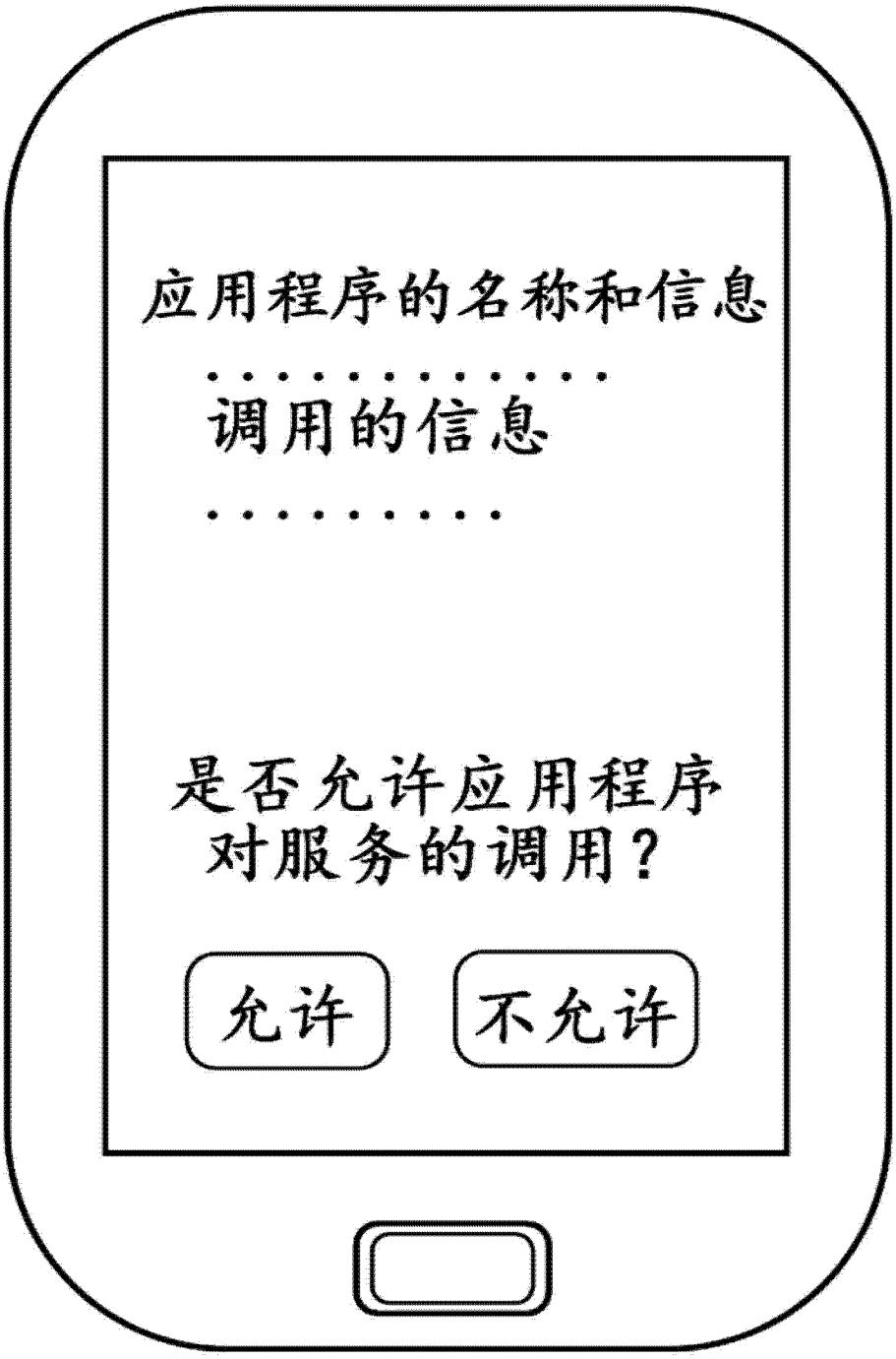


图 2

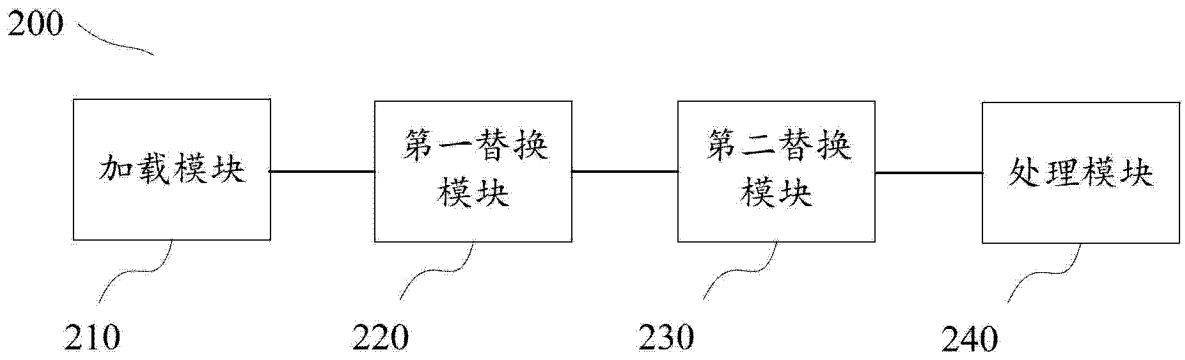


图 3