(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119180030 A
(43)申请公布日 2024.12.24

(21)申请号 202410117593.3

(22)申请日 2024.01.26

(71)申请人 北京小米移动软件有限公司
地址 100085 北京市海淀区西二旗中路33号院6号楼8层018号

(72)发明人 王宝林 张倞诚 张云鹏

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
专利代理师 靳玫

(51)Int.Cl.
*G06F 21/56*(2013.01)
*G06F 21/12*(2013.01)
*G06F 21/57*(2013.01)

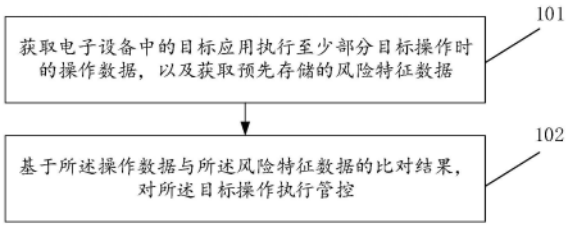
权利要求书2页 说明书12页 附图7页

(54)发明名称

# 风险管控方法、装置、存储介质和电子设备

(57)摘要

本公开提供一种风险管控方法、装置、存储介质和电子设备,其中,所述方法包括:获取电子设备中的目标应用执行至少部分目标操作时的操作数据,以及获取预先存储的风险特征数据;所述风险特征数据是所述目标应用利用所述电子设备中的系统漏洞执行非法操作时产生的数据;基于所述操作数据与所述风险特征数据的比对结果,对所述目标操作执行管控。本公开实施例提供的方法,有助于提高电子设备中的操作系统的安全性。




CN 119180030 A

1.一种风险管控方法,其特征在于,所述方法包括:

获取电子设备中的目标应用执行至少部分目标操作时的操作数据,以及获取预先存储的风险特征数据;所述风险特征数据是所述目标应用利用所述电子设备中的系统漏洞执行非法操作时产生的数据;

基于所述操作数据与所述风险特征数据的比对结果,对所述目标操作执行管控。

2.根据权利要求1所述的方法,其特征在于,所述获取预先存储的风险特征数据,包括:

获取所述电子设备中的第一应用传输的风险特征数据;所述风险特征数据是设备服务器在确定电子设备存在系统漏洞后发送至所述第一应用,所述目标应用未连接至所述设备服务器。

3.根据权利要求1所述的方法,其特征在于,所述获取电子设备中的目标应用执行至少部分目标操作时的操作数据,包括:

对电子设备中的多个目标接口进行监听;

当监听到所述电子设备中的目标应用调用任一个所述目标接口时,获取所述目标应用对所述目标接口的调用信息、和/或所述目标应用的系统权限信息;

将所述调用信息、和/或所述系统权限信息确定为所述操作数据。

4.根据权利要求3所述的方法,其特征在于,所述目标接口是所述目标应用与所述电子设备中的第二应用交互的接口;

所述目标操作包括以下至少一项:

基于所述目标接口调用第二应用;

基于所述目标接口从所述第二应用获取到目标权限后,执行指定操作。

5.根据权利要求1所述的方法,其特征在于,所述基于所述操作数据与所述风险特征数据的比对结果,对所述目标操作执行管控,包括:

当所述操作数据与所述风险特征数据的比对结果指示所述目标操作存在风险时,对所述目标操作执行第一管控;所述第一管控至少包括:将所述目标操作的操作数据传输至设备服务器。

6.根据权利要求5所述的方法,其特征在于,所述当所述操作数据与所述风险特征数据的比对结果指示所述目标操作存在风险时,对所述目标操作执行第一管控,包括:

当确定所述操作数据与所述风险特征数据的特征相似度大于或等于第一阈值时,允许所述目标应用继续执行目标操作,或者,控制所述目标应用停止执行目标操作。

7.根据权利要求6所述的方法,其特征在于,所述当所述操作数据与所述风险特征数据的比对结果指示所述目标操作存在风险时,对所述目标操作执行第一管控,包括:

当确定所述操作数据与所述风险特征数据的特征相似度大于或等于第二阈值时,控制所述目标应用停止执行目标操作;所述第一阈值小于所述第二阈值。

8.根据权利要求6或7所述的方法,其特征在于,所述控制所述目标应用停止执行目标操作,包括以下至少一项:

关闭所述目标应用的指定权限;

阻断所述目标应用通过目标接口调用第二应用的操作;所述目标接口是所述目标应用与所述电子设备中的第二应用交互的接口;

设置所述第二应用仅能被目标应用调用,所述目标应用的风险数值小于指定阈值。

9.根据权利要求1所述的方法,其特征在于,所述基于所述操作数据与所述风险特征数据的比对结果,对所述目标操作执行管控,包括:

当所述操作数据与所述风险特征数据的比对结果指示所述目标操作不存在风险时,对所述目标操作执行第二管控;

其中,所述第二管控包括:允许所述目标应用继续执行目标操作。

10.一种风险管控装置,其特征在于,所述装置包括:

获取模块,用于获取电子设备中的目标应用执行至少部分目标操作时的操作数据,以及获取预先存储的风险特征数据;所述风险特征数据是所述目标应用利用所述电子设备中的系统漏洞执行非法操作时产生的数据;

管控模块,用于基于所述操作数据与所述风险特征数据的比对结果,对所述目标操作执行管控。

11.一种电子设备,其特征在于,包括:

处理器;

用于存储处理器可执行指令的存储器;

其中,所述处理器被配置为通过运行所述可执行指令以实现权利要求1~9任一所述方法的步骤。

12.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现权利要求1~9任一所述方法的步骤。

# 风险管控方法、装置、存储介质和电子设备

## 技术领域

[0001] 本公开技术方案涉及数据安全技术领域,尤其涉及一种风险管控方法、装置、存储介质和电子设备。

## 背景技术

[0002] 电子设备中设置有系统自带的应用(简称为系统应用),用户在拿到电子设备之后,还会根据自己的使用需求额外安装一些第三方应用。例如,当电子设备是手机时,常见的系统应用有:手机管家、应用权限管理、短信等等;常见的第三方应用有:短视频播放软件、修图软件等等。

[0003] 由于系统应用是电子设备出厂时自带的应用,可靠性是较高的,因此系统应用通常具有较高的权限;而第三方应用是其他厂商提供的,可靠性是未知的,因此第三方应用通常具有较低的权限。

[0004] 用户在电子设备中运行第三方应用的时候,通常会授予第三方应用访问系统应用的权限,例如访问通讯录的权限、获取用户相册的权限、获取用户身份信息的权限等等。这就使得非法人员在发现系统漏洞之后,容易利用第三方应用与系统应用之间的交互关系执行一些非法操作。基于此,需要提供一种解决方案。

## 发明内容

[0005] 有鉴于此,本公开提供一种风险管控方法、装置、存储介质和电子设备,有助于提高电子设备中的操作系统的安全性。

[0006] 根据本公开实施例的第一方面,提供了一种风险管控方法,所述方法包括:

[0007] 获取电子设备中的目标应用执行至少部分目标操作时的操作数据,以及获取预先存储的风险特征数据;所述风险特征数据是所述目标应用利用所述电子设备中的系统漏洞执行非法操作时产生的数据;

[0008] 基于所述操作数据与所述风险特征数据的比对结果,对所述目标操作执行管控。

[0009] 根据本公开实施例的第二方面,提供了一种风险管控装置,所述装置包括:

[0010] 获取模块,用于获取电子设备中的目标应用执行至少部分目标操作时的操作数据,以及获取预先存储的风险特征数据;所述风险特征数据是所述目标应用利用所述电子设备中的系统漏洞执行非法操作时产生的数据;

[0011] 管控模块,用于基于所述操作数据与所述风险特征数据的比对结果,对所述目标操作执行管控。

[0012] 根据本公开实施例的第三方面,提供了一种电子设备,包括:

[0013] 处理器;

[0014] 用于存储处理器可执行指令的存储器;

[0015] 其中,所述处理器被配置为通过运行所述可执行指令以实现第一方面任一所述风险管控方法的步骤。

[0016] 根据本公开实施例的第四方面,提供了一种非临时性计算机可读存储介质,其上存储有计算机程序,该程序被处理器执行时实现上述第一方面任一所述风险管控方法的步骤。

[0017] 根据本公开实施例的第五方面,提供了一种计算机程序,所述计算机程序被处理器执行时实现上述第一方面任一所述风险管控方法的步骤。

[0018] 本公开实施例提供的技术方案可以包括以下有益效果:

[0019] 由于预先存储有目标应用攻击系统漏洞所执行的非法操作的数据,因此,在获取到目标应用执行至少部分目标操作时的操作数据后,可以将操作数据与风险特征数据进行比对,得到比对结果。

[0020] 通过比对结果,能够确定目标应用的目标操作是否也按照上述非法操作的方式攻击系统漏洞,以便根据比对结果对目标操作执行相应的管控操作。

[0021] 这样,在电子设备存在系统漏洞时,即使用户尚未更新操作系统,也能够根据上述方法及时发现目标应用的目标操作是否存在风险、并能够及时进行管控,有助于提高电子设备中的操作系统的安全性。

[0022] 应当理解的是,以上的一般描述和后文的细节描述仅是示例性和解释性的,并不能限制本公开。

## 附图说明

[0023] 此处的附图被并入说明书中并构成本说明书的一部分,示出了符合本公开的实施例,并与说明书一起用于解释本公开的原理。

[0024] 图1是本公开根据一示例性实施例示出的一种风险管控方法的流程图;

[0025] 图2是本公开根据一示例性实施例示出的一种风险管控方法的应用框架图;

[0026] 图3是本公开根据一示例性实施例示出的另一种风险管控方法的流程图;

[0027] 图4是本公开根据一示例性实施例示出的另一种风险管控方法的应用框架图;

[0028] 图5是本公开根据一示例性实施例示出的另一种风险管控方法的应用框架图;

[0029] 图6是本公开根据一示例性实施例示出的另一种风险管控方法的应用框架图;

[0030] 图7是本公开根据一示例性实施例示出的一种风险管控装置的结构示意图;

[0031] 图8是本公开根据一示例性实施例示出的一种电子设备的结构示意图。

## 具体实施方式

[0032] 这里将详细地对示例性实施例进行说明,其示例表示在附图中。下面的描述涉及附图时,除非另有表示,不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反,它们仅是与如所附权利要求书中所详述的、本公开的一些方面相一致的装置和方法的例子。

[0033] 在本公开使用的术语是仅仅出于描述特定实施例的目的,而非旨在限制本公开。在本公开和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式,除非上下文清楚地表示其他含义。还应当理解,本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0034] 应当理解,尽管在本公开可能采用术语第一、第二、第三等来描述各种信息,但这

些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如,在不脱离本公开范围的情况下,第一信息也可以被称为第二信息,类似地,第二信息也可以被称为第一信息。取决于语境,如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0035] 电子设备中设置有系统自带的应用(简称为系统应用),用户在拿到电子设备之后,还会根据自己的使用需求额外安装一些第三方应用。例如,当电子设备是手机时,常见的系统应用有:手机管家、应用权限管理、短信等等;常见的第三方应用有:短视频播放软件、修图软件等等。

[0036] 用户在电子设备中运行第三方应用的时候,通常会授予第三方应用访问系统应用的权限,或者是允许第三方应用调用系统应用的接口,执行特定的服务。以下进行示例性说明:

[0037] 例如,当用户在智能手机上安装并使用一款天气预报应用时,该第三方天气预报应用可能需要访问系统的定位服务(如GPS信息)来获取用户的实时地理位置信息,以便提供准确的本地天气预报。这时,系统会弹出权限请求提示,询问用户是否允许这款天气预报应用访问位置信息,并在用户允许访问位置信息之后、提供相应的访问接口、访问路径。

[0038] 又如,用户下载并安装了一款社交媒体应用,为了能够将拍摄的照片直接分享到该社交平台,这款第三方社交媒体应用就需要获得访问设备相机和相册的权限,以便调用系统相机接口拍照,并读取或写入手机相册中的图片。

[0039] 再比如,一些第三方日历应用需要获取访问系统日历的权限,以便添加、编辑或查看用户的日程安排。这就需要用户授权第三方日历应用访问系统日历应用的接口、然后通过接口在系统日历中编辑一些日程。

[0040] 这就使得,非法人员容易利用第三方应用所拥有的权利,窃取用户相册内的数据、编辑系统日历中的日程等。

[0041] 现有技术中,想要进行漏洞修补,往往需要经历如下过程:发布新的操作系统、或安全补丁,提示用户安装,等待用户确认安装(用户未必愿意更新),这就使得在用户尚未更新新的操作系统(或者安全补丁)的情况下,非法分子随时可以利用系统漏洞执行非法操作,这会导致用户的信息被非法窃取等情况。

[0042] 因此,需要提供一种方案,能够在用户未更新操作系统的情况下,保障电子设备和操作系统的安全性。

[0043] 以下进行简单介绍:

[0044] 假设第三方应用(第三方日历)想要实现:在系统日历中添加用户日程这个目标操作的时候,需要执行以下部分操作:

[0045] 操作一、发送想要调用目标接口的调用请求。

[0046] 操作二、获取到目标接口的信息之后,通过目标接口调用系统应用(系统日历)。

[0047] 操作三、在系统日历中写入用户日程。

[0048] 上述三个操作中,操作三最容易被非法人员利用来执行非法操作。

[0049] 例如,非法人员在在通过操作一、操作二合法的获取到对系统日历的调用接口的访问权限之后,将操作三替换为如下非法操作:

[0050] 在系统日历中写入非法广告、恶意链接、敏感信息或其他侵犯用户隐私的数据等

等,或者是被非法人员利用更改用户想要写入的信息等等。

[0051] 因此,在上述三个操作中,需要格外管控操作三,避免被非法人员利用执行相应的非法操作。也即,可以根据目标操作的前几个操作(例如操作一、或者操作二)确定是否为风险操作,进而在目标操作尚未执行完毕(未执行操作三)的时候及时制止。

[0052] 也即:通过获取至少部分目标操作(例如上述操作一、操作二)的操作数据,以及预先存储的风险特征数据,将操作数据与风险特征数据进行比对,能够确定目标操作是否与风险特征数据吻合,从而根据不同的比对结果对目标操作执行不同程度的管控。

[0053] 以下进行详细介绍:

[0054] 图1是本公开根据一示例性实施例示出的一种风险管控方法的流程图,如图1所示,所述方法包括以下步骤:

[0055] 步骤101,获取电子设备中的目标应用执行至少部分目标操作时的操作数据,以及获取预先存储的风险特征数据;所述风险特征数据是所述目标应用利用所述电子设备中的系统漏洞执行非法操作时产生的数据。

[0056] 目标应用,是指电子设备中安装的任一个或任意多个第三方应用;目标操作,是目标应用需要调用系统应用的组件、或是需要获取特定的系统权限才能够执行的操作。例如:在系统日历中写入日程、对系统相册中的图像进行编辑等操作。

[0057] 风险特征数据是预先发现目标应用利用电子设备中的系统漏洞执行非法操作之后根据这些非法操作提取出的数据,是预先存储到电子设备中的。

[0058] 例如,当非法人员发现系统相机应用接口中存在系统漏洞,正常情况下,第三方应用调用此接口是为了合法获取拍照或录制视频权限。然而,该漏洞使得恶意目标应用可以利用这一权限执行额外的非法操作。例如:在用户授权目标应用使用相机功能后,该应用不仅进行正常的拍照或录像,还在后台悄悄地将拍摄的照片或视频上传至远程服务器,这会侵犯用户的隐私权。

[0059] 此时,风险特征数据包括如下操作的数据:目标应用获取系统相机应用接口的请求、目标应用利用获取到系统相机应用接口之后在后台非法启动相机或者是非法修改、删除、增加相册中的图像、再或者是非法上传到服务器。

[0060] 步骤102,基于所述操作数据与所述风险特征数据的比对结果,对所述目标操作执行管控。

[0061] 可以理解的是,如果操作数据是目标应用执行的非法操作,那么这个非法操作的操作数据会与风险特征数据一致或相似,因此,通过将操作数据与风险特征数据进行比对,能够确定操作数据是否存在风险。

[0062] 这样,可以根据比对结果对目标操作执行相应的管控,确保目标操作不会攻击电子设备和电子设备的操作系统。

[0063] 由于预先存储有目标应用攻击系统漏洞所执行的非法操作的数据,因此,在获取到目标应用执行至少部分目标操作时的操作数据后,可以将操作数据与风险特征数据进行比对,得到比对结果。

[0064] 比对方式可以是:将两种数据一一对应,确定是否一致;或者是将两种数据指示的应用想要执行的操作行为一一进行比对,确定是否一致,本方案不对具体的比对方式进行限定。

[0065] 通过比对结果,能够确定目标应用的目标操作是否也按照上述非法操作的方式攻击系统漏洞,以便根据比对结果对目标操作执行相应的管控操作。

[0066] 这样,在电子设备存在系统漏洞时,即使用户尚未更新操作系统,也能够根据上述方法及时发现目标应用的目标操作是否存在风险、并能够及时进行管控,有助于提高电子设备中的操作系统的安全性。

[0067] 可选的,执行步骤101获取预先存储的风险特征数据,包括:

[0068] 获取所述电子设备中的第一应用传输的风险特征数据;所述风险特征数据是设备服务器在确定电子设备存在系统漏洞后发送至所述第一应用,所述目标应用未连接至所述设备服务器。

[0069] 第一应用,是电子设备中安装的系统应用,主要是系统应用中用来保障电子设备安全的安全管控应用。其中,为了保障电子设备出厂后能够更好的为用户提供服务,厂家会设置设备服务器,用于为电子设备提供一些重要服务,例如系统升级、账户服务等服务。由于第一应用是系统应用,因此第一应用能够与电子设备的操作系统的设备服务器通信;而第三方应用不是系统应用,不能够与设备服务器通信,仅能够与第三方服务器通信。

[0070] 设备服务器在发现电子设备存在系统漏洞之后,会实时更新相应的风险特征数据,并将实时更新的风险特征数据传输到第一应用。这样,在第三方应用对应的第三方服务器未更新第三方应用、或者是用户并未手动更新操作系统的情况下,也可以将第一应用获取到的风险特征数据存储到电子设备中,并通过电子设备中存储的风险特征数据与目标应用的操作数据的比对结果,执行相应的管控。

[0071] 图2是本公开根据一示例性实施例示出的一种风险管控方法的应用框架图,如图2所示:

[0072] 第一应用与设备服务器通信,获取到风险特征数据,并存储到核心服务中。目标应用(第三方应用)在执行目标操作时,会和核心服务中的部分服务组件或接口产生交互,会产生操作数据。

[0073] 此时,可以在核心服务中将操作数据与风险特征数据进行比对,得到比对结果。

[0074] 可选的,图3是本公开根据一示例性实施例示出的另一种风险管控方法的流程图,如图3所示,执行步骤101获取电子设备中的目标应用执行至少部分目标操作时的操作数据时,包括以下步骤:

[0075] 步骤301,对电子设备中的多个目标接口进行监听。

[0076] 目标接口是从电子设备的组件(例如核心服务)中预先确定出的组件接口,目标应用在执行目标操作时,需要调用这些目标接口。因此,可以通过电子设备中的核心服务实现对目标接口的监听。

[0077] 步骤302,当监听到所述电子设备中的目标应用调用任一个所述目标接口时,获取所述目标应用对所述目标接口的调用信息、和/或所述目标应用的系统权限信息。

[0078] 其中,调用信息,包括但不限于:

[0079] 调用的应用的信息:主要指发起调用请求的应用程序(目标应用)的信息(例如身份标识)。

[0080] Uri信息(Uniform Resource Identifier,统一资源标识符):指向要操作的数据或服务的位置,在跨应用通信时,Uri可以用来表示要访问的具体内容、数据或者功能模块。

[0081] 调用类型:调用的动作类型或者是对被调用服务的请求类型,例如“ACTION_INSERT”表示要在日历应用中插入一个新事件。被调用的应用包名:待调用的系统应用的信息。

[0082] 被调用的应用的信息,包括但不限于:应用组件名、调用行为名、和/或应用版本号。其中,被调用的应用组件通常指的为电子设备中的核心服务,在Intent(一种消息传递对象,用于描述应用组件之间的交互请求)中通过组件类名或动作(action)来指定。例如,如果是要启动另一个应用的特定Activity,则需要提供该Activity的完整类名;而如果是使用隐式Intent,则会通过action和类别(category)来匹配系统中能够响应这个Intent的目标组件。

[0083] 这里,可以注意到,目标接口是所述目标接口是所述目标应用与所述电子设备中的第二应用交互的接口;此时,所述目标操作包括以下至少一项:

[0084] 基于所述目标接口调用第二应用;基于所述目标接口从所述第二应用获取到目标权限后,执行指定操作。

[0085] 目标应用的系统权限信息,包括但不限于:

[0086] 权限列表:列出目标应用为了执行目标操作而必须获得的系统权限集合,例如读取电话状态、访问外部存储、获取设备位置等;以及当前已经拥有的系统权限集合。

[0087] 权限级别:说明这些权限属于普通权限还是危险权限。在某些操作系统中,危险权限需要用户在运行时明确授权,而普通权限则会在安装时自动授予。

[0088] 权限用途描述:解释为何目标应用需要这些权限,以及它们如何与调用的操作或服务关联起来。例如,如果一个日历应用请求了“ACTION_INSERT”动作来插入新事件,那么它可能需要读写日历数据的权限以便实际进行数据操作。

[0089] 缺失权限的影响:用于告知如果不授权特定权限将会导致哪些功能受限或无法正常使用。

[0090] 权限管理策略:说明目标应用如何处理和保护通过权限获取的用户数据,以及用户可以在何处查看或更改已授权的权限。

[0091] 目标应用在调用任一个目标接口时,都会产生以上至少部分信息,将这些信息全部收集起来作为操作数据,也即执行步骤303。

[0092] 步骤303,将所述调用信息、和/或所述系统权限信息确定为所述操作数据。

[0093] 图4是本公开根据一示例性实施例示出的另一种风险管控方法的应用框架图,如图4所示:

[0094] 核心服务包括第一核心服务401,以及第二核心服务402。

[0095] 其中,第一核心服务401中包括活动管理服务以及活动管理服务提供的四大核心服务4011,当活动管理服务接收到目标应用发送的调用请求之后,会确定目标应用想要调用的服务和服务组件所对应的接口。

[0096] 其中,四大核心服务4011包括:

[0097] ActivityStarter(活动启动服务)、ActiveServices(服务管理服务)、ContentProviderHelper(内容提供者管理服务)、BroadcastQueue(广播队列管理服务)。

[0098] 其中,ActivityStarter通常指的是启动新Activity(一种组件)相关逻辑的组件。它负责处理Intent的解析、目标Activity的查找以及执行相应的启动流程,确保从一个

Activity切换到另一个Activity时的正确性与安全性。ActiveServices是操作系统中负责管理运行中的后台服务(Background Services)以及前台服务(Foreground Services)的重要组件。它承担着服务的启动、绑定、停止等生命周期管理职责,以及根据系统资源状况优化服务调度,确保服务的高效运行及系统资源的有效利用。ContentProviderHelper是指协助开发者或系统调用Content Provider(内容提供者)的相关工具类或服务模块,用于简化对系统或应用间共享数据的访问和管理。BroadcastQueue是消息传递机制中的一部分,主要用于管理系统内部和应用之间发送的广播消息。它按照优先级将接收到的广播事件有序地放入队列中,然后分发给注册了对应接收器的组件进行处理,保证了广播消息的安全可靠传递。

[0099] 第二核心服务402中包括:

[0100] 4021:SecurityManagerService(安全管理服务),用于从第一应用中获取到设备服务器发送的风险特征数据,并传输到4022中进行存储。

[0101] 4022:DefenseManager(防御管理模块),存储有从4023获取到的风险特征数据(可以进行分类存储,例如根据不同的行为类型进行分类存储、或者是根据操作时长、操作次数分类存储,再或者是根据设定的标识分类存储),并用于将风险特征数据传输到4021中进行比对。

[0102] 4023:DefenseChecker(防御模块),用于监听四大核心服务4011对应的目标接口,并将监听到的数据作为操作数据进行存储(可以采用与4022中相同的存储方式进行存储),然后在获取到4022传输的风险特征数据之后,将操作数据与风险特征数据进行比对,得到比对结果。

[0103] 可选的,执行步骤102基于所述操作数据与所述风险特征数据的比对结果,对所述目标操作执行管控,包括如下两种管控方式:

[0104] 方式一、针对目标操作存在风险的情况:

[0105] 当所述操作数据与所述风险特征数据的比对结果指示所述目标操作存在风险时,对所述目标操作执行第一管控;所述第一管控至少包括:将所述目标操作的操作数据传输至设备服务器。

[0106] 当确定目标操作存在风险时,为了防止目标应用再次通过目标操作去攻击电子设备,需要及时将操作数据上传至设备服务器,完成风险的上报。这样,可以,可以在应用商店下架这些风险应用,或者是统一给这些应用设置较低的系统权限,或者是提示用户卸载这些应用等等。这里的上传方式可以是通过第一应用转发到设备服务器。

[0107] 除了将目标操作的操作数据传输至设备服务器这种管控方式之外,还包括其他的管控方式,例如:根据比对结果确定是否控制目标应用停止执行目标操作,也即:允许所述目标应用继续执行目标操作,或者,控制所述目标应用停止执行目标操作。

[0108] 这里,可以进一步限定比对方式是:

[0109] 分别提取操作数据与风险特征数据的特征,然后通过特征比对的方式,得到特征相似度数值。当二者的特征相似度数值大于或等于第一阈值时,认为目标操作存在风险;当二者的相似度数值小于第一阈值时,认为目标操作不存在风险。

[0110] 也即,述当所述操作数据与所述风险特征数据的比对结果指示所述目标操作存在风险时,对所述目标操作执行第一管控,包括:

[0111] 当确定所述操作数据与所述风险特征数据的特征相似度大于或等于第一阈值时，允许所述目标应用继续执行目标操作，或者，控制所述目标应用停止执行目标操作。

[0112] 示例性的，这里的第一阈值可以设置为75％。

[0113] 那么如何确定到底是允许目标应用继续执行还是不允许目标应用继续执行，可以通过如下方式确定：

[0114] 当确定所述操作数据与所述风险特征数据的特征相似度大于或等于第二阈值时，控制所述目标应用停止执行目标操作；所述第一阈值小于所述第二阈值。

[0115] 这里，假设第二阈值为100％(仅是示例性的数值)，那么，当二者的特征相似度大于或等于100％时，认为目标操作一定为非法操作，则直接控制目标应用停止执行目标操作(这里通常是指目标应用尚未执行完目标操作的时候，若是目标应用已经执行完目标操作，可以设定目标应用后续不允许执行目标操作)。

[0116] 当二者的特征相似度大于或等于75％，但是小于100％时，可以仅将操作数据传输至设备服务器即可，此时允许目标应用继续执行目标操作。

[0117] 通过上述方法，能够及时制止目标操作，或者是有效预防非法人员通过目标操作攻击电子设备的行为。

[0118] 需要注意的是，第一阈值和第二阈值的具体数值可以结合实际需求进行调整。

[0119] 图5是本公开根据一示例性实施例示出的另一种风险管控方法的应用框架图，如图5所示，第二核心服务402还包括：

[0120] 4024：APPSecurityHelper(应用安全辅助模块)，用于在DefenseChecker4023通过比对结果确定目标应用的操作数据存在一定风险时，控制目标应用停止执行目标操作(不允许目标应用通过活动管理服务提供的接口调用第二应用)。这里的第二应用也是系统应用。

[0121] 进一步的，控制所述目标应用停止执行目标操作，包括以下至少一项：

[0122] 关闭所述目标应用的指定权限；阻断所述目标应用通过目标接口调用第二应用的操作；所述目标接口是所述目标应用与所述电子设备中的第二应用交互的接口；设置所述第二应用仅能被目标应用调用，所述目标应用的风险数值小于指定阈值。

[0123] 指定权限，包括但不限于：用于执行非法操作的权限、风险特征数据中所体现的权限。设置第二应用仅能被信任的应用(例如系统应用)调用，通过APPSecurityHelper4024，或者是活动管理服务阻断目标应用通过目标接口调用第二应用的操作。

[0124] 其中，本公开的其中一个示例中，当第一应用中包括能够进行权限管理的应用时，关闭所述目标应用的指定权限是由第一应用完成的。此时，可以包括以下方式：

[0125] 设备服务器给第一应用发送非法特征数据之后，第一应用确定出非法特征数据所使用的权限，直接通过第一应用中的权限管理应用关闭目标应用的指定权限。或者是，DefenseChecker4023在比对之后，确定比对结果指示目标操作存在风险后，通过4022-4021传输到第一应用，然后通过第一应用中的权限管理应用关闭目标应用的指定权限。具体如图6所示：

[0126] 第一应用601包括：

[0127] 应用6011：PermissionManagerAPP(权限管理应用)，用于设置管理各个应用的系统权限。

[0128] 应用6012:Security App(安全应用),用于对电子设备进行安全防护。

[0129] 方式二、针对目标操作不存在风险的情况:

[0130] 当所述操作数据与所述风险特征数据的比对结果指示所述目标操作不存在风险时,对所述目标操作执行第二管控;其中,所述第二管控包括:允许所述目标应用继续执行目标操作。

[0131] 此时,第二管控为:既不上报、也不阻止目标应用的目标操作。仅通过比对的方式监控目标操作是否存在风险。

[0132] 示例性的,确定目标操作不存在风险的方式可以是:操作数据与风险特征数据的特征相似度小于第一阈值(例如75%)。

[0133] 对于前述的各方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本公开并不受所描述的动作顺序的限制,因为依据本公开,某些步骤可以采用其他顺序或者同时进行。

[0134] 其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于可选实施例,所涉及的动作和模块并不一定是本公开所必须的。

[0135] 与前述应用功能实现方法实施例相对应,本公开还提供了风险管控装置及相应的终端的实施例。

[0136] 本公开提供了一种计算机程序,所述计算机程序被处理器执行时实现上述任一所述风险管控方法的步骤。

[0137] 图7是本公开根据一示例性实施例示出的一种风险管控装置的结构示意图,如图7所示,该风险管控装置可以包括:

[0138] 获取模块701,用于获取电子设备中的目标应用执行至少部分目标操作时的操作数据,以及获取预先存储的风险特征数据;所述风险特征数据是所述目标应用利用所述电子设备中的系统漏洞执行非法操作时产生的数据。

[0139] 管控模块702,用于基于所述操作数据与所述风险特征数据的比对结果,对所述目标操作执行管控。

[0140] 可选的,所述获取模块701在用于获取预先存储的风险特征数据时,用于:

[0141] 获取所述电子设备中的第一应用传输的风险特征数据;所述风险特征数据是设备服务器在确定电子设备存在系统漏洞后发送至所述第一应用,所述目标应用未连接至所述设备服务器。

[0142] 可选的,所述获取模块701在用于获取电子设备中的目标应用执行至少部分目标操作时的操作数据时,用于:

[0143] 对电子设备中的多个目标接口进行监听。

[0144] 当监听到所述电子设备中的目标应用调用任一个所述目标接口时,获取所述目标应用对所述目标接口的调用信息、和/或所述目标应用的系统权限信息。

[0145] 将所述调用信息、和/或所述系统权限信息确定为所述操作数据。

[0146] 可选的,所述目标接口是所述目标应用与所述电子设备中的第二应用交互的接口;

[0147] 所述目标操作包括以下至少一项:

[0148] 基于所述目标接口调用第二应用;基于所述目标接口从所述第二应用获取到目标

权限后,执行指定操作。

[0149] 可选的,管控模块702在用于基于所述操作数据与所述风险特征数据的比对结果,对所述目标操作执行管控时,用于:

[0150] 当所述操作数据与所述风险特征数据的比对结果指示所述目标操作存在风险时,对所述目标操作执行第一管控;所述第一管控至少包括:将所述目标操作的操作数据传输至设备服务器。

[0151] 可选的,管控模块702在用于当所述操作数据与所述风险特征数据的比对结果指示所述目标操作存在风险时,对所述目标操作执行第一管控时,用于:

[0152] 当确定所述操作数据与所述风险特征数据的特征相似度大于或等于第一阈值时,允许所述目标应用继续执行目标操作,或者,控制所述目标应用停止执行目标操作。

[0153] 可选的,管控模块702在用于当所述操作数据与所述风险特征数据的比对结果指示所述目标操作存在风险时,对所述目标操作执行第一管控时,用于:

[0154] 当确定所述操作数据与所述风险特征数据的特征相似度大于或等于第二阈值时,控制所述目标应用停止执行目标操作;所述第一阈值小于所述第二阈值。

[0155] 可选的,管控模块702在用于控制所述目标应用停止执行目标操作时,用于执行以下至少一项:

[0156] 关闭所述目标应用的指定权限;阻断所述目标应用通过目标接口调用第二应用的操作;所述目标接口是所述目标应用与所述电子设备中的第二应用交互的接口;设置所述第二应用仅能被目标应用调用,所述目标应用的风险数值小于指定阈值。

[0157] 可选的,管控模块702在用于基于所述操作数据与所述风险特征数据的比对结果,对所述目标操作执行管控时,用于:

[0158] 当所述操作数据与所述风险特征数据的比对结果指示所述目标操作不存在风险时,对所述目标操作执行第二管控;其中,所述第二管控包括:允许所述目标应用继续执行目标操作。

[0159] 对于装置实施例而言,由于其基本对应于方法实施例,所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的,其中上述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本公开方案的目的。本领域普通技术人员在不付出创造性劳动的情况下,即可以理解并实施。

[0160] 相应的,本公开实施例提供了一种电子设备,包括:处理器;用于存储处理器可执行指令的存储器;其中,上述处理器被配置为通过运行所述可执行指令以实现上述任一方法的步骤。

[0161] 图8是本公开根据一示例性实施例示出的一种电子设备的结构示意图。例如,电子设备800可以是用户设备,可以具体为移动电话,计算机,数字广播终端,消息收发设备,游戏控制台,平板设备,医疗设备,健身设备,个人数字助理,可穿戴设备如智能手表、智能眼镜、智能手环、智能跑鞋等。

[0162] 参照图8,电子设备800可以包括以下一个或多个组件:处理组件802,存储器804,电源组件806,多媒体组件808,音频组件810,输入/输出(I/O)的接口812,传感器组件814,

以及通信组件816。

[0163] 处理组件802通常控制电子设备800的整体操作,诸如与显示,电话呼叫,数据通信,相机操作和记录操作相关联的操作。处理组件802可以包括一个或多个处理器820来执行指令,以完成上述的方法的全部或部分步骤。此外,处理组件802可以包括一个或多个模块,便于处理组件802和其他组件之间的交互。例如,处理组件802可以包括多媒体模块,以方便多媒体组件808和处理组件802之间的交互。

[0164] 存储器804被配置为存储各种类型的数据以支持在设备800的操作。这些数据的示例包括用于在电子设备800上操作的任何应用程序或方法的指令,联系人数据,电话簿数据,消息,图片,视频等。存储器804可以由任何类型的易失性或非易失性存储设备或者它们的组合实现,如静态随机存取存储器(SRAM),电可擦除可编程只读存储器(EEPROM),可擦除可编程只读存储器(EPROM),可编程只读存储器(PROM),只读存储器(ROM),磁存储器,快闪存储器,磁盘或光盘。

[0165] 电源组件806为电子设备800的各种组件提供电力。电源组件806可以包括电源管理系统,一个或多个电源,及其他与为电子设备800生成、管理和分配电力相关联的组件。

[0166] 多媒体组件808包括在上述电子设备800和用户之间的提供一个输出接口的屏幕。在一些实施例中,屏幕可以包括液晶显示器(LCD)和触摸面板(TP)。如果屏幕包括触摸面板,屏幕可以被实现为触摸屏,以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。上述触摸传感器可以不仅感测触摸或滑动动作的边界,而且还检测与上述触摸或滑动操作相关的持续时间和压力。在一些实施例中,多媒体组件808包括一个前置摄像头和/或后置摄像头。当电子设备800处于操作模式,如拍摄模式或视频模式时,前置摄像头和/或后置摄像头可以接收外部的多媒体数据。每个前置摄像头和后置摄像头可以是一个固定的光学透镜系统或具有焦距和光学变焦能力。

[0167] 音频组件810被配置为输出和/或输入音频信号。例如,音频组件810包括一个麦克风(MIC),当电子设备800处于操作模式,如呼叫模式、记录模式和语音识别模式时,麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器804或经由通信组件816发送。在一些实施例中,音频组件810还包括一个扬声器,用于输出音频信号。

[0168] I/O接口812为处理组件802和外围接口模块之间提供接口,上述外围接口模块可以是键盘,点击轮,按钮等。这些按钮可包括但不限于:主页按钮、音量按钮、启动按钮和锁定按钮。

[0169] 传感器组件814包括一个或多个传感器,用于为电子设备800提供各个方面的状态评估。例如,传感器组件814可以检测到电子设备800的打开/关闭状态,组件的相对定位,例如上述组件为电子设备800的显示器和小键盘,传感器组件814还可以检测电子设备800或电子设备800一个组件的位置改变,用户与电子设备800接触的存在或不存在,电子设备800方位或加速/减速和电子设备800的温度变化。传感器组件814可以包括接近传感器,被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件814还可以包括光传感器,如CMOS或CCD图像传感器,用于在成像应用中使用。在一些实施例中,该传感器组件814还可以包括加速度传感器,陀螺仪传感器,磁传感器,压力传感器或温度传感器。

[0170] 通信组件816被配置为便于电子设备800和其他设备之间有线或无线方式的通信。电子设备800可以接入基于通信标准的无线网络,如WiFi,4G或5G,4G LTE、5G NR或它们的

组合。在一个示例性实施例中,通信组件816经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中,上述通信组件816还包括近场通信(NFC)模块,以促进短程通信。例如,在NFC模块可基于射频识别(RFID)技术,红外数据协会(IrDA)技术,超宽带(UWB)技术,蓝牙(BT)技术和其他技术来实现。

[0171] 在示例性实施例中,电子设备800可以被一个或多个应用专用集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理设备(DSPD)、可编程逻辑器件(PLD)、现场可编程门阵列(FPGA)、控制器、微控制器、微处理器或其他电子元件实现,用于执行上述方法。

[0172] 在示例性实施例中,还提供了一种非临时性计算机可读存储介质,例如包括指令的存储器804,当存储介质中的指令由电子设备800的处理器820执行时,使得电子设备800能够执行上述任一方法。

[0173] 所述非临时性计算机可读存储介质可以是ROM、随机存取存储器(RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0174] 本领域技术人员在考虑说明书及实践这里公开的发明后,将容易想到本公开的其它实施方案。本公开旨在涵盖本公开的任何变型、用途或者适应性变化,这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的,本公开的真正范围和精神由下面的权利要求指出。

[0175] 应当理解的是,本公开并不局限于上面已经描述并在附图中示出的精确结构,并且可以在不脱离其范围进行各种修改和改变。本公开的范围仅由所附的权利要求来限制。

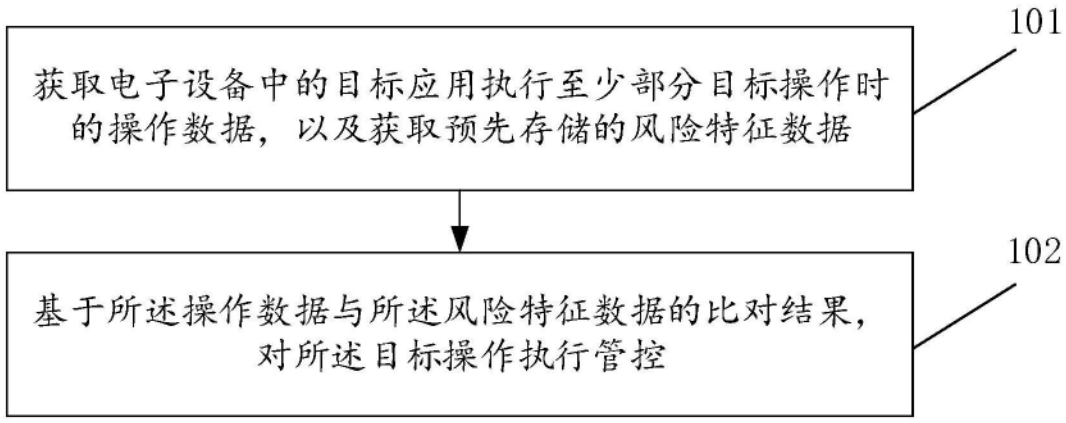

101
获取电子设备中的目标应用执行至少部分目标操作时的操作数据，以及获取预先存储的风险特征数据
102
基于所述操作数据与所述风险特征数据的比对结果，对所述目标操作执行管控

图1

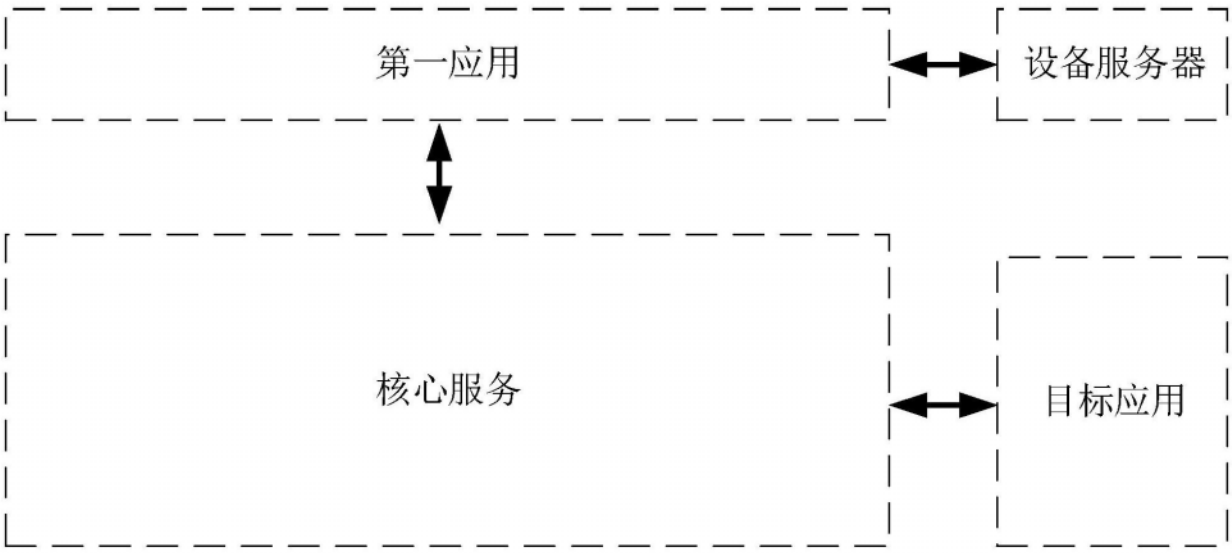

第一应用
设备服务器
核心服务
目标应用

图2

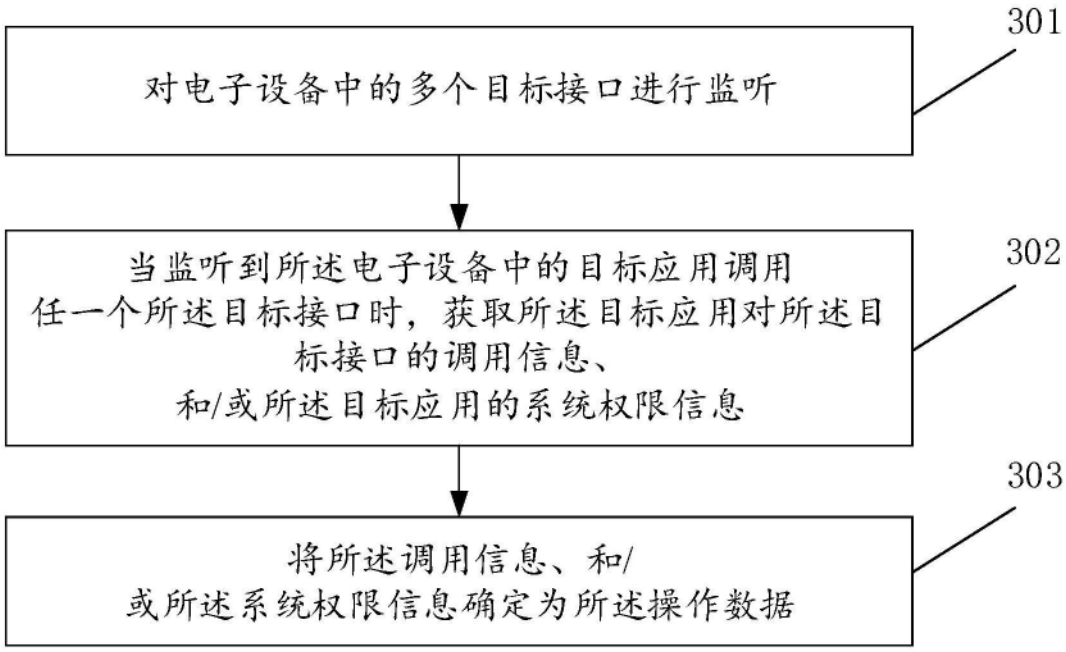

301
对电子设备中的多个目标接口进行监听
302
当监听到所述电子设备中的目标应用调用任一个所述目标接口时，获取所述目标应用对所述目标接口的调用信息、和/或所述目标应用的系统权限信息
303
将所述调用信息、和/或所述系统权限信息确定为所述操作数据

图3

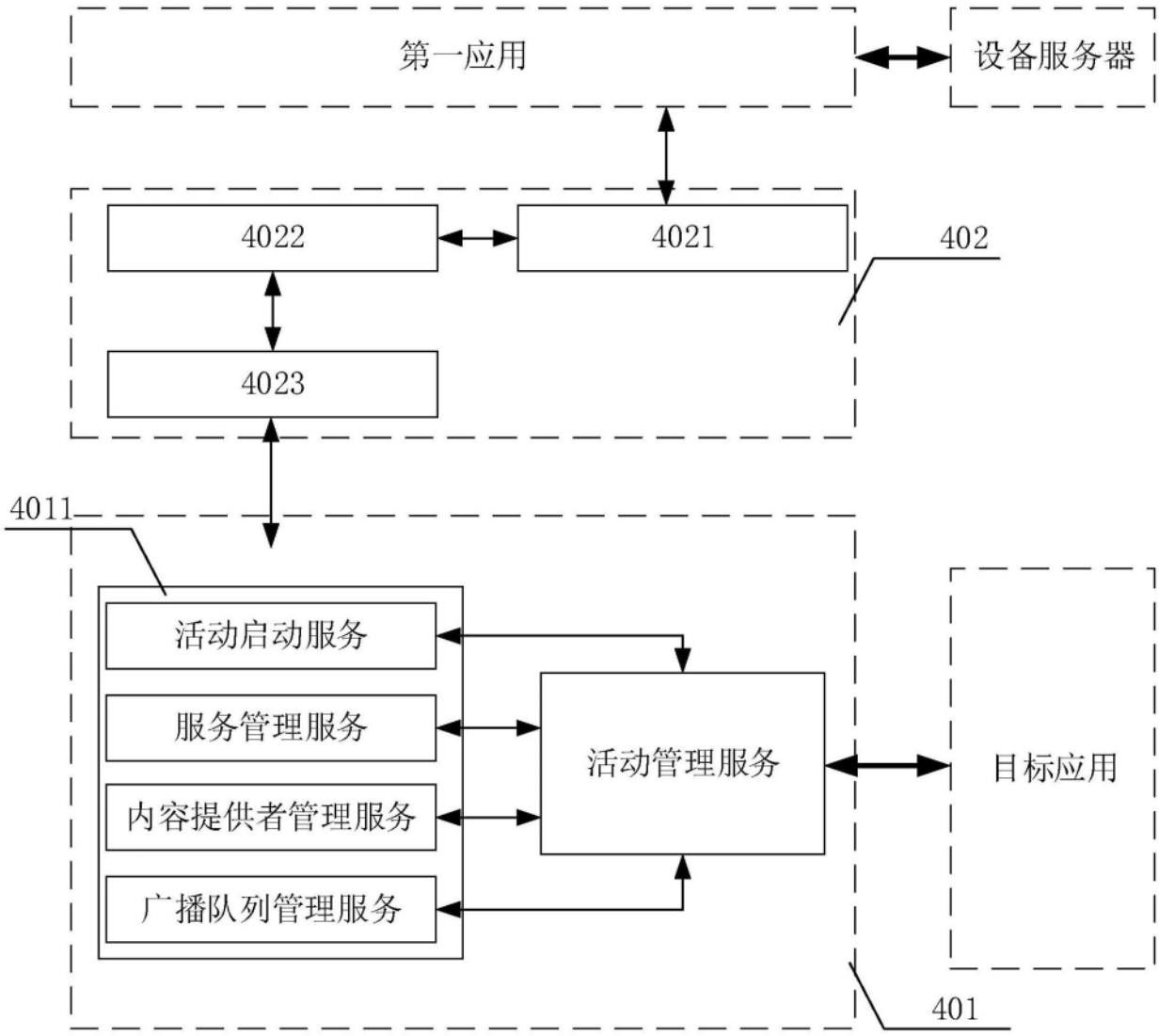

第一应用
设备服务器
4022
4021
402
4023
4011
活动启动服务
服务管理服务
内容提供者管理服务
广播队列管理服务
活动管理服务
目标应用
401

图4

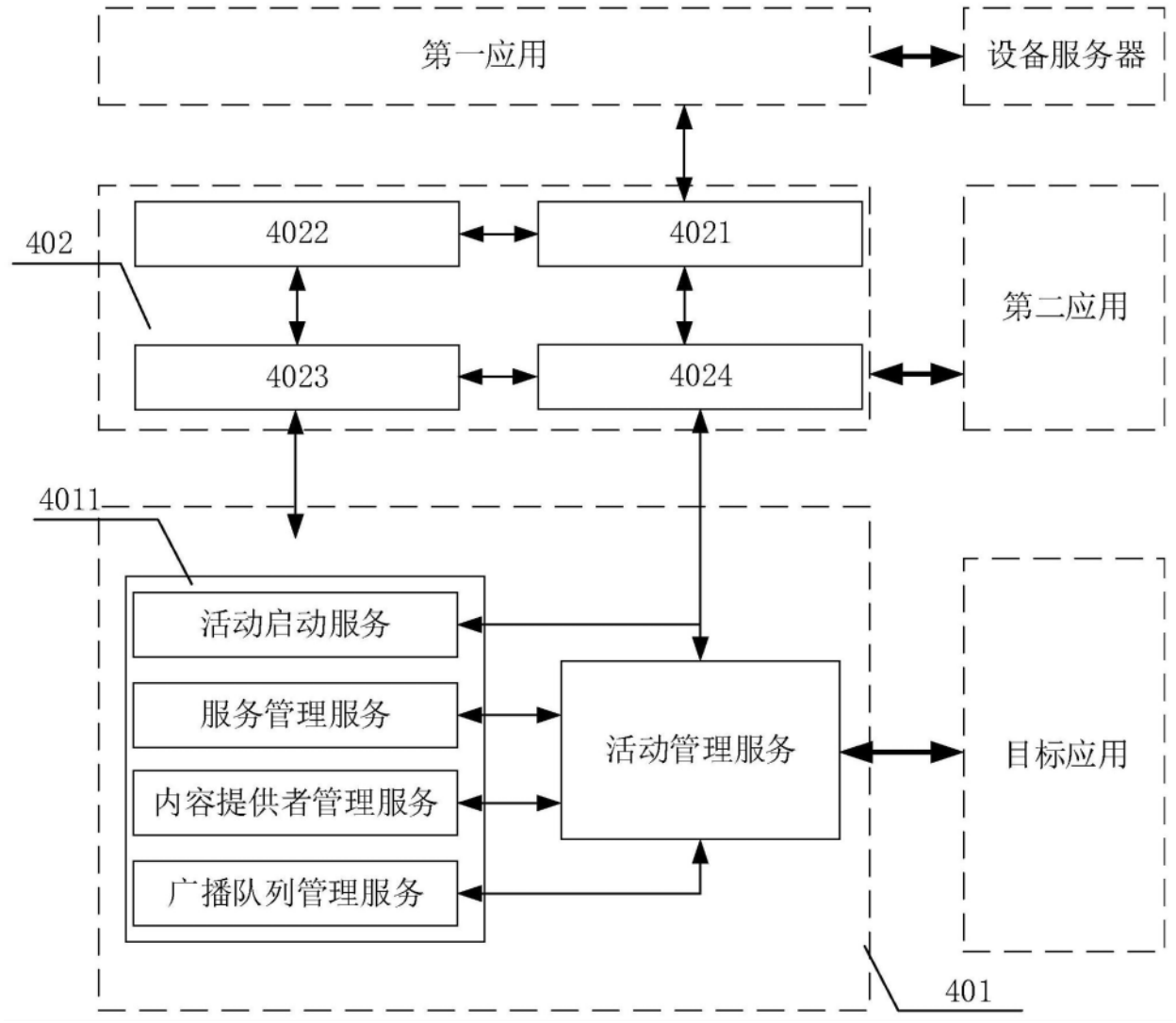

第一应用
设备服务器
402
4022
4021
4023
4024
第二应用
4011
活动启动服务
服务管理服务
内容提供者管理服务
广播队列管理服务
活动管理服务
目标应用
401

图5

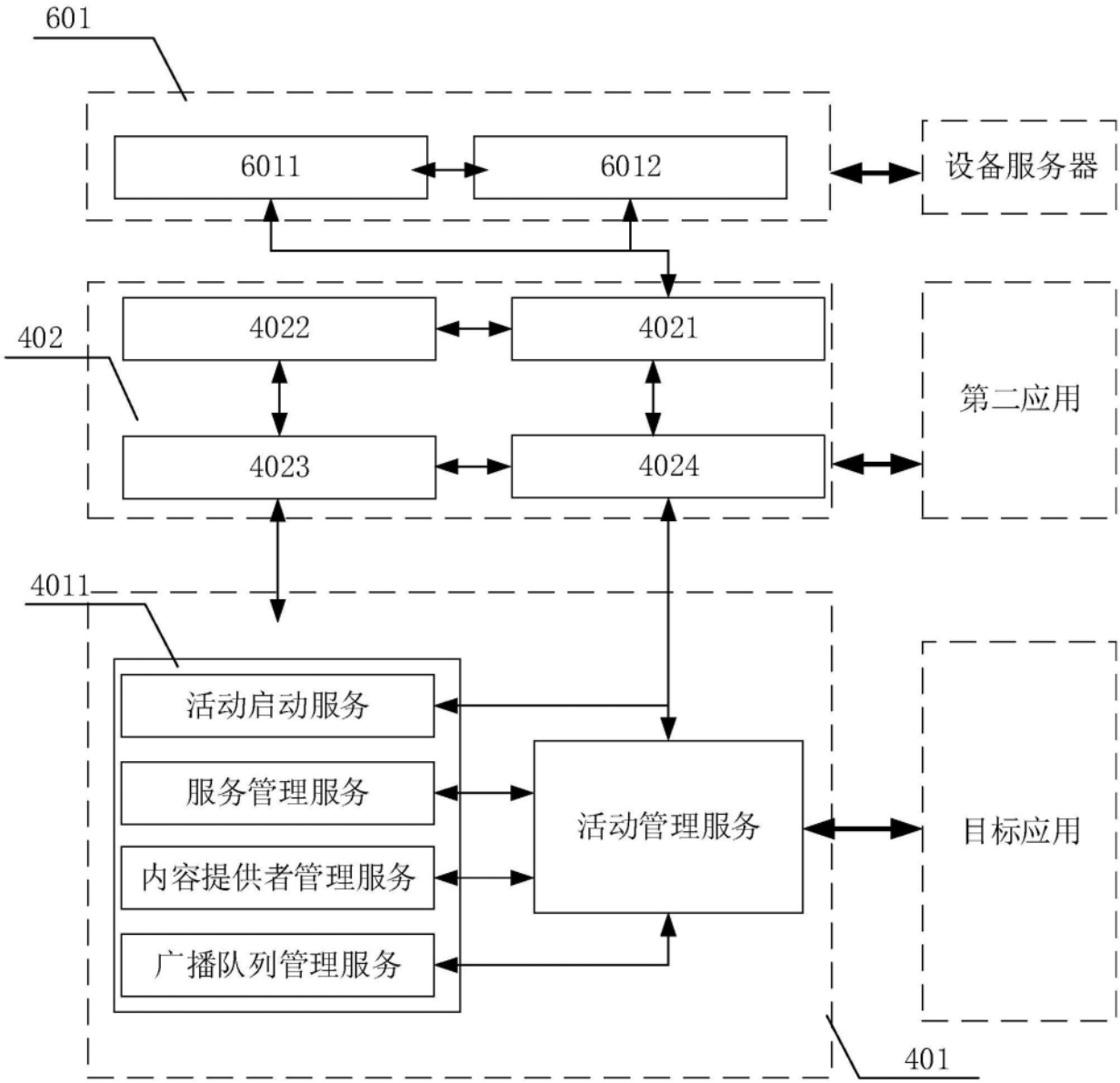

601
6011
6012
设备服务器
402
4022
4021
第二应用
4023
4024
4011
活动启动服务
服务管理服务
内容提供者管理服务
广播队列管理服务
活动管理服务
目标应用
401

图6

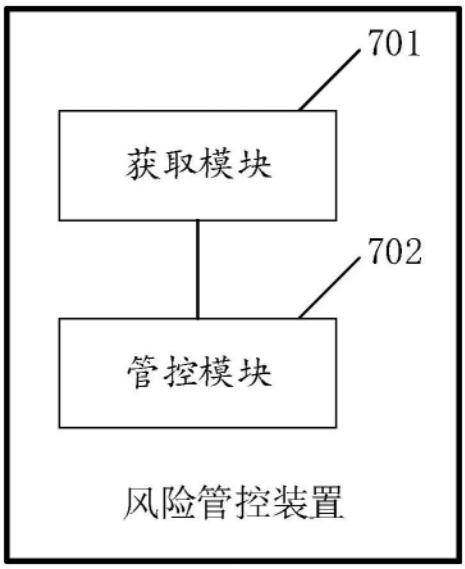



图7

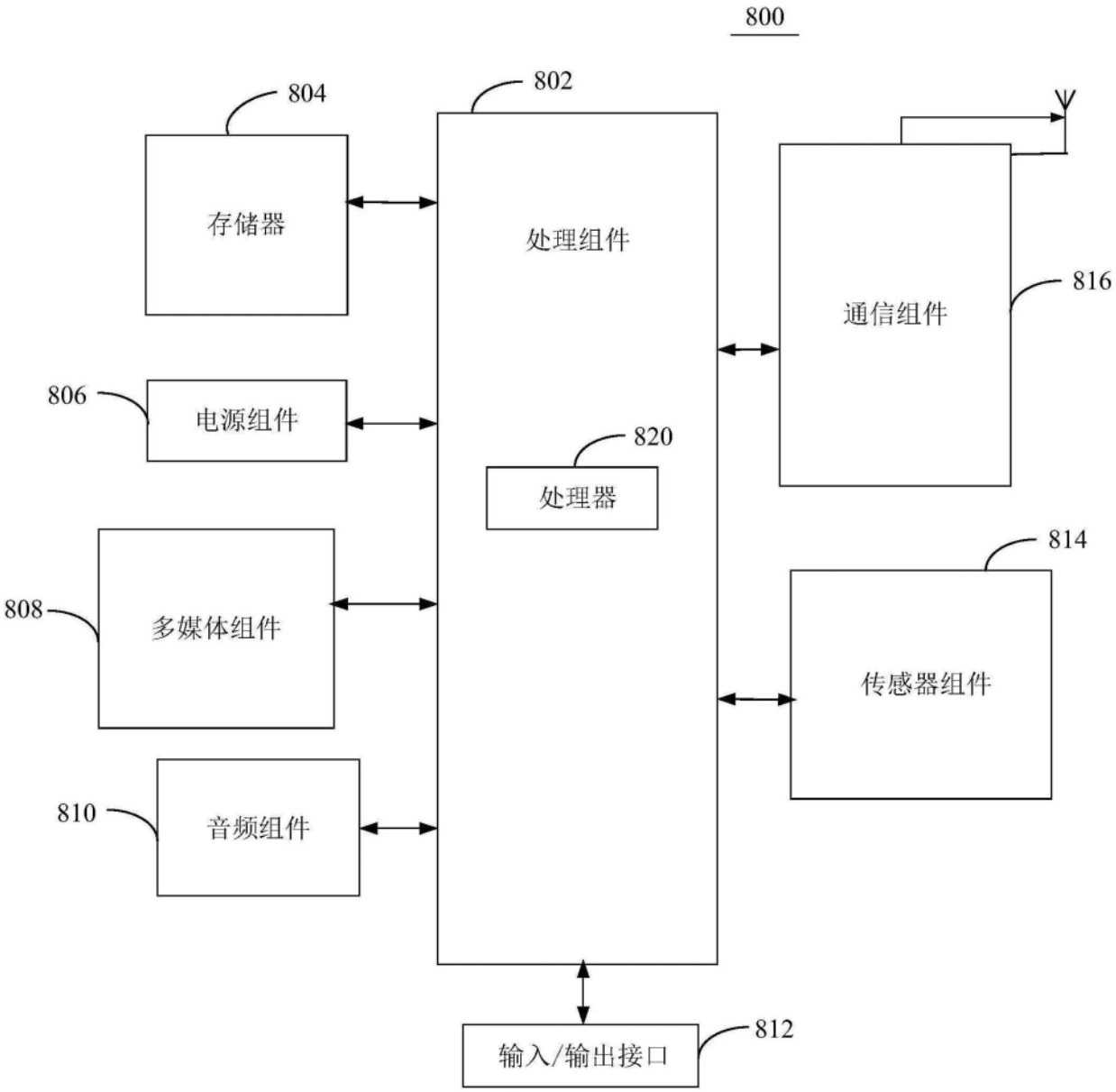

800
804
存储器
802
处理组件
816
通信组件
806
电源组件
820
处理器
814
808
多媒体组件
传感器组件
810
音频组件
812
输入/输出接口

图8