

小程序的安全扫描方法、装置以及电子设备

技术领域

[01] 本说明书涉及计算机应用领域，尤其涉及一种小程序的安全扫描方法、装置以及电子设备。

5 背景技术

[02] 小程序，是指一种基于特定编程语言开发完成，无需下载和安装，就可以使用的移动端 APP。小程序的最大特点是使用便捷，无需手动在移动端的操作系统中安装，但通常需要依托于大型 APP 作为载体进行使用；例如，在一些大型 APP 的服务端通常会对接第三方的小程序开发平台，开发人员通过小程序开发平台完成小程序的开发后，可以
10 将开发完成的小程序发布至该大型 APP 的服务端，与该大型 APP 实现对接。

发明内容

[03] 本说明书提出一种小程序的安全扫描方法，所述方法包括：

[04] 获取待发布的目标小程序；

[05] 调用安全扫描策略组合对所述目标小程序进行多维度的安全扫描；

15 [06] 当所述目标小程序通过所述多维度的安全扫描时，将所述目标小程序发布至与搭载所述目标小程序的目标 APP 对应的服务端。

[07] 可选的，所述安全扫描策略组合包括以下安全扫描策略中多个的组合：

[08] 对所述目标小程序进行恶意代码扫描；

[09] 对所述目标小程序进行安全漏洞扫描；

20 [10] 对与所述目标小程序对应的服务端接口进行安全漏洞扫描。

[11] 可选的，所述对所述目标小程序进行恶意代码扫描，包括以下示出的扫描方式中的一个或者多个的组合：

[12] 检测所述目标小程序是否携带攻击载荷；

[13] 检测所述目标小程序调用的所有函数是否存在为所述目标小程序定义的合法调用函
25 数以外的恶意调用函数；

- [14]检测所述目标小程序调用的媒体以及文本内容是否存在违规内容。
- [15]可选的,所述对所述目标小程序进行安全漏洞扫描,包括以下示出的扫描方式中的一个或者多个的组合:
- [16]检测所述目标小程序是否存在敏感信息泄露漏洞;
- 5 [17]检测所述目标小程序是否存在 HTML 代码漏洞;
- [18]检测所述目标小程序是否存在 JS 代码漏洞;
- [19]检测所述目标小程序是否存在非法外部资源引用漏洞。
- [20]可选的,所述对所述目标小程序的服务端接口进行安全漏洞扫描,包括:
- [21]解析所述目标小程序的服务端接口;
- 10 [22]对解析出的所述服务端接口进行接口漏洞扫描。
- [23]本说明书还提出一种小程序的安全扫描装置,所述装置包括:
- [24]获取模块,获取待发布的目标小程序;
- [25]扫描模块,调用安全扫描策略组合对所述目标小程序进行多维度的安全扫描;
- [26]发布模块,当所述目标小程序通过所述多维度的安全扫描时,将所述目标小程序发
- 15 布至与搭载所述目标小程序的目标 APP 对应的服务端。
- [27]可选的,所述扫描模块进一步执行以下扫描策略中的多个的组合:
- [28]对所述目标小程序进行恶意代码扫描;
- [29]对所述目标小程序进行安全漏洞扫描;
- [30]对与所述目标小程序对应的服务端接口进行安全漏洞扫描。
- 20 [31]可选的,所述扫描模块进一步执行以下恶意代码扫描方式中的一个或者多个的组合:
- [32]检测所述目标小程序是否携带攻击载荷;
- [33]检测所述目标小程序调用的所有函数是否存在为所述目标小程序定义的合法调用函数以外的恶意调用函数;
- [34]检测所述目标小程序调用的媒体以及文本内容是否存在违规内容。
- 25 [35]可选的,所述扫描模块进一步执行以下安全漏洞扫描方式中的一个或者多个的组合:

- [36]检测所述目标小程序是否存在敏感信息泄露漏洞;
- [37]检测所述目标小程序是否存在 HTML 代码漏洞;
- [38]检测所述目标小程序是否存在 JS 代码漏洞;
- [39]检测所述目标小程序是否存在非法外部资源引用漏洞。
- 5 [40]可选的,所述扫描模块进一步:
- [41]解析所述目标小程序的服务端接口;
- [42]对解析出的所述服务端接口进行接口漏洞扫描。
- [43]本说明书还提出一种电子设备,包括:
- [44]处理器;
- 10 [45]用于存储机器可执行指令的存储器;
- [46]其中,通过读取并执行所述存储器存储的与机器学习模型的训练的控制逻辑对应的机器可执行指令,所述处理器被促使:
- [47]获取待发布的目标小程序;
- [48]调用安全扫描策略组合对所述目标小程序进行多维度的安全扫描;
- 15 [49]当所述目标小程序通过所述多维度的安全扫描时,将所述目标小程序发布至与搭载所述目标小程序的目标 APP 对应的服务端。
- [50]在本说明书中,通过调用安全扫描策略组合对待发布的目标小程序进行多维度的安全扫描,并在该目标小程序通过所述多维度的安全扫描时,再将该目标小程序发布至与搭载所述目标小程序的目标 APP 对应的服务端,从而可以有效避免将一些恶意小程序
- 20 发布上线,而影响用户的使用安全。

附图说明

- [51]图 1 是本说明书一实施例示出的小程序的安全扫描方法的流程图;
- [52]图 2 为本说明书一实施例示出的扫描平台对目标小程序进行多维度安全扫描的流程图;
- 25 [53]图 3 是本说明书一实施例提供的承载一种小程序的安全扫描装置的电子设备所涉及的硬件结构图;

[54]图 4 是本说明书一实施例提供的所述一种小程序的安全扫描装置的逻辑框图。

具体实施方式

[55]本说明书旨在提出一种对待发布的小程序进行多维度的安全扫描，进而避免将一些恶意小程序发布上线的技术方案。

- 5 [56]在实现时，搭载小程序的 APP 对应的服务端，可以对接独立的小程序开发平台，开发人员可以基于自身的业务需求通过该开发平台来开发小程序，并通过上述小程序开发平台与上述服务端进行通信，将开发完成的小程序打包上传提交至上述服务端进行审核。

- 10 [57]而在搭载小程序的 APP 对应的服务端上，可以部署用于对待发布小程序进行安全扫描的扫描平台，在该扫描平台中可以预先搭载安全扫描策略组合。当该扫描平台收到开发人员通过上述开发平台上传提交的待发的小程序后，可以调用上述安全扫描策略组合，对该待发布的小程序进行多维度的安全扫描；

[58]例如，在实际应用中，上述安全扫描策略组合，具体可以包括对小程序进行恶意代码扫描、安全漏洞扫描、以及对小程序对应的服务端接口进行安全漏洞扫描等安全策略。

- 15 上述扫描平台可以通过调用上述安全扫描策略组合，对小程序执行恶意代码扫描、安全漏洞扫描、服务端接口漏洞扫描等维度的安全扫描。

[59]如果待发布的小程序通过了上述多维度的安全扫描，此时可以将该小程序发布至搭载该小程序的 APP 对应的服务端；反之，如果待发布的小程序未通过上述多维度的安全扫描，表明该小程序可能为恶意小程序，可以直接终止该小程序的发布流程。

- 20 [60]可见，扫描平台通过调用安全扫描策略组合对待发布的目标小程序进行多维度的安全扫描，并在该目标小程序通过所述多维度的安全扫描时，再将该目标小程序发布至与搭载所述目标小程序的目标 APP 对应的服务端，从而可以有效避免将一些恶意小程序发布上线，而影响用户的使用安全。

[61]下面通过具体实施例并结合具体的应用场景对本说明书进行描述。

- 25 [62]请参考图 1，图 1 是本说明书一实施例提供的一种小程序的安全扫描方法，应用于扫描平台，执行以下步骤：

[63]步骤 102，获取待发布的目标小程序；

[64]上述扫描平台，具体可以包括对待发布的小程序进行安全扫描的业务平台。在实际应用中，上述扫描平台具体可以部署于搭载小程序的 APP 对应的服务端上；例如，在一种实现方式中，当承载上述服务端的硬件环境具体可以是一个分布式的服务器集群，在这种情况下，可以在该服务器集群中选定一台或者多台物理服务器，作为承载上述扫描平台的硬件环境，来搭建上述扫描平台。

[65]或者，在实际应用中，上述扫描平台也可以独立于上述服务端进行单独部署；例如，上述扫描平台可以独立部署于上述服务端以外的一台或者多台物理服务器上，并与上述服务端保持对接。

[66]其中，搭载小程序的 APP，具体可以包括原生的 APP，也可以包括基于 web 技术开发的 Web APP，在本说明书中不进行特别限定。

[67]在本说明书中，搭载小程序的 APP 对应的服务端，还可以对接独立的小程序开发平台；

[68]其中，该小程序开发平台具体可以是上述搭载小程序的 APP 的运营方独立运营的小程序开发平台，也可以与上述搭载小程序的 APP 的运营方具有合作关系的第三方小程序开发平台，在本说明书中不进行特别限定。

[69]开发人员可以基于自身的业务需求通过上述小程序开发平台来开发小程序，并在小程序开发完成后，将开发完成的小程序打包上传提交至上述扫描平台进行安全扫描。其中，对开发完成的小程序进行打包，具体是指将开发完成的小程序的执行代码封装成可执行的程序的过程。

[70]在实际应用中，上述小程序开发平台，可以与上述扫描平台保持数据连接，并面向开发人员提供一个与开发完成的小程序对应的上传入口，当小程序开发完成后，开发人员可以通过触发上述上传入口，将打包完成的小程序通过上述数据连接上传提交至上述扫描平台。

[71]例如，在一种实现方式中，上述数据连接具体可以是一个 http 连接，上述上传入口具体可以是开发平台通过可视化界面向开发人员提供的一个用于触发上传开发完成的小程序的功能按钮。

[72]当开发人员完成小程序的执行代码的开发后，可以对执行代码进行编译打包，然后触发上述功能按钮，将打包后的小程序上传至上述扫描平台。而上述开发平台在后台监听到针对上述功能按钮的触发事件时，可以在后台构建一个用于承载打包完成的小程序

的 http 请求包（比如 http post 请求），然后将打包完成的小程序作为载荷携带在该 http 请求包，比你更将该 http 请求包通过上述 http 连接上传至上述扫描平台。而上述扫描平台在收到上述 http 请求包时，可以对该 http 请求包进行解析，获取该 http 请求包中携带的打包完成的小程序。

5

[73] 步骤 104，调用安全扫描策略组合对所述目标小程序进行多维度的安全扫描；

[74] 在本说明书中，在上述扫描平台上可以预先搭载安全扫描策略组合。在该安全扫描策略组合中，可以包括预先定义的多个维度的安全扫描策略。其中，对于该安全扫描策略组合中的每一个维度的安全扫描策略，都可以预先开发完成一个对应的调用接口；从而，当上述扫描平台接收到上述开发平台上传的待发布的目标小程序后，可以进入安全扫描流程，依次调用各安全扫描策略的调用接口，执行各安全扫描策略，对该目标小程序进行多维度的安全扫描。

[75] 其中，需要说明的是，上述安全扫描策略组合中的安全扫描策略的调用顺序，在本说明书中不进行特别限定，在实际应用中，本领域技术人员可以基于实际的业务需求来为各安全扫描策略设置优先级，并基于优先级来为各安全扫描策略设置调用顺序。

[76] 在示出的一种实施方式中，上述安全扫描策略组合中所包含的安全扫描策略，具体可以包括以下安全扫描策略的多个的组合：

[77] 对目标小程序进行恶意代码扫描；

[78] 对目标小程序进行安全漏洞扫描；

20 [79] 对与目标小程序对应的服务端接口进行安全漏洞扫描。

[80] 在这种情况下，上述扫描平台可以通过调用上述安全扫描策略组合，对小程序执行恶意代码扫描、安全漏洞扫描、服务端接口漏洞扫描等维度的安全扫描。

[81] 以下通过具体的实施例，以扫描平台对待发布的目标小程序执行恶意代码扫描、安全漏洞扫描、服务端接口漏洞扫描等三个维度的安全扫描为例进行详细说明。

25 [82] 请参见图 2，图 2 为本说明书示出的一种扫描平台对目标小程序进行多维度安全扫描的流程图。

[83] 如图 2 所示，在本实施例中，扫描平台对待发布的小程序进行安全扫描可以包括恶意代码扫描、安全漏洞扫描、服务端接口漏洞扫描等三个扫描维度。

[84]如图 2 所示,在示出的一种实施方式中,对目标小程序的恶意代码扫描,可以由以下示出的一个或者多个扫描程序组成:

[85]攻击载荷(payload)检测程序;

[86]恶意函数调用检测程序;

5 [87]恶意内容检测程序。

[88]其中,上述攻击载荷检测程序,具体用于检测上述目标小程序的载荷中是否携带攻击载荷;

[89]例如,在实现时,可以预先准备大量的已攻击载荷的样本;比如,攻击代码样本、攻击数据样本等;当需要对目标小程序进行攻击载荷检测时,可以解析小程序中的载荷
10 中的所有代码和数据,将解析出的这些代码和数据与预先准备的已知攻击载荷的样本进行对比分析,来确定该目标小程序的载荷中是否携带攻击载荷;如果确定出该目标小程序的载荷中携带攻击载荷,则可以判定该目标小程序为恶意小程序;如果确定出该目标小程序的载荷中携带攻击载荷,则可以判定该目标小程序为非恶意小程序,此时扫描通过。

15 [90]上述恶意函数调用检测程序,具体用于检测上述目标小程序调用的所有函数中是否存在为上述目标小程序定义的合法调用函数以外的恶意调用函数;

[91]例如,在实现时,对于每一个开发完成的小程序而言,可以预先定义若干种可调用的合法函数,或者定义一个可调函数的合法调用范围;比如,可以由开发者在小程序的代码中定义,也可以由搭载小程序的 APP 的运营方来单独定义;

20 [92]当需要对目标小程序进行恶意函数调用检测时,可以解析该目标小程序调用的所有函数,并确定该目标小程序调用的所有函数中,是否存在可调用的合法函数以外的函数,或者上述可调函数的合法调用范围以外的函数;如果存在,表明该目标小程序调用的所有函数中存在恶意函数,此时可以判定该目标小程序为恶意小程序;反之,如果不存在,表明该目标小程序调用的所有函数中不存在恶意函数,则可以判定该目标小程序为
25 费恶意小程序,此时扫描通过。

[93]上述恶意内容检测程序,具体用于检测上述目标小程序调用的媒体以及文本内容是否存在违规内容;

[94]例如,在实现时,可以预先定义大量的违规内容样本;比如,违规的文本关键词、

媒体片段等等；当需要对目标小程序进行恶意内容检测时，可以解析该目标小程序调用的所有媒体以及文本内容，将解析出的这些媒体以及文本内容，与上述违规内容样本进行比对分析，来确定该目标小程序调用的媒体以及文本内容中是否携带违规内容；如果确定出该目标小程序调用的媒体以及文本内容中是否携带违规内容，则可以判定该目标小程序为恶意小程序；反之，可以判定该目标小程序为非恶意小程序，此时扫描通过。

[95]请继续参见图 2，在示出的一种实施方式中，对所述目标小程序进行安全漏洞扫描，可以由以下示出的一个或者多个扫描程序组成：

[96]敏感信息泄露漏洞检测程序；

[97]HTML 代码漏洞检测程序；

10 [98]JS 代码漏洞检测程序；

[99]外部资源引用漏洞检测程序。

[100] 其中，上述敏感信息泄露漏洞检测程序，具体用于检测上述目标小程序是否存在敏感信息泄露漏洞；上述 HTML 代码漏洞检测程序，具体用于检测上述目标小程序是否存在 HTML 代码漏洞；上述 JS 代码漏洞检测程序，具体用于检测上述目标小程序是否存在 JS 代码漏洞；上述外部资源引用漏洞检测程序，具体用于检测上述目标小程序是否存在引用了非法外部资源的安全漏洞；比如，检测上述目标小程序是否引用了诸如非法的链接等，为目标小程序定义的合法外部资源以外的非法外部资源的漏洞；

[101] 其中，在实现时，扫描平台在调用以上示出的各个漏洞扫描程序，对上述目标小程序进行相关的漏洞扫描时，均可以通过调用扫描平台搭载的与各个漏洞扫描程序相关的漏洞扫描工具来完成；

[102] 例如，对于扫描平台而言，可以分别搭载与敏感信息泄露漏洞、HTML 代码漏洞、JS 代码漏洞以及外部资源引用漏洞对应的不同类型的漏洞扫描器，并配置对应的漏洞数据库，然后通过软件环境中分别运行以上各漏洞扫描器，对上述目标小程序进行扫描，与漏洞数据库进行比对分析，来识别和发现上述目标小程序中可能存在的安全漏洞。

[103] 当扫描平台通过执行以上各漏洞扫描程序，检测到上述目标小程序中存在相关的安全漏洞时，还可以将漏洞扫描结果反馈给上述目标小程序的开发人员，对相关的安全漏洞进行修复。当开发人员对安全漏洞修复后，可以通过小程序开发平台重新打包上传上述目标小程序，由上述扫描平台重新进行安全扫描。当然，当扫描平台通过执行以

上各漏洞扫描程序,检测到上述目标小程序中不存在相关的安全漏洞时,此时扫描通过。

[104] 请继续参见图 2,扫描平台除了可以对待发布的上述目标小程序进行恶意代码扫描和安全漏洞扫描以外,在示出的一种实施方式中,扫描平台还可以对上述目标小程序对应的服务端接口进行安全漏洞扫描。

5 [105] 在实现时,上述扫描平台可以解析出与该小程序中所有的功能相关的接口,并从解析出的这些接口中筛选和梳理出与该小程序对应的服务端接口,然后对这些服务端接口进行安全漏洞扫描;

[106] 例如,对于扫描平台而言,仍然可以搭载与服务端接口漏洞对应的漏洞扫描器,并配置对应的漏洞数据库,然后通过软件环境中分别运行以上漏洞扫描器,对上述目
10 标小程序的各服务端接口进行扫描,与漏洞数据库进行比对分析,来识别和发现这些服务端接口中可能存在的接口漏洞。

[107] 当扫描平台检测到上述目标小程序对应的服务端接口存在接口漏洞时,还可以将漏洞扫描结果反馈给上述目标小程序的开发人员,对接口漏洞进行修复。当开发人员对安全漏洞修复后,可以通过小程序开发平台重新打包上传上述目标小程序,由上述扫
15 描平台重新进行安全扫描。当然,如果通过扫描确认不存在服务端接口漏洞时,此时扫描通过。

[108] 其中,需要说明的是,在以上实施例,以扫描平台对待发布的目标小程序执行恶意代码扫描、安全漏洞扫描、服务端接口漏洞扫描等三个维度的安全扫描为例,仅为示例性的。在实际应用中,上述安全扫描策略组合中所包含的安全扫描策略,以及扫
20 描平台对上述目标小程序的安全扫描维度,可以基于实际的需求进行扩充,在本说明书中不再进行一一列举。

[109] 步骤 106,当所述目标小程序通过所述多维度的安全扫描时,将所述目标小程序发布至与搭载所述目标小程序的目标 APP 对应的服务端。

[110] 在本说明书中,当扫描平台通过调用上述安全扫描策略组合,对小程序执行多
25 个维度的安全扫描后,如果该目标小程序通过了上述多个维度的安全扫描,此时认为该目标小程序为非恶意小程序;在这种情况下,上述扫描平台可以进入针对该目标小程序的发布流程,进一步将该目标小程序发布至搭载该目标小程序的 APP 对应的服务端进行上线。

[111] 当然,如果该目标小程序未通过上述多个维度的安全扫描,表明该目标小程序

可能为恶意小程序；在这种情况下，上述扫描平台可以对该目标小程序的发布流程进行拦截，直接终止该目标小程序的发布流程，从而可以避免一些恶意小程序被发布上线，而影响用户的使用安全。

[112] 例如，请继续参见图 2，如果上述目标小程序分别通过了恶意代码扫描、安全漏洞扫描以及服务端接口漏洞扫描等维度的安全扫描后，此时可以确定该目标小程序为非恶意程序，可以对该目标小程序进行正常的发布；反之，如果上述目标小程序未通过恶意代码扫描、安全漏洞扫描以及服务端接口漏洞扫描等任一维度的安全扫描，此时都可以认为该目标小程序是潜在的恶意小程序，可以主动向开发人员反馈扫描结果，由开发人员对该目标小程序进行修复后，对该目标小程序重新进行多维度的安全扫描；或者，也可以直接对该小程序的发布流程进行拦截，终止该小程序的发布流程。

[113] 通过以上实施例可见，扫描平台在获取待通过调用安全扫描策略组合对待发布的目标小程序进行多维度的安全扫描，并在该目标小程序通过所述多维度的安全扫描时，再将该目标小程序发布至与搭载所述目标小程序的目标 APP 对应的服务端，可以有效避免将一些恶意小程序发布上线，而影响用户的使用安全。

[114] 与上述方法实施例相对应，本说明书还提供了一种小程序的安全扫描装置的实施例。

[115] 本说明书的小程序的安全扫描装置的实施例可以应用在电子设备上。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在电子设备的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，如图 3 所示，为本说明书的小程序的安全扫描装置所在电子设备的一种硬件结构图，除了图 3 所示的处理器、传感器、内存、网络接口、以及非易失性存储器之外，实施例中装置所在的电子设备通常根据该电子设备的实际功能，还可以包括其他硬件，对此不再赘述。

[116] 图 4 是本说明书一示例性实施例示出的一种小程序的安全扫描装置的框图。

[117] 请参考图 4，所述小程序的安全扫描装置 40 可以应用在前述图 3 所示的电子设备中，包括有：获取模块 401、扫描模块 402 以及发布模块 403。

[118] 获取模块 401，获取待发布的目标小程序；

[119] 扫描模块 402，调用安全扫描策略组合对所述目标小程序进行多维度的安全扫描；

- [120] 发布模块 403, 当所述目标小程序通过所述多维度的安全扫描时, 将所述目标小程序发布至与搭载所述目标小程序的目标 APP 对应的服务端。
- [121] 在本实施例中, 所述扫描模块 402 进一步执行以下扫描策略中的多个的组合:
- [122] 对所述目标小程序进行恶意代码扫描;
- 5 [123] 对所述目标小程序进行安全漏洞扫描;
- [124] 对与所述目标小程序对应的服务端接口进行安全漏洞扫描。
- [125] 在本实施例中, 所述扫描模块 402 进一步执行以下恶意代码扫描方式中的一个或者多个的组合:
- [126] 检测所述目标小程序是否携带攻击载荷;
- 10 [127] 检测所述目标小程序调用的所有函数是否存在为所述目标小程序定义的合法调用函数以外的恶意调用函数;
- [128] 检测所述目标小程序调用的媒体以及文本内容是否存在违规内容。
- [129] 在本实施例中, 所述扫描模块 402 进一步执行以下安全漏洞扫描方式中的一个或者多个的组合:
- 15 [130] 检测所述目标小程序是否存在敏感信息泄露漏洞;
- [131] 检测所述目标小程序是否存在 HTML 代码漏洞;
- [132] 检测所述目标小程序是否存在 JS 代码漏洞;
- [133] 检测所述目标小程序是否存在非法外部资源引用漏洞。
- [134] 在本实施例中, 所述扫描模块 402 进一步:
- 20 [135] 解析所述目标小程序的服务端接口;
- [136] 对解析出的所述服务端接口进行接口漏洞扫描。
- [137] 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, 其中所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在其中选择部分或者全部模块来实现本说明书方案的目的。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。

- [138] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是服务器、个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。
- [139] 与上述方法实施例相对应，本说明书还提供了一种电子设备的实施例。该电子设备包括：处理器以及用于存储机器可执行指令的存储器；其中，处理器和存储器通常通过内部总线相互连接。在其他可能的实现方式中，所述设备还可能包括外部接口，以能够与其他设备或者部件进行通信。
- 10 [140] 在本实施例中，通过读取并执行所述存储器存储的与小程序的安全扫描的控制逻辑对应的机器可执行指令，所述处理器被促使：
- [141] 获取待发布的目标小程序；
- [142] 调用安全扫描策略组合对所述目标小程序进行多维度的安全扫描；
- [143] 当所述目标小程序通过所述多维度的安全扫描时，将所述目标小程序发布至与
- 15 搭载所述目标小程序的目标 APP 对应的服务端。
- [144] 在本实施例中，通过读取并执行所述存储器存储的与小程序的安全扫描的控制逻辑对应的机器可执行指令，所述处理器还被促使执行以下动作中的一个或者多个的组合：
- [145] 对所述目标小程序进行恶意代码扫描；
- 20 [146] 对所述目标小程序进行安全漏洞扫描；
- [147] 对与所述目标小程序对应的服务端接口进行安全漏洞扫描。
- [148] 在本实施例中，通过读取并执行所述存储器存储的与小程序的安全扫描的控制逻辑对应的机器可执行指令，所述处理器还被促使执行以下动作中的一个或者多个的组合：
- 25 [149] 检测所述目标小程序是否携带攻击载荷；
- [150] 检测所述目标小程序调用的所有函数是否存在为所述目标小程序定义的合法调用函数以外的恶意调用函数；
- [151] 检测所述目标小程序调用的媒体以及文本内容是否存在违规内容。

- [152] 在本实施例中，通过读取并执行所述存储器存储的与小程序的安全扫描的控制逻辑对应的机器可执行指令，所述处理器还被促使执行以下动作中的一个或者多个的组合：
- [153] 检测所述目标小程序是否存在敏感信息泄露漏洞；
- 5 [154] 检测所述目标小程序是否存在 HTML 代码漏洞；
- [155] 检测所述目标小程序是否存在 JS 代码漏洞；
- [156] 检测所述目标小程序是否存在非法外部资源引用漏洞。
- [157] 在本实施例中，通过读取并执行所述存储器存储的与小程序的安全扫描的控制逻辑对应的机器可执行指令，所述处理器还被促使：
- 10 [158] 解析所述目标小程序的服务端接口；
- [159] 对解析出的所述服务端接口进行接口漏洞扫描。
- [160] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本说明书的其它实施方案。本说明书旨在涵盖本说明书的任何变型、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说明书的一般性原理并包括本说明书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，本说明书的真正范围和精神由下面的权利要求指出。
- [161] 应当理解的是，本说明书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。本说明书的范围仅由所附的权利要求来限制。
- 20 [162] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。
- 25 [163] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的范围之内。