(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 111639021 A
(43)申请公布日 2020.09.08

(21)申请号 202010406908.8

(22)申请日 2020.05.14

(71)申请人 深圳壹账通智能科技有限公司
地址 518000 广东省深圳市前海深港合作区前湾一路1号A栋201室

(72)发明人 张美苑

(74)专利代理机构 深圳中一联合知识产权代理有限公司 44414
代理人 张全文

(51)Int.Cl.
G06F 11/36(2006.01)
G06F 8/71(2018.01)
G06F 21/10(2013.01)

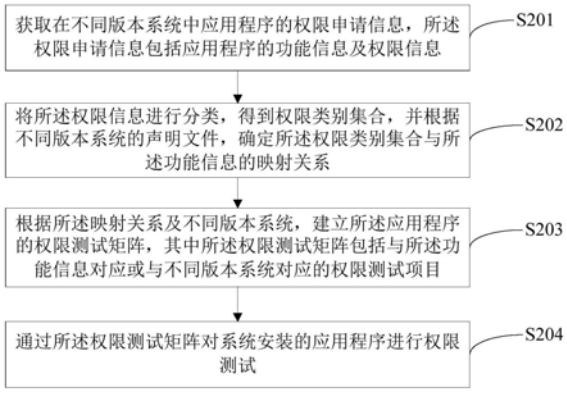
权利要求书2页 说明书13页 附图6页

(54)发明名称

应用程序的权限测试方法、装置及终端设备

(57)摘要

本申请适用于权限测试技术领域，提供了应用程序的权限测试方法、装置及终端设备，所述方法包括：获取在不同版本系统中应用程序的权限申请信息，权限申请信息包括应用程序的功能信息及权限信息；将权限信息进行分类，得到权限类别集合，并根据不同版本系统的声明文件，确定权限类别集合与功能信息的映射关系；根据映射关系及不同版本系统，建立应用程序的权限测试矩阵；通过权限测试矩阵对系统安装的应用程序进行权限测试。通过本申请，可以解决测试工具对应用程序测试不全面以及使得所安装的应用程序质量得不到保障的问题；为应用程序测试提供全面的测试用例；提升测试效率，全面改善了测试覆盖的完整性和准确性。另外，本申请还涉及区块链技术。



CN 111639021 A

1.一种应用程序的权限测试方法,其特征在于,包括:

获取在不同版本系统中应用程序的权限申请信息,所述权限申请信息包括应用程序的功能信息及权限信息;

将所述权限信息进行分类,得到权限类别集合,并根据不同版本系统的声明文件,确定所述权限类别集合与所述功能信息的映射关系;

根据所述映射关系及不同版本系统,建立所述应用程序的权限测试矩阵,其中所述权限测试矩阵包括与所述功能信息对应或与不同版本系统对应的权限测试项目;

通过所述权限测试矩阵对系统安装的应用程序进行权限测试。

2.如权利要求1所述的应用程序的权限测试方法,其特征在于,所述获取在预设类别系统中应用程序的权限申请信息,包括:

针对不同版本系统,获取与系统版本对应的软件开发工具包;

根据所述软件开发工具包,确定应用程序在不同版本系统中安装或运行时的所述权限申请信息。

3.如权利要求1所述的应用程序的权限测试方法,其特征在于,所述将所述权限信息进行分类,得到权限类别集合,并根据不同版本系统的声明文件,确定所述权限类别集合与所述功能信息的映射关系,包括:

根据不同版本系统的系统声明文件,确定第一业务权限列表与所述功能类别集合的第一映射关系;

根据不同版本系统的应用程序声明文件,确定第二业务权限列表与所述功能类别集合的第二映射关系。

4.如权利要求1所述的应用程序的权限测试方法,其特征在于,所述根据所述映射关系及不同版本系统,建立所述应用程序的权限测试矩阵,包括:

根据所述声明文件,将不同版本系统及所述功能信息设置为若干项测试参考指标;

根据所述功能信息与所述权限类别集合的映射关系,确定每一项所述测试参考指标与权限类别集合的对应关系;

根据所述对应关系,确定每一项所述测试参考指标对应的所述权限类别集合中的权限测试项目及权限测试项目的个数;

根据所述测试参考指标、所述权限测试项目以及所述权限测试项目的个数,建立所述权限测试矩阵。

5.如权利要求4所述的应用程序的权限测试方法,其特征在于,所述通过所述权限测试矩阵对系统安装的应用程序进行权限测试,包括:

获取与系统版本对应的软件开发工具包以及应用程序的安装包文件;

根据所述软件开发工具包,确定所述系统版本所属的所述测试参考指标;

根据所述安装包文件,确定所述应用程序对应的所述权限测试项目;

根据所述权限测试项目对系统安装的应用程序进行权限测试。

6.如权利要求1所述的应用程序的权限测试方法,其特征在于,所述方法还包括:

基于区块链技术对所述权限申请信息进行管理。

7.一种应用程序的权限测试装置,其特征在于,包括:

获取模块,用于获取在不同版本系统中应用程序的权限申请信息,所述权限申请信息

包括应用程序的功能信息及权限信息；

映射模块，用于将所述权限信息进行分类，得到权限类别集合，并根据不同版本系统的声明文件，确定所述权限类别集合与所述功能信息的映射关系；

矩阵模块，用于根据所述映射关系及不同版本系统，建立所述应用程序的权限测试矩阵，其中所述权限测试矩阵包括与所述功能信息对应或与不同版本系统对应的权限测试项目；

测试模块，用于通过所述权限测试矩阵对系统安装的应用程序进行权限测试。

8.如权利要求7所述的应用程序的权限测试装置，其特征在于，所述获取模块还用于针对不同版本系统，获取与系统版本对应的软件开发工具包；根据所述软件开发工具包，确定应用程序在不同版本系统中安装或运行时的所述权限申请信息。

9.一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如权利要求1至6任一项所述的方法。

10.一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至6任一项所述的方法。

应用程序的权限测试方法、装置及终端设备

技术领域

[0001] 本申请属于权限测试技术领域，尤其涉及应用程序的权限测试方法、装置及终端设备。

背景技术

[0002] 随着计算机技术的发展，智能移动终端成为人们生活中的必需品，安卓系统在智能移动终端的应用也越来越广泛。由于安卓系统的开源性，可以由移动终端厂商或应用开发者根据需要进行定制，从而使安卓系统碎片化严重，功能应用也多种多样；在安卓系统复杂多样的应用中，给人们带来巨大便利的同时，还混杂了大量的恶意应用，给用户的数据安全、隐私安全以及财产安全带来一定隐患。

[0003] 目前，应用程序的权限测试是安卓系统的一种安全检测机制。由于安卓系统碎片化严重，不同的厂商对于应用程序的授权页面指定特有的权限规则，使得关于安卓系统的应用程序权限类测试复杂多样化，导致现有的安卓系统终端应用程序的测试工具测试不全面，系统终端的应用程序质量得不到保障。

发明内容

[0004] 本申请实施例提供了应用程序的权限测试方法、装置及终端设备，可以解决安卓系统的应用程序权限类测试复杂多样化，导致现有的安卓系统终端应用程序的测试工具测试不全面，系统终端的应用程序质量得不到保障的问题。

[0005] 第一方面，本申请实施例提供了一种应用程序的权限测试方法，包括：

[0006] 获取在不同版本系统中应用程序的权限申请信息，所述权限申请信息包括应用程序的功能信息及权限信息；

[0007] 将所述权限信息进行分类，得到权限类别集合，并根据不同版本系统的声明文件，确定所述权限类别集合与所述功能信息的映射关系；

[0008] 根据所述映射关系及不同版本系统，建立所述应用程序的权限测试矩阵，其中所述权限测试矩阵包括与所述功能信息对应或与不同版本系统对应的权限测试项目；

[0009] 通过所述权限测试矩阵对系统安装的应用程序进行权限测试。

[0010] 在第一方面的一种可能的实现方式中，获取在预设类别系统中应用程序的权限申请信息，包括：

[0011] 针对不同版本系统，获取与系统版本对应的软件开发工具包；

[0012] 根据所述软件开发工具包，确定应用程序在不同版本系统中安装或运行时的所述权限申请信息。

[0013] 在一种可能的实现方式中，所述将所述权限信息进行分类，得到权限类别集合，并根据不同版本系统的声明文件，确定所述权限类别集合与所述功能信息的映射关系，包括：

[0014] 根据不同版本系统的系统声明文件，确定第一业务权限列表与所述功能类别集合的第一映射关系；

[0015] 根据不同版本系统的应用程序声明文件，确定第二业务权限列表与所述功能类别集合的第二映射关系。

[0016] 在一种可能的实现方式中，根据所述映射关系建立所述应用程序的权限测试矩阵，包括：

[0017] ，根据所述映射关系及不同版本系统，建立所述应用程序的权限测试矩阵，包括：

[0018] 根据系统的声明文件，将不同版本系统及所述功能信息设置为若干项测试参考指标；

[0019] 根据所述功能信息与所述权限类别集合的映射关系，确定每一项所述测试参考指标与权限类别集合的对应关系；

[0020] 根据所述对应关系，确定每一项所述测试参考指标对应的所述权限类别集合中的权限测试项目及权限测试项目的个数；

[0021] 根据所述测试参考指标、所述权限测试项目以及所述权限测试项目的个数，建立所述权限测试矩阵。

[0022] 在一种可能的实现方式中，通过所述权限测试矩阵对系统安装的应用程序进行权限测试，包括：

[0023] 获取与系统版本对应的软件开发工具包以及应用程序的安装包文件；

[0024] 根据所述软件开发工具包，确定所述系统版本所属的所述测试参考指标；

[0025] 根据所述安装包文件，确定所述应用程序对应的所述权限测试项目；

[0026] 根据所述权限测试项目对系统安装的应用程序进行权限测试。

[0027] 在一种可能的实现方式中，所述方法还包括：

[0028] 基于区块链技术对所述权限申请信息进行管理。

[0029] 第二方面，本申请实施例提供了一种应用程序的权限测试装置，包括：

[0030] 获取模块，用于获取在不同版本系统中应用程序的权限申请信息，所述权限申请信息包括应用程序的功能信息及权限信息；

[0031] 映射模块，用于将所述权限信息进行分类，得到权限类别集合，并根据不同版本系统的声明文件，确定所述权限类别集合与所述功能信息的映射关系；

[0032] 矩阵模块，用于根据所述映射关系及不同版本系统，建立所述应用程序的权限测试矩阵，其中所述权限测试矩阵包括与所述功能信息对应或与不同版本系统对应的权限测试项目；

[0033] 测试模块，用于通过所述权限测试矩阵对系统安装的应用程序进行权限测试。

[0034] 在一种可能的实现方式中，所述获取模块还用于针对不同版本系统，获取与系统版本对应的软件开发工具包；根据所述软件开发工具包，确定应用程序在不同版本系统中安装或运行时的所述权限申请信息。

[0035] 在一种可能的实现方式中，所述映射模块还用于根据不同版本系统的系统声明文件，确定第一业务权限列表与所述功能类别集合的第一映射关系；根据不同版本系统的应用程序声明文件，确定第二业务权限列表与所述功能类别集合的第二映射关系。

[0036] 第三方面，本申请实施例提供了一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现所述的方法。

[0037] 第四方面，本申请实施例提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行时实现所述的方法。

[0038] 第五方面，本申请实施例提供了一种计算机程序产品，当计算机程序产品在终端设备上运行时，使得终端设备执行上述第一方面中任一项所述的应用程序的权限测试方法。

[0039] 本申请实施例与现有技术相比存在的有益效果是：通过本实施例，获取在不同版本系统中应用程序的权限申请信息，所述权限申请信息包括应用程序的功能信息及权限信息；将所述权限信息进行分类，得到权限类别集合，并根据不同版本系统的声明文件，确定所述权限类别集合与所述功能信息的映射关系；根据所述映射关系及不同版本系统，建立所述应用程序的权限测试矩阵，其中所述权限测试矩阵包括与所述功能信息对应或与不同版本系统对应的权限测试项目；通过所述权限测试矩阵对系统安装的应用程序进行权限测试；解决了统终端应用程序的测试工具测试不全面以及系统终端所安装的应用程序质量得不到保障的问题；为应用程序测试，提供了全面的测试用例；同时，通过测试矩阵对应用程序进行针对性的测试，减少了权限类测试用例的冗余，提升了测试效率，全面提升了测试覆盖的完整性和准确性，具有较强的易用性与实用性。

[0040] 可以理解的是，上述第二方面至第五方面的有益效果可以参见上述第一方面中的相关描述，在此不再赘述。

附图说明

[0041] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0042] 图1是本申请一实施例提供的系统示意图；

[0043] 图2是本申请一实施例提供的应用程序的权限测试方法的流程示意图；

[0044] 图3是本申请一实施例提供的建立功能与权限的映射关系的示意图；

[0045] 图4是本申请一实施例提供的建立权限测试矩阵的示意图；

[0046] 图5是本申请一实施例提供的厂商权限验证点的设置示意图；

[0047] 图6是本申请实施例提供的应用程序的权限测试装置的结构示意图；

[0048] 图7是本申请实施例提供的终端设备的结构示意图。

具体实施方式

[0049] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本申请实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本申请。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本申请的描述。

[0050] 应当理解，当在本申请说明书和所附权利要求书中使用时，术语“包括”指示所描述特征、整体、步骤、操作、元素和/或组件的存在，但并不排除一个或多个其它特征、整体、步骤、操作、元素、组件和/或其集合的存在或添加。

[0051] 还应当理解，在本申请说明书和所附权利要求书中使用的术语“和/或”是指相关联列出的项中的一个或多个的任何组合以及所有可能组合，并且包括这些组合。

[0052] 如在本申请说明书和所附权利要求书中所使用的那样，术语“如果”可以依据上下文被解释为“当...时”或“一旦”或“响应于确定”或“响应于检测到”。类似地，短语“如果确定”或“如果检测到[所描述条件或事件]”可以依据上下文被解释为意指“一旦确定”或“响应于确定”或“一旦检测到[所描述条件或事件]”或“响应于检测到[所描述条件或事件]”。

[0053] 另外，在本申请说明书和所附权利要求书的描述中，术语“第一”、“第二”、“第三”等仅用于区分描述，而不能理解为指示或暗示相对重要性。

[0054] 在本申请说明书中描述的参考“一个实施例”或“一些实施例”等意味着在本申请的一个或多个实施例中包括结合该实施例描述的特定特征、结构或特点。由此，在本说明书中的不同之处出现的语句“在一个实施例中”、“在一些实施例中”、“在其他一些实施例中”、“在另外一些实施例中”等不是必然都参考相同的实施例，而是意味着“一个或多个但不是所有的实施例”，除非是以其他方式另外特别强调。术语“包括”、“包含”、“具有”及它们的变形都意味着“包括但不限于”，除非是以其他方式另外特别强调。

[0055] 本申请实施例提供的应用程序的权限测试方法可以应用于手机、平板电脑、笔记本电脑、超级移动个人计算机(ultra-mobile personal computer,UMPC)、上网本、个人数字助理(personal digital assistant,PDA)等终端设备上，本申请实施例对终端设备的具体类型不作任何限制。

[0056] 本申请实施例提供的应用程序的权限测试方法的执行主体包括但不限于服务端、终端等能够被配置为执行本申请实施例提供的该方法的电子设备中的至少一种。换言之，所述实例权限测试方法可以由安装在终端设备或服务端设备的软件或硬件来执行，所述软件可以是区块链平台。所述服务端包括但不限于：单台服务器、服务器集群、云端服务器或云端服务器集群等。

[0057] 区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链(Blockchain)，本质上是一个去中心化的数据库，是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一批次网络交易的信息，用于验证其信息的有效性(防伪)和生成下一个区块。区块链可以包括区块链底层平台、平台产品服务层以及应用服务层。

[0058] 区块链底层平台可以包括用户管理、基础服务、智能合约以及运营监控等处理模块。其中，用户管理模块负责所有区块链参与者的身份信息管理，包括维护公私钥生成(账户管理)、密钥管理以及用户真实身份和区块链地址对应关系维护(权限管理)等，并且在授权的情况下，监管和审计某些真实身份的交易情况，提供风险控制的规则配置(风控审计)；基础服务模块部署在所有区块链节点设备上，用来验证业务请求的有效性，并对有效请求完成共识后记录到存储上，对于一个新的业务请求，基础服务先对接口适配解析和鉴权处理(接口适配)，然后通过共识算法将业务信息加密(共识管理)，在加密之后完整一致的传输至共享账本上(网络通信)，并进行记录存储；智能合约模块负责合约的注册发行以及合约触发和合约执行，开发人员可以通过某种编程语言定义合约逻辑，发布到区块链上(合约注册)，根据合约条款的逻辑，调用密钥或者其它的事件触发执行，完成合约逻辑，同时还提供对合约升级注销的功能；运营监控模块主要负责产品发布过程中的部署、配置的修改、合

约设置、云适配以及产品运行中的实时状态的可视化输出，例如：告警、监控网络情况、监控节点设备健康状态等。

[0059] 参见图1，是本申请一实施例提供的系统示意图，本申请提供的应用程序权限测试方法可以应用于，测试终端对移动设备中安装的应用程序的权限设置进行测试；如图所示，测试终端20依据应用程序的权限测试矩阵，并根据移动设备10的版本及应用程序的安装包确定权限测试矩阵中所需的测试用例，对应用程序进行全面的权限测试，保证了应用程序的测试质量，提高了测试效率。另外，移动设备10可以是安卓系统的手机或平板电脑等，测试终端20可以是电脑或具有数据处理功能的终端设备等。移动设备10与测试终端可以通过有线或无线的方式进行连接和通信，有线方式例如，通过USB数据线等；无线通信方式例如，通过移动网络(2G/3G/4G/5G等)或互联网、WiFi等。

[0060] 图2示出了本申请提供的应用程序的权限测试方法的示意性流程图。

[0061] 步骤S201，获取在不同版本系统中应用程序的权限申请信息，所述权限申请信息包括应用程序的功能信息及权限信息。

[0062] 在一种可能的实现方式中，安卓系统是权限分离的操作系统，将不同的应用程序之间以及应用程序与系统之间分隔开；任何一个应用程序在使用安卓的权限资源之前，都要先向安卓系统提出申请，等待安卓系统批准后应用程序可使用相应的资源。

[0063] 其中，以安卓操作系统为例，由于安卓系统版本是向前兼容，系统的软件开发工具包SDK的新版本(也可以称作目标版本)可以兼容旧版本，即目标SDK版本决定应用程序与系统的兼容性。针对不同版本的安卓系统，对应不同的应用程序权限管理机制，即不同的系统版本，应用程序向系统获取权限的方式不同，应用程序的权限申请信息可以根据系统版本或系统的目标SDK版本确定。

[0064] 可选的，获取在预设类别系统中应用程序的权限申请信息，包括：

[0065] A1、针对不同版本系统，获取与系统版本对应的软件开发工具包；

[0066] A2、根据所述软件开发工具包，确定应用程序在不同版本系统中安装或运行时的所述权限申请信息。

[0067] 具体地，在系统的软件开发工具包SDK中，记录当前版本系统的权限申请方式，针对不同版本的系统，所对应的权限申请方式也不同。在系统版本大于等于6.0且目标SDK版本>＝23时，应用程序在安装成功后，获取应用程序向系统申请权限的权限申请信息。在应用程序安装过程，不会向系统申请获取权限；而是直接安装成功后，运行时，向系统动态申请权限。

[0068] 在应用程序安装成功后，启动并运行应用程序，针对某一权限或某一类权限，例如相机权限，判断当前应用有没有该权限，若没有该权限，则发出对该权限的申请；并判断是否需要解释对应权限的用途(或者判断是否需要展示请求权限的提示)；若需要，则弹出解释权限询问的对话框，例如‘要允许某某应用程序拍摄照片和录制视频吗’，以及对话框包括显示的‘允许’和‘拒绝’操作控件。

[0069] 另外，对于解释权限及询问的对话框，可以针对用户的授权信号或移动终端厂家的不同，获取对应的响应结果，响应结果可以代表某一类权限针对某一项功能的权限申请原理，例如：接收到用户选择的‘允许’消息后，执行请求对应权限的动作，并回调相应的权限；在接收到用户选择的‘拒绝’且没有选择‘不再提示’的选项时，在应用程序下次运行时，

继续对该权限的使用执行弹窗询问;在接收到用户选择‘拒绝’且选择‘不再提示’,则下次应用程序运行时,不再动态申请权限,只能通过设置界面接收用户的权限设置指令;另外一种是针对一些特定的厂商,在对权限访问时,返回的错误的响应信息,表示该应用程序不可以申请该类权限。

[0070] 示例性的,针对上述系统版本,应用程序安装成功后,运行过程中,判断是否有对应的权限,若有对应的权限,则直接调用相应的权限接口。在应用程序运行过程中,在需要申请应用程序不具有的权限,且不需要解释对应权限用途时,则直接请求对应的权限,并调用相应的权限。

[0071] 另外,在系统版本大于等于6.0且目标SDK版本小于23,或者系统版本小于6.0且目标SDK版本小于23,或者系统版本小于6.0且目标SDK版本大于等于23,获取应用程序在安装过程中向系统申请权限的方式。

[0072] 具体的,在应用程序安装过程中获取权限,通过权限申请接口,读取文件中应用程序正常运行所需要申请的权限,生成权限列表并显示对话框,接收用户输入的选择权限,根据用户的选择指令,做出安装成功或退出安装的响应。

[0073] 针对以上系统版本,统计应用程序申请权限的各种方式,作为应用程序在相应版本的系统中的权限申请信息。通过上述针对不同版本系统以及不同厂商定制的系统版本,获取应用程序在安装过程或运行过程向系统申请权限的方式或原理,作为预设类别系统中应用程序的权限申请信息,为下一步通过静态扫描获取权限与功能对应关系做准备。

[0074] 步骤S202,将所述权限信息进行分类,得到权限类别集合,并根据不同版本系统的声明文件,确定所述权限类别集合与所述功能信息的映射关系。

[0075] 在一种可能的实现方式中,不同版本系统的声明文件中记录系统不同的业务权限对应的申请方式;根据权限信息可以将权限分为非主要业务权限和业务权限;例如系统的蓝牙、联网模块及振动等的权限则可以分为非主要业务权限,也可以作为普通权限,将SD卡数据的访问权限则分为业务权限或敏感权限。不同版本或不同厂商定制的操作系统,在安装应用程序过程中的,权限申请方式不同,对应的权限申请信息不同,在对应版本的操作系统中声明的权限内容也不同,不同的权限对应不同的功能实现或应用场景。

[0076] 在本实施例中,通过获取不同版本或厂商的操作系统中的设定的权限申请方式,可以针对不同申请方式分别确定应用程序功能和系统权限的对应关系,从而可以设定不同的测试用例范围;例如系统版本在6.0以下的,在应用程序安装过程中,应用程序所声明的权限可以由操作系统直接授权,则不用再考虑其它需要动态申请的权限,进而不用设置其他需要动态申请的权限与功能的对应关系的测试用例;针对6.0版本以上的,则需要根据权限申请方式,分别设定不同的权限与功能的对应关系,从而建立相应的测试用例。

[0077] 具体的,根据应用程序的权限申请信息,通过静态扫描,在不运行代码的情况下,采用词法分析、语法分析等分析方式对程序文件进行功能代码的扫描,生成程序的反汇编代码,根据反汇编代码分析检测应用程序的功能;应用程序的功能可以从应用程序安装包APK文件中获取相应的功能描述。

[0078] 需要说明的是,不同的权限申请信息对应的权限申请过程中,还可以获知相应权限所对应的功能,可以根据在权限申请过程的权限申请信息,建立权限类别集合与功能信息的对应关系。

[0079] 可选的，所述将所述权限信息进行分类，得到权限类别集合，并根据不同版本系统的声明文件，确定所述权限类别集合与所述功能信息的映射关系，包括：

[0080] B1、根据不同版本系统的系统声明文件，确定第一业务权限列表与所述功能类别集合的第一映射关系；

[0081] B2、根据不同版本系统的应用程序声明文件，确定第二业务权限列表与所述功能类别集合的第二映射关系。

[0082] 具体的，对应用程序的功能进行分类，分析应用程序的安装包文件，获取所在系统的权限配置文件，得到非主要业务权限列表的权限内容，即第一业务权限列表。非主要权限业务列表的权限内容，通常为普通的权限，一般由应用程序的开发者在配置列表中声明，在应用程序安装过程中直接被操作系统授予的权限，不会涉及个人隐私的权限，例如网络INTERNET、蓝牙、震动等权限。

[0083] 示例性的，通过开源静态分析工具androguard的配置文件静态读取模块androaxml.py获取系统的配置文件androidmanifest.xml，得到非主要业务权限列表android.permission的权限内容。对于低于6.0版本的，应用程序在安装过程，配置表中的权限列表中的权限可以由操作系统直接授予，从而可以直读取配置表中的权限列表。

[0084] 在一种可能的实现方式中，分析应用程序的安装包文件，通过应用程序管理语句，读取应用程序的相关信息；相关信息可以包括应用程序的名称以及需要申请的权限。根据相关信息获得对应应用程序的业务权限列表，即第二业务权限列表；其中还包括敏感权限，主要针对需要向用户申请授权的权限，例如，相机CAMERA、联系人CONTACTS、存储设备STORAGE等权限。对于高于6.0版本的，针对不同的操作系统，需要通过动态申请的方式获取相应的权限列表。

[0085] 具体的，根据获取的非业务权限列表以及业务权限列表，针对不同的应用场景，对相应的权限进行基于代码的扫描、查询功能代码或功能开发等方式进行功能实现的测试，确定在不同应用场景下的应用程序的功能，进一步确定功能与权限列表的对应关系。另外，可以根据应用程序安装包调用接口API函数序列，判断该接口函数是否符合某个权限类型，若符合则将该接口函数放入权限类别对应的集合中，从而找出关键的触发权限的接口；其中功能和权限的对应关系存在一对多或多对一或者多对多的对应关系。

[0086] 示例性的，如图3所示的，本申请一实施例提供的建立功能与权限的映射关系的示意图。根据权限申请信息，通过静态扫描，对应用程序的功能进行识别并分类，获取功能类别集合；其中功能类别集合也可以为不同应用场景对应的功能集合，例如调用麦克风相关场景的语音识别功能、调用相机相册相关场景的人脸识别及图文识别功能等。根据权限申请信息，针对不同版本的系统，通过确定应用程序的业务权限列表，分别对应系统的照相权限、麦克风权限、存储权限以及网络相关权限，通过开源静态分析工具androguard的配置文件的配置表中确定直接获取权限列表或需要向系统动态申请的权限列表，对权限进行分类，得到权限类别集合，权限类别集合可以包括业务权限列表对应的集合和非业务类权限列表对应的集合，还可以包括敏感类权限集合。

[0087] 如图3所示，结合应用程序安装包文件，确定功能类别集合与权限类别集合的对应关系，例如图中的业务权限列表中的照相权限、麦克风权限、存储权限及网络相关权限分别对应的功能；照相权限对应的光纤检测、视频录制及人脸识别功能；麦克风权限对应噪声检

测、从文本到语音的TTS播报及语音识别的功能；存储权限对应的视频录制、人脸识别及语音识别权限；网络相关权限对应的网络检测和视频上传功能等。

[0088] 另外，在建立映射关系时，还可以考虑屏蔽某个权限，针对另一个权限所对应的功能，建立相关的测试案例，例如，屏蔽掉存储权限，对照相机权限对应的光纤检测、视频录制、人脸识别功能进行测试，增加对应用程序功能多方位的测试用例，以确保应用程序的功能和质量。

[0089] 需要说明的是，本实施例建立映射关系还可以针对不同机型的有权限列表和无权限列表进行测试，使得测试用例覆盖更全面。

[0090] 在一种可能的实现方式中，在进行功能与权限列表对应关系测试过程中，可以对权限进行分类，获取基于不同系统版本或厂商的移动终端系统的权限类别，通用的权限类别可以包括：照相机权限、存储权限、通讯录权限、定位权限、麦克风权限、短信权限、电话权限、传感器权限、日历权限等；也可对应用程序的功能进行分类，包括地图类、系统工具类、影音播放类、聊天社交类、图书阅读类、购物类、办公类、摄影类、医疗健康类、体育运动类、理财类、新闻类等。针对每个权限，测试相应的应用程序的功能类别属性；通过代码的扫描、查询功能代码或功能开发等测试方式，获取应用程序的功能与权限的第一映射关系。例如：照相机权限可以对应光线检测、视频录制、人脸识别的功能类别或业务场景，麦克风权限对应噪声检测、TTS播报、语音识别的功能类别或业务场景，存储权限对应视频录制、人脸识别、语音识别的功能类别或业务场景。

[0091] 针对某第一权限，在屏蔽另一外某一项第二权限时，对第一权限对应的业务场景或功能类别进行测试，判断应用程序在第一权限是否可以正常启用对应的功能类别，经过分析测试获取相应的第二映射关系；例如相机权限在屏蔽存储权限的情况下，对光线检测侧、视频录制、人脸识别的功能进行对应的测试；防止应用程序通过其他途径获取相应功能的权限，增加权限与功能的对应关系的测试用例。根据第一映射关系、第二映射关系以及不同机型的权限列表，进行综合分析评估，获取所有机型系统版本的权限以及功能的对应关系。

[0092] 针对移动终端不同的机型，获取对应的有权限列表和无权限列表，可以通过系统内的权限配置列表进行读取；不同的机型包括不同的系统版本或不同的厂商对应的有权限列表和无权限列表。

[0093] 另外，在获取非主要业务权限列表的内容后，对该应用程序的功能进行分类，针对非主要业务权限列表中的每一项权限针对功能分类进行代码扫描测试，获取应用程序的风险权限的测试列表，从而可以确定风险较高的应用程序。

[0094] 步骤S203，根据所述映射关系及不同版本系统，建立所述应用程序的权限测试矩阵，其中所述权限测试矩阵包括与所述功能信息对应或与不同版本系统对应的权限测试项目。

[0095] 在一种可能的实现方式中，根据所建立的功能与权限的映射关系，针对不同的厂商的定制特点以及不同操作方式生成与权限类别对应的权限测试矩阵；提供全面的、适用性较强的权限测试用例。

[0096] 具体的，从验证场景出发，提取出公共通用场景，再从权限类型、系统特征、厂商、操作方式、屏蔽方式特征维度进行组合，生成通用的权限测试设计矩阵。

[0097] 可选的，根据所述映射关系及不同版本系统，建立所述应用程序的权限测试矩阵，包括：

[0098] C1、根据所述声明文件，将不同版本系统及所述功能信息设置为若干项测试参考指标；

[0099] C2、根据所述功能信息与所述权限类别集合的映射关系，确定每一项所述测试参考指标与权限类别集合的对应关系；

[0100] C3、根据所述对应关系，确定每一项所述测试参考指标对应的所述权限类别集合中的权限测试项目及权限测试项目的个数；

[0101] C4、根据所述测试参考指标、所述权限测试项目以及所述权限测试项目的个数，建立所述权限测试矩阵。

[0102] 在一种可能的实现方式中，如图4所示的，本申请一实施例提供的建立权限测试矩阵的示意图。设置若干项测试参考指标，所述测试参考指标为应用程序或操作系统所属的类别，如图4所示，测试参考指标可以包括权限类型、系统的特征、厂商定制、操作方式及屏幕测试管理权限(root-xposed管理权限)等；具体可以根据不同版本系统声明文件，将系统对应的所有版本及应用程序的权限申请信息中的功能信息或应用场景设置为测试参考指标。所述的权限测试项目可以依据应用场景进行分类，如图4所示的，可以包括相机或相册相关场景、读取通讯录相关场景、调用定位相关场景、调用麦克风相关场景、调用短信相关场景、调用日历相关场景以及调用传感器相关场景等对应的测试用例。并根据上述所建立的功能与权限的映射关系，确定测试项目的个数，从而建立包括所述测试参考指标、所述权限测试项目以及所述权限测试项目的个数的所述权限测试矩阵，如图所示，有的对应1次，有的对应10次。

[0103] 具体的，验证场景包括人脸识别、地图定位等具体的某一业务场景，例如针对相机权限进行的光线检测、视频录制以及人脸识别的测试，针对存储权限进行的视频录制、人脸识别、语音识别的测试。

[0104] 提取出的公共通用场景包括调用相机或相册相关场景、读取通讯录相关场景、调用定位相关场景、调用麦克风相关场景、调用短信相关场景、调用日历相关场景以及调用传感器相关场景等，对应不同的权限，所进行的相同的业务场景的测试，例如针对相机权限和存储权限，均对视频录制以及人脸识别的业务场景进行了测试。

[0105] 权限类型可以包括：照相机权限、存储权限、通讯录权限、定位权限、麦克风权限、短信权限、电话权限、传感器权限、日历权限；还可以针对不同的机型分为业务权限和非业务权限，或者必要权限和敏感权限。

[0106] 系统的特征为针对不同版本的系统，其不同的权限申请方式不同，对应提取出的公共通用场景通过建立的权限功能对应关系设置相应的测试用例。

[0107] 根据不同厂商的定制特征，具有不同的权限管理机制或对系统的权限申请方式，结合功能与权限对应关系，建立对应不同厂商的测试用例，并设定相应的测试用的个数。如图5所示的，根据不同厂商的定制特征设置厂商权限验证点，验证点根据不同系统版本设置对应的验证点，将权限的申请方式设置为允许、拒绝、询问或默认权限等方式。

[0108] 操作方式是指在应用程序启动运行过程中接收到的选择询问授权的方式，根据不同的方式对调用相关场景时的授权，结合功能与权限的对应关系，设置与公共通用场景对

应的测试用例。

[0109] 屏蔽方式包括针对某一项权限，在屏蔽另外一项权限或开启另一项权限时，结合功能与权限的对应关系，设定其进行业务场景的测试的测试用例。

[0110] 另外，根据以上特征维度，设定对应测试的用例的验证点数，也就是针对这一特征维度所需要的测试用例的个数，根据不同的特征维度设置相应的测试案例数，以全面覆盖对针对某一功能的权限测试，从而确定通用的权限测试矩阵。

[0111] 步骤S204，通过所述权限测试矩阵对系统安装的应用程序进行权限测试。

[0112] 在一种可能的实现方式中，所生成的权限测试矩阵，在应用程序安装的过程中或者在应用程序安装后启动某项功能时，对应用程序的功能对应请求的权限进行权限检测，通过建立的正交矩阵测试用例全面检测应用程序的权限，保障应用程序的权限测试质量；不仅减少测试案例的冗余，大大提升测试效率；而且全面提高测试覆盖的完整性和准确性。

[0113] 可选的，通过所述权限测试矩阵对系统安装的应用程序进行权限测试，包括：

[0114] D1、获取与系统版本对应的软件开发工具包以及应用程序的安装包文件；

[0115] D2、根据所述软件开发工具包，确定所述系统版本所属的所述测试参考指标；

[0116] D3、根据所述安装包文件，确定所述应用程序对应的所述权限测试项目；

[0117] D4、根据所述权限测试项目对系统安装的应用程序进行权限测试。

[0118] 在一个实施例中，本申请所提供的方法还包括以下步骤：基于区块链技术对权限申请信息进行管理。通过区块链节点对权限申请信息进行存储、读取，增加权限申请信息存储过程中的安全性和可靠性。同理，测试过程中的权限类别集合、权限类别集合与功能信息的映射关系以及测试结果等等亦可以存储至区块链节点中，从而增加整个方案的安全性和易操作性。

[0119] 通过本实施例，获取在不同版本系统中应用程序的权限申请信息，所述权限申请信息包括应用程序的功能信息及权限信息；将所述权限信息进行分类，得到权限类别集合，并根据不同版本系统的声明文件，确定所述权限类别集合与所述功能信息的映射关系；根据所述映射关系及不同版本系统，建立所述应用程序的权限测试矩阵，其中所述权限测试矩阵包括与所述功能信息对应或与不同版本系统对应的权限测试项目；通过所述权限测试矩阵对系统安装的应用程序进行权限测试；解决了统终端应用程序的测试工具测试不全面以及系统终端所安装的应用程序质量得不到保障的问题；为应用程序测试，提供了全面的测试用例；同时，通过测试矩阵对应用程序进行针对性的测试，减少了权限类测试用例的冗余，提升了测试效率，全面提升了测试覆盖的完整性和准确性。

[0120] 应理解，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

[0121] 对应于上文实施例所述的应用程序的权限测试方法，图5示出了本申请实施例提供的应用程序的权限测试装置的结构框图，为了便于说明，仅示出了与本申请实施例相关的部分。

[0122] 参照图6，该装置包括：获取模块61，映射模块62，矩阵模块63，测试模块64。

[0123] 其中，获取模块61，用于获取在不同版本系统中应用程序的权限申请信息，所述权限申请信息包括应用程序的功能信息及权限信息；

[0124] 映射模块62，用于将所述权限信息进行分类，得到权限类别集合，并根据不同版本系统的声明文件，确定所述权限类别集合与所述功能信息的映射关系；

[0125] 矩阵模块63，用于根据所述映射关系及不同版本系统，建立所述应用程序的权限测试矩阵，其中所述权限测试矩阵包括与所述功能信息对应或与不同版本系统对应的权限测试项目；

[0126] 测试模块64，用于通过所述权限测试矩阵对系统安装的应用程序进行权限测试。

[0127] 在一种可能的实现方式中所述获取模块还用于针对不同版本系统，获取与系统版本对应的软件开发工具包；根据所述软件开发工具包，确定应用程序在不同版本系统中安装或运行时的所述权限申请信息。

[0128] 在一种可能的实现方式中，所述映射模块还用于根据不同版本系统的系统声明文件，确定第一业务权限列表与所述功能类别集合的第一映射关系；根据不同版本系统的应用程序声明文件，确定第二业务权限列表与所述功能类别集合的第二映射关系。

[0129] 在一种可能的实现方式中，所述矩阵模块还用于，根据所述声明文件，将不同版本系统及所述功能信息设置为若干项测试参考指标；根据所述功能信息与所述权限类别集合的映射关系，确定每一项所述测试参考指标与权限类别集合的对应关系；根据所述对应关系，确定每一项所述测试参考指标对应的所述权限类别集合中的权限测试项目及权限测试项目的个数；根据所述测试参考指标、所述权限测试项目以及所述权限测试项目的个数，建立所述权限测试矩阵。

[0130] 在一种可能的实现方式中，所述测试模块还用于，获取与系统版本对应的软件开发工具包以及应用程序的安装包文件；根据所述软件开发工具包，确定所述系统版本所属的所述测试参考指标；根据所述安装包文件，确定所述应用程序对应的所述权限测试项目；根据所述权限测试项目对系统安装的应用程序进行权限测试。

[0131] 通过本实施例，获取在不同版本系统中应用程序的权限申请信息，所述权限申请信息包括应用程序的功能信息及权限信息；将所述权限信息进行分类，得到权限类别集合，并根据不同版本系统的声明文件，确定所述权限类别集合与所述功能信息的映射关系；根据所述映射关系及不同版本系统，建立所述应用程序的权限测试矩阵，其中所述权限测试矩阵包括与所述功能信息对应或与不同版本系统对应的权限测试项目；通过所述权限测试矩阵对系统安装的应用程序进行权限测试；解决了统终端应用程序的测试工具测试不全面以及系统终端所安装的应用程序质量得不到保障的问题；为应用程序测试，提供了全面的测试用例；同时，通过测试矩阵对应用程序进行针对性的测试，减少了权限类测试用例的冗余，提升了测试效率，全面提升了测试覆盖的完整性和准确性。

[0132] 需要说明的是，上述装置/单元之间的信息交互、执行过程等内容，由于与本申请方法实施例基于同一构思，其具体功能及带来的技术效果，具体可参见方法实施例部分，此处不再赘述。

[0133] 所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元、模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元、模块完成，即将所述装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中，上述集成的

单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。另外，各功能单元、模块的具体名称也只是为了便于相互区分，并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0134] 图7为本申请一实施例提供的测试终端的结构示意图。如图7所示，该实施例的测试终端7包括：至少一个处理器70(图7中仅示出一个)处理器、存储器71以及存储在所述存储器71中并可在所述至少一个处理器70上运行的计算机程序72，所述处理器70执行所述计算机程序72时实现上述任意各个应用程序的权限测试方法实施例中的步骤。

[0135] 所述测试终端7可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。该测试终端可包括，但不仅限于，处理器70、存储器71。本领域技术人员可以理解，图7仅仅是测试终端7的举例，并不构成对测试终端7的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如还可以包括输入输出设备、网络接入设备等。

[0136] 所称处理器70可以是中央处理单元(Central Processing Unit,CPU)，该处理器70还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0137] 所述存储器71在一些实施例中可以是所述测试终端7的内部存储单元，例如测试终端7的硬盘或内存。所述存储器71在另一些实施例中也可以是所述测试终端7的外部存储设备，例如所述测试终端7上配备的插接式硬盘，智能存储卡(Smart Media Card,SMC)，安全数字(Secure Digital,SD)卡，闪存卡(Flash Card)等。进一步地，所述存储器71还可以既包括所述测试终端7的内部存储单元也包括外部存储设备。所述存储器71用于存储操作系统、应用程序、引导装载程序(BootLoader)、数据以及其他程序等，例如所述计算机程序的程序代码等。所述存储器71还可以用于暂时地存储已经输出或者将要输出的数据。

[0138] 本申请实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行时实现可实现上述各个方法实施例中的步骤。

[0139] 本申请实施例提供了一种计算机程序产品，当计算机程序产品在移动终端上运行时，使得移动终端执行时实现可实现上述各个方法实施例中的步骤。

[0140] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请实现上述实施例方法中的全部或部分流程，可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一计算机可读存储介质中，该计算机程序在被处理器执行时，可实现上述各个方法实施例的步骤。其中，所述计算机程序包括计算机程序代码，所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质至少可以包括：能够将计算机程序代码携带到拍照装置/终端设备的任何实体或装置、记录介质、计算机存储器、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、电载波信号、电信信号以及软件分发介质。例如U盘、移动硬盘、磁碟或者光盘等。在某些司法管辖区，根据立法和专利实践，计算机可读介质不可以是电载波信号和

电信信号。

[0141] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述或记载的部分，可以参见其它实施例的相关描述。

[0142] 本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

[0143] 在本申请所提供的实施例中，应该理解到，所揭露的装置/网络设备和方法，可以通过其它的方式实现。例如，以上所描述的装置/网络设备实施例仅仅是示意性的，例如，所述模块或单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通讯连接可以是通过一些接口，装置或单元的间接耦合或通讯连接，可以是电性，机械或其它的形式。

[0144] 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选择其中的部分或者全部单元来实现本实施例方案的目的。

[0145] 以上所述实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围，均应包含在本申请的保护范围之内。

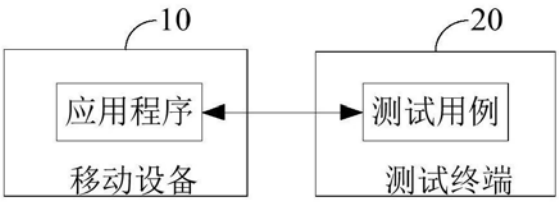

10
20
应用程序
测试用例
移动设备
测试终端

图1

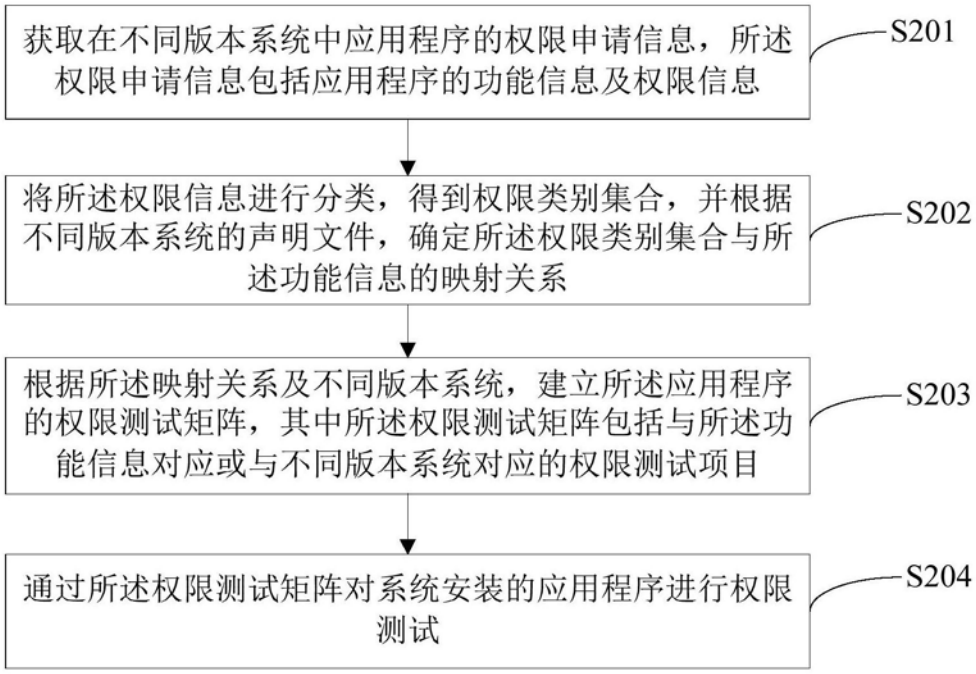

获取在不同版本系统中应用程序的权限申请信息，所述权限申请信息包括应用程序的功能信息及权限信息
S201
将所述权限信息进行分类，得到权限类别集合，并根据不同版本系统的声明文件，确定所述权限类别集合与所述功能信息的映射关系
S202
根据所述映射关系及不同版本系统，建立所述应用程序的权限测试矩阵，其中所述权限测试矩阵包括与所述功能信息对应或与不同版本系统对应的权限测试项目
S203
通过所述权限测试矩阵对系统安装的应用程序进行权限测试
S204

图2

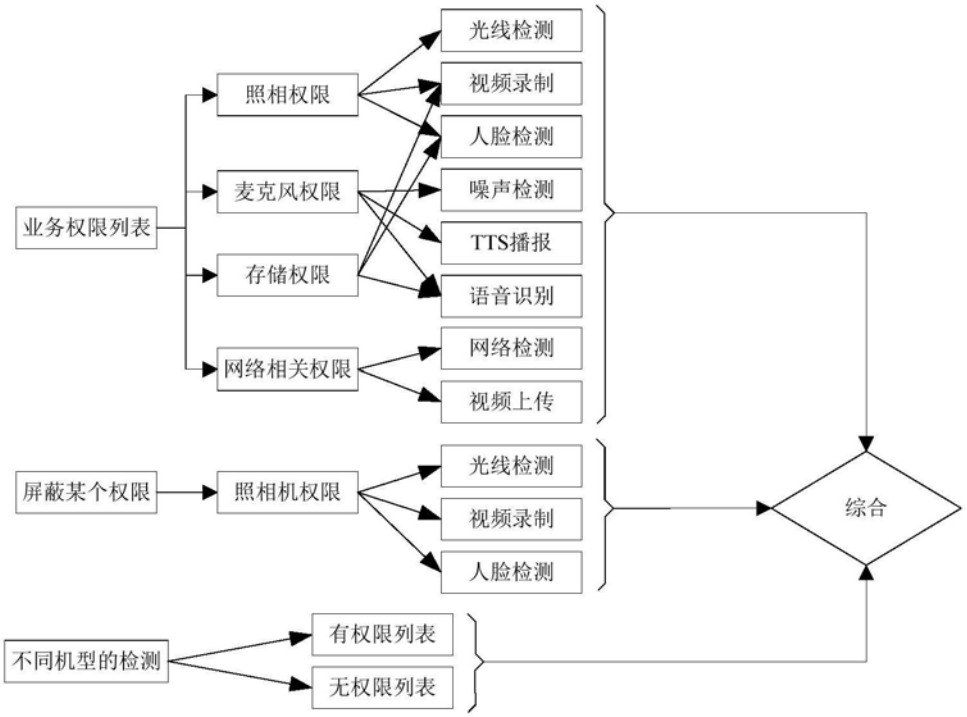


图3

安卓权限测试设计矩阵									
验证点/验证场景	特征细节	调用相机相册相关场景（OCR、人脸识别等）	读写通讯录相关场景（充话费流量等）	调用定位相关场景（地图定位等）	调用麦克风相关场景（语音识别等）	调用电话相关场景（客服等）	调用短信相关场景（验证码读取等）	调用日历相关场景	调用传感器相关场景（运动计步、摇一摇等）
根据权限	照相机	1	0	0	0	0	0	0	0
	存储	1	1	1	1	0	0	0	0
	通讯录	0	1	0	0	0	1	0	0
	定位	0	0	1	0	0	0	0	0
	麦克风	1	0	0	1	0	0	0	0
	短信	0	0	0	0	0	1	0	0
	电话	0	0	0	0	1	0	0	0
	传感器	0	0	0	0	0	0	0	1
	日历	0	0	0	0	0	0	0	0
根据系统特征不同	安卓 6.0 以下（安装赋予）	1	1	1	1	1	1	1	1
	安卓 6.0（动态申请权限）	1	1	1	1	1	1	1	1
	安卓 7.x（私有目录被限制访问\StrictMode API政策）	1	0	0	0	0	0	0	0

	安卓 8.x（纠正将属于同一权限组并且在清单中注册的其他权限也一起授予应用的 bug，系统只会授予应用明确请求的权限）	1	1	1	1	1	1	1	0
	安卓 9.0（支持 WiFi 定位）	0	0	1	0	0	0	0	0
根据厂商定制	小米（miui 系统：双重权限系统，miui 拥有最高权限，安卓用于第二权限）	10	10	10	10	10	10	10	10
	Vivo（funtouch os:定制的权限管理）	10	10	10	10	10	10	10	10
	魅族（Flyme：强大的权限管理）	10	10	10	10	10	10	10	10
	OPPO（color os:定制的权限管理）	10	10	10	10	10	10	10	10
	华为（emui:定制的权限管理）	10	10	10	10	10	10	10	10
	三星（去设置页面关闭此 APP 的权限，APP 会被重置）	10	10	10	10	10	10	10	10
根据不同操作方式	启动运行时允许授权-调用相关场景-可使用	1	1	1	1	1	1	1	1
	启动运行时拒绝授权（勾选不再弹窗）-调用相关场景-提示不可使用	1	1	1	1	1	1	1	1
	启动运行时拒绝授权（不勾选弹窗）-调用相关场景时选择允许-可使用	1	1	1	1	1	1	1	1
	启动运行时拒绝授权（不勾选弹窗）-调用相关场景时弹窗询问选择拒绝-不可使用	1	1	1	1	1	1	1	1
	启动运行时选择询问授权-调用相关场景-继续弹窗询问	1	1	1	1	1	1	1	1
	已允许授权-后台	1	1	1	1	1	1	1	1

	设置询问-调用相关场景-不可使用								
	已允许授权-后台设置询问-调用相关场景-弹窗询问	1	1	1	1	1	1	1	1
	已拒绝授权（勾选不再弹窗）-后台设置询问-调用相关场景弹窗询问	1	1	1	1	1	1	1	1
	已拒绝授权（勾选不再弹窗）-后台设置允许-调用相关场景-可使用	1	1	1	1	1	1	1	1
	已拒绝授权（不勾选不再弹窗）-后台设置允许-调用相关场景-可使用	1	1	1	1	1	1	1	1
需root-exposed管理权限	屏蔽相关权限	1	1	1	1	1	1	1	1
	开启相关权限	1	1	1	1	1	1	1	1

图4

备注	验证点
厂商权限验证点：	1.6.0 以下：设置成允许，即允许权限
	2.6.0 以下：设置成拒绝，然后再设置为允许
	3.6.0 以下：设置成询问模式：然后弹出对话框，选择拒绝
	4.6.0 以下：设置成询问模式：然后弹出对话框，选择允许
	5.6.0 以下：不设置申请权限，默认有权限
	6.6.0+：设置成允许，即允许权限
	7..6.0+：设置成拒绝，然后再设置为允许
	8..6.0+：设置成询问模式：然后弹出对话框，选择拒绝
	9..6.0+：设置成询问模式：然后弹出对话框，选择允许
	10..6.0+：不设置申请权限，默认有权限

图5

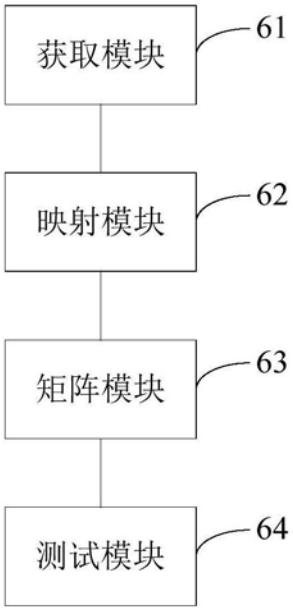


图6

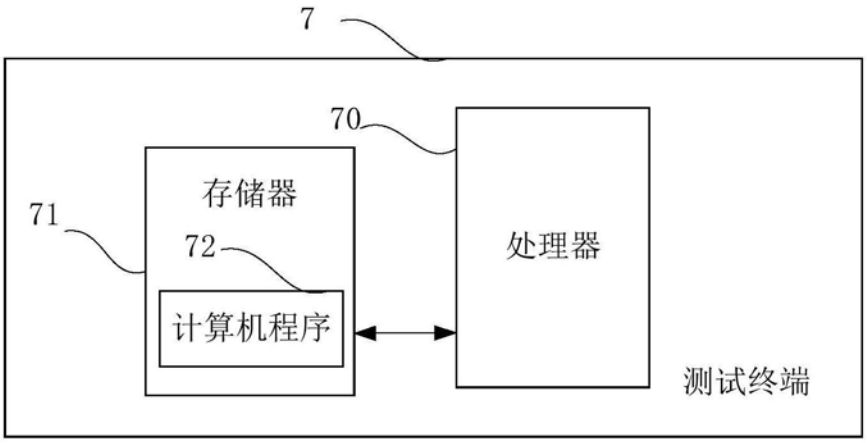


图7