



(12) 发明专利

(10) 授权公告号 CN 110336777 B

(45) 授权公告日 2020.10.16

(21) 申请号 201910363436.X

G06K 9/62 (2006.01)

(22) 申请日 2019.04.30

(56) 对比文件

(65) 同一申请的已公布的文献号

CN 106713332 A, 2017.05.24

申请公布号 CN 110336777 A

CN 103473346 A, 2013.12.25

US 8843573 B2, 2014.09.23

(43) 申请公布日 2019.10.15

CN 108712403 A, 2018.10.26

(73) 专利权人 北京邮电大学

审查员 李姮

地址 100876 北京市海淀区西土城路10号

(72) 发明人 张淼 徐国爱 李婧 王浩宇

(74) 专利代理机构 北京同立钧成知识产权代理

有限公司 11205

代理人 张子青 刘芳

(51) Int. Cl.

H04L 29/06 (2006.01)

H04L 29/08 (2006.01)

H04L 29/12 (2006.01)

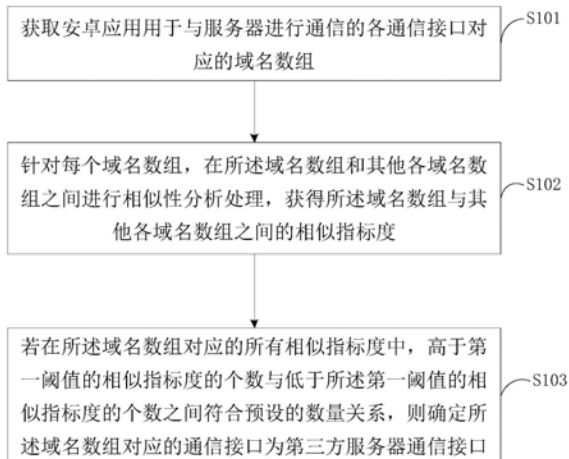
权利要求书2页 说明书14页 附图4页

(54) 发明名称

安卓应用的通信接口采集方法及装置

(57) 摘要

本申请提供安卓应用的通信接口采集方法及装置。方法获取安卓应用用于与服务器进行通信的各通信接口对应的域名数组；针对每个域名数组，在所述域名数组和其他各域名数组之间进行相似性分析处理，获得所述域名数组与其他各域名数组之间的相似指标度；若在所述域名数组对应的所有相似指标度中，高于第一阈值的相似指标度的个数与低于所述第一阈值的相似指标度的个数之间符合预设的数量关系，则确定所述域名数组对应的通信接口为第三方服务器通信接口。本发明提供的安卓应用的通信接口采集方法及装置通过通信接口域名的相似度筛选识别筛选出安卓应用中的第三方服务器通信接口，准确度高，大大提高了通信接口采集的纯净度。



1. 一种安卓应用的通信接口采集方法,其特征在于,包括:

获取安卓应用用于与服务器进行通信的各通信接口对应的域名数组;

针对每个域名数组,在所述域名数组和其他各域名数组之间进行相似性分析处理,获得所述域名数组与其他各域名数组之间的相似指标度,所述域名数组为对域名按照域名层级进行分割后得到的多个字符串组合构成的数组,所述相似指标度为待比较的两个域名数组中字符串相同位置的相同字符的个数;

若在所述域名数组对应的所有相似指标度中,高于第一阈值的相似指标度的个数小于低于所述第一阈值的相似指标度的个数,则确定所述域名数组对应的通信接口为第三方服务器通信接口。

2. 根据权利要求1所述的方法,其特征在于,所述获取安卓应用与服务器通信的各通信接口对应的域名数组包括:

获取安卓应用用于与服务器进行通信的各通信接口的接口信息,其中,所述接口信息中包括URL地址;

针对每个通信接口,对所述通信接口对应的URL地址进行域名截取处理,得到所述通信接口对应的域名数组;其中,所述通信接口对应的域名数组包含根据域名层级对该通信接口对应的域名进行分割后得到的多个字符串。

3. 根据权利要求2所述的方法,其特征在于,所述获取安卓应用用于与服务器进行通信的各通信接口的接口信息包括:

运行所述安卓应用的应用程序,并逐一切换到所述安卓应用的各运行页面上,针对每个运行页面,确定所述运行页面用于与服务器进行通信的第一通信接口,并获取所述第一通信接口对应的接口信息;

对所述安卓应用的应用程序进行静态分析,确定所述安卓应用用于与所述服务器进行通信的多个第二通信接口,并获取各第二通信接口对应的接口信息;

对所有第一通信接口的接口信息和所有第二通信接口的接口信息进行求并集处理,获得所述安卓应用用于与服务器进行通信的各通信接口的接口信息。

4. 根据权利要求3所述的方法,其特征在于,所述运行所述安卓应用的应用程序,并逐一切换到所述安卓应用的各运行页面上,包括:

运行所述安卓应用的可执行安装包,通过自动遍历方式对所述安卓应用的可点击元素进行遍历点击,以切换到所述安卓应用的各运行页面上。

5. 根据权利要求3所述的方法,其特征在于,所述针对每个运行页面,确定所述运行页面用于与服务器进行通信的第一通信接口,并获取所述第一通信接口对应的接口信息包括:

针对每个运行页面,确定所述运行页面用于与服务器进行通信的第一通信接口,在第一时刻对所述第一通信接口进行钩取,得到所述第一通信接口调用函数的传入参数,并从所述传入参数中获取所述第一通信接口对应的接口信息,其中,所述第一时刻为对所述第一通信接口发送的请求数据包进行封装之后,在对所述请求数据包进行加密之前的时刻。

6. 根据权利要求5所述的方法,其特征在于,所述方法还包括:

在第一时刻对所述第一通信接口进行钩取,得到所述第一通信接口调用函数的传入参数的同时,获取所述运行页面调用所述第一通信接口的活动,建立所述第一通信接口与所

述活动的对应关系。

7. 根据权利要求2所述的方法,其特征在于,所述针对每个域名数组,在所述域名数组和其他各域名数组之间进行相似性分析处理,获得所述域名数组与其他各域名数组之间的相似指标度包括:

针对每个域名数组,将所述数组中的每个字符串与待对比域名数组的各字符串进行两两对比,获得所述字符串与所述待对比域名数组中各字符串的相似个数,所述字符串的相似个数为在对比的两个字符串相同位置具有相同的字符的情况发生的次数;其中,所述待对比域名数组为其他各域名数组中的一个域名数组;

统计所述域名数组中的所有字符串的相似个数,将该相似个数确定为所述域名数组与待对比域名数组之间的相似指标度。

8. 一种安卓应用的通信接口采集装置,其特征在于,包括:

获取模块,用于获取安卓应用用于与服务器进行通信的各通信接口对应的域名数组;

相似性分析模块,用于针对每个域名数组,在所述域名数组和其他各域名数组之间进行相似性分析处理,获得所述域名数组与其他各域名数组之间的相似指标度,所述域名数组为对域名按照域名层级进行分割后得到的多个字符串组合构成的数组,所述相似指标度为待比较的两个域名数组中字符串相同位置的相同字符的个数;

确定模块,用于若在所述域名数组对应的所有相似指标度中,高于第一阈值的相似指标度的个数小于低于所述第一阈值的相似指标度的个数,则确定所述域名数组对应的通信接口为第三方服务器通信接口。

9. 一种安卓应用的通信接口采集设备,其特征在于,包括存储器、处理器;

存储器:用于存储所述处理器可执行指令;

其中,所述处理器被配置为:执行所述可执行指令以实现如权利要求1至7任一项所述的方法。

10. 一种计算机可读存储介质,其特征在于,所述计算机可读存储介质中存储有计算机执行指令,所述计算机执行指令被处理器执行时用于实现如权利要求1至7任一项所述的方法。

安卓应用的通信接口采集方法及装置

技术领域

[0001] 本申请涉及软件开发技术领域,尤其涉及一种安卓应用的通信接口采集方法及装置。

背景技术

[0002] 随着安卓(Android)移动智能终端的迅速普及,安卓应用(APP)的种类及数量越来越多,安卓应用实现的功能也越来越复杂。安卓客户端处理器和存储空间有限,如果将安卓应用中承载的功能放在客户端处理则会极大的影响用户体验。基于此,安卓应用客户端通常只负责与用户交互,然后将用户数据发送给服务器,由服务器处理后返回结果,安卓应用客户端再对数据进行图形化渲染和展示。

[0003] 安卓应用与服务器通信过程中的安全缺陷将会极大程度的影响安卓应用整体的安全性,安卓应用中诸如支付、推送、统计等功能不可避免地会使用第三方服务器通信接口,该部分通信接口不属于安卓应用的私有服务器,安卓应用私有服务器通信接口的准确采集有助于针对性地分析和改善安卓应用服务器端的安全设计。现有技术中主要基于动态分析采集安卓应用的通信接口,通过网络通信的分析获取安卓应用的通信接口。

[0004] 由于通信接口采集不是动态分析主要关注点,只作为附加功能存在,故动态分析中未对安卓应用的第三方服务器通信接口进行识别,导致现有技术中安卓应用的通信接口的采集结果纯净度低。

发明内容

[0005] 本申请提供一种安卓应用的通信接口采集方法及装置,用以解决现有技术中安卓应用的通信接口采集中未对第三方服务器通信接口进行识别的技术问题。

[0006] 第一方面,本发明实施例提供了一种安卓应用的通信接口采集方法,包括:

[0007] 获取安卓应用用于与服务器进行通信的各通信接口对应的域名数组;

[0008] 针对每个域名数组,在所述域名数组和其他各域名数组之间进行相似性分析处理,获得所述域名数组与其他各域名数组之间的相似指标度;

[0009] 若在所述域名数组对应的所有相似指标度中,高于第一阈值的相似指标度的个数与低于所述第一阈值的相似指标度的个数之间符合预设的数量关系,则确定所述域名数组对应的通信接口为第三方服务器通信接口。

[0010] 第二方面,本发明实施例提供了一种安卓应用的通信接口采集装置,包括:

[0011] 获取模块,用于获取安卓应用用于与服务器进行通信的各通信接口对应的域名数组;

[0012] 相似性分析模块,用于针对每个域名数组,在所述域名数组和其他各域名数组之间进行相似性分析处理,获得所述域名数组与其他各域名数组之间的相似指标度;

[0013] 确定模块,用于若在所述域名数组对应的所有相似指标度中,高于第一阈值的相似指标度的个数与低于所述第一阈值的相似指标度的个数之间符合预设的数量关系,则确

定所述域名数组对应的通信接口为第三方服务器通信接口。

[0014] 第三方面,本发明实施例提供了一种安卓应用的通信接口采集设备,包括存储器、处理器;

[0015] 存储器:用于存储所述处理器可执行指令;

[0016] 其中,所述处理器被配置为:执行所述可执行指令以实现上述第一方面任一项所述的方法。

[0017] 第四方面,本发明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中存储有计算机执行指令,所述计算机执行指令被处理器执行时用于实现上述第一方面任一项所述的方法。

[0018] 本发明实施例提供的安卓应用的通信接口采集方法及装置,获取安卓应用用于与服务器进行通信的各通信接口对应的域名数组;针对每个域名数组,在所述域名数组和其他各域名数组之间进行相似性分析处理,获得所述域名数组与其他各域名数组之间的相似指标度;若在所述域名数组对应的所有相似指标度中,高于第一阈值的相似指标度的个数与低于所述第一阈值的相似指标度的个数之间符合预设的数量关系,则确定所述域名数组对应的通信接口为第三方服务器通信接口。本发明实施例提供的安卓应用的通信接口采集方法通过通信接口域名的相似度筛选出安卓应用中所有的第三方服务器通信接口,实现了第三方服务器通信接口和安卓应用私有服务器通信接口的分类,以便剔除安卓应用的第三方服务器通信接口,准确度高,大大提高了安卓应用通信接口采集的纯净度。

附图说明

[0019] 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。

[0020] 图1为本发明一实施例提供的安卓应用的通信接口采集方法的流程示意图;

[0021] 图2为本发明另一实施例提供的安卓应用的通信接口采集方法的流程示意图;

[0022] 图3为本发明再一实施例提供的安卓应用的通信接口采集方法的流程示意图;

[0023] 图4为本发明又一实施例提供的安卓应用的通信接口采集方法的流程示意图;

[0024] 图5为本发明下一实施例提供的安卓应用的通信接口采集方法的流程示意图;

[0025] 图6为本发明一实施例提供的安卓应用的通信接口采集装置的结构示意图;

[0026] 图7为本发明另一实施例提供的安卓应用的通信接口采集装置的结构示意图;

[0027] 图8为本发明又一实施例提供的安卓应用的通信接口采集装置的结构示意图;

[0028] 图9为本发明一实施例提供的安卓应用的通信接口采集设备的硬件结构示意图。

[0029] 通过上述附图,已示出本公开明确的实施例,后文中将有更详细的描述。这些附图和文字描述并不是为了通过任何方式限制本公开构思的范围,而是通过参考特定实施例为本领域技术人员说明本公开的概念。

具体实施方式

[0030] 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。

[0031] 此外,参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。

[0032] 安卓恶意应用造成个人信息的泄露,给广大用户带来了财产损失和安全风险,并且危及了移动互联网的网络空间安全。在这种情况下,对移动智能终端的安卓应用进行安全检测,遏制移动互联网恶意应用的泛滥,有着尤为重要的意义。

[0033] 安卓应用与服务器通信过程中的安全缺陷将会极大程度的影响安卓应用整体的安全性,安卓应用中诸如支付、推送、统计等功能不可避免地会使用第三方服务器通信接口,该部分通信接口不属于安卓应用的私有服务器,不属于安全应用安全监测的范畴,故安卓应用私有服务器通信接口的准确采集有助于针对性地分析和改善安卓应用服务器端的安全设计。本申请提供的安卓应用的通信接口采集方法,通过通信接口域名的相似度筛选出安卓应用中所有的第三方服务器通信接口,识别准确度高,进而大大提高了安卓应用通信接口采集的纯净度。

[0034] 下面以具体地实施例对本申请的技术方案以及本申请的技术方案如何解决上述技术问题进行详细说明。下面这几个具体的实施例可以相互结合,对于相同或相似的概念或过程可能在某些实施例中不再赘述。下面将结合附图,对本申请的实施例进行描述。

[0035] 首先,对本申请中涉及的专有名词进行解释如下:

[0036] 域名数组,对域名按照域名层级进行分割后得到的多个字符串组合构成的数组。

[0037] 相似指标度 k ,指两个域名数组之间的相似指标度,具体是指待比较的两个域名数组中的字符串之间的相似度,由待比较的两个域名数组中字符串相同位置的相同字符的个数表示。

[0038] 动态分析,是指在严格控制的环境中(如沙盒、虚拟机、物理隔绝的主机等)执行软件的安装、运行等操作,借助受控环境监测并记录该对象的行为,如API调用及参数、网络通信、文件读写、进程操作等。

[0039] 静态分析,是指在不执行程序的情况下对安卓应用进行的分析或基于程序的形式、结构或者文档评估安卓应用的过程。

[0040] 图1为本发明一实施例提供的安卓应用的通信接口采集方法的流程示意图。如图1所示,该方法包括:

[0041] S101、获取安卓应用用于与服务器进行通信的各通信接口对应的域名数组。

[0042] 安卓应用用于与服务器进行通信的通信接口包括安卓应用运行中调用的第三方服务器接口和安卓应用私有服务器接口。可选地,依据域名进行第三方服务器接口和安卓应用私有服务器接口的划分。

[0043] 可选地,获取安卓应用用于与服务器进行通信的通信接口接口信息的方法包括下述任一项:对安卓应用的apk文件进行静态分析、对安卓应用的可执行程序进行动态分析以及对安卓应用与服务器之间的通信进行流量分析。可选地,动态分析工具包括Inspeckage、DroidBox中任意一项。

[0044] 通信接口的接口信息包括统一资源定位符URL、参数以及请求方式,URL中包含有通信接口的域名。实际应用中,通过上述任一项方式获取通信接口的URL,然后对各通信接口对应的URL进行截取和分割获得各通信接口对应的域名数组。应理解的是,域名数组中包含有多个字符串。

[0045] S102、针对每个域名数组,在所述域名数组和其他各域名数组之间进行相似性分析处理,获得所述域名数组与其他各域名数组之间的相似指标度 k 。

[0046] 安卓应用用于与服务器进行通信的通信接口有多个,每个通信接口具有对应的域名数组。针对每个域名数组,将所述域名数据与其他各域名数据进行相似性分析处理。实际应用中,首先选择一个域名数组为第一域名数组,然后在除第一域名数组之外的其他各域名数组中选择一个域名数组为第二域名数组;对第一域名数组和第二域名数组进行相似性分析处理,获得第一域名数组和第二域名数组之间的相似指标度 k ,即第一域名数组中各字符串和第二域名数组中各字符串中相同位置的相同字符的个数。然后更换第二域名数组,重复上述步骤,直至第一域名数组和其他各域名数组均完成相似性分析处理,获得第一域名数组与其他各域名数组之间的多个相似指标度 k 。可选地,将多个相似指标度 k 按照数组组合构成第一域名数组对应的相似指标数组。

[0047] S103、若在所述域名数组对应的所有相似指标度中,高于第一阈值的相似指标度的个数与低于所述第一阈值的相似指标度的个数之间符合预设的数量关系,则确定所述域名数组对应的通信接口为第三方服务器通信接口。

[0048] 实际应用中,具有完全相同或高度相似域名的两个通信接口可以判定为同一功能类别的通信接口,由于第三方服务器功能差异大、种类多,故第三方服务器通信接口与多个其他通信接口进行相似度分析处理后,高相似指标度的数量应远远小于低相似指标度的数量,即高于第一阈值的相似指标度的个数远低于第一阈值的相似指标度的个数时,可判定所述域名数组对应的通信接口为第三方服务器通信接口。可选地,预设的数量关系为小于1大于0的数字,优选地,预设的数量关系小于0.1。

[0049] 具体地,获取安卓应用用于与服务器进行通信的所有通信接口的接口信息,对每个通信接口的域名数组进行上述步骤S102和步骤S103的处理,识别安卓应用所有的第三方服务器通信接口。

[0050] 为了获得安卓应用私有服务器接口,可选地,在一种具体的实施方式中,剔除安卓应用的所有通信接口中的第三方服务器通信接口,获得安卓应用私有服务器接口,以便进行后续的私有服务器接口安全性分析。

[0051] 本发明实施例提供的安卓应用的通信接口采集方法,获取安卓应用用于与服务器进行通信的各通信接口对应的域名数组;针对每个域名数组,在所述域名数组和其他各域名数组之间进行相似性分析处理,获得所述域名数组与其他各域名数组之间的相似指标度;若在所述域名数组对应的所有相似指标度中,高于第一阈值的相似指标度的个数与低于所述第一阈值的相似指标度的个数之间符合预设的数量关系,则确定所述域名数组对应的通信接口为第三方服务器通信接口。本发明实施例提供的安卓应用的通信接口采集方法通过通信接口域名的相似度筛选出安卓应用中所有的第三方服务器通信接口,实现了第三方服务器通信接口和安卓应用私有服务器通信接口的分类,以便剔除安卓应用的第三方服务器通信接口,准确度高,大大提高了安卓应用通信接口采集的纯净度。

[0052] 图2为本发明另一实施例提供的安卓应用的通信接口采集方法的流程示意图。本实施例对图1所述实施例的基础上,对步骤S101进行了优化。如图2所述,步骤S101获取安卓应用用于与服务器进行通信的各通信接口对应的域名数组包括:

[0053] S201、获取安卓应用用于与服务器进行通信的各通信接口的接口信息,其中,所述接口信息中包括URL地址。

[0054] S202、针对每个通信接口,对所述通信接口对应的URL地址进行域名截取处理,得到所述通信接口对应的域名数组;其中,所述通信接口对应的域名数组包含根据域名层级对该通信接口对应的域名进行分割后得到的多个字符串。

[0055] 可选地,获取安卓应用用于与服务器进行通信的通信接口接口信息的方法包括下述任一项:对安卓应用的apk文件进行静态分析、对安卓应用的可执行程序进行动态分析以及对安卓应用与服务器之间的通信进行流量分析。可选地,动态分析工具包括Inspeckage、DroidBox中任意一项。

[0056] 通信接口的接口信息包括统一资源定位符URL地址、参数以及请求方式,具体地,URL地址由IP或域名、端口号、资源位置、参数、锚点依次组合在一起构成,即URL地址中包含有通信接口的域名。

[0057] 域名中包括有多个字符串,一个完整的域名由2个或2个以上的部分(具体体现为字符串)组成,各部分之间用英文的句号“.”来分隔,最后一个“.”的右边部分称为顶级域名(TLD,也称为一级域名),最后一个“.”的左边部分称为二级域名(SLD),二级域名的左边部分称为三级域名,以此类推,每一级的域名控制它下一级域名的分配。如:something.domainpeople.com这个域名,由三级域名something和二级域名domainpeople及顶级域名com组成。实际应用中,根据域名的层级对域名进行分割后得到的多个字符串,将多个字符串按照数组方式组合生成域名数组。

[0058] 为了获取通信接口对应的域名数组,在一种实施方式中,对安卓应用的可执行性程序进行动态分析,获得安全应用各通信接口的接口信息,针对每个通信接口,所述接口信息包括该通信接口的URL,对所述通信接口的URL地址进行域名截取处理,得到所述通信接口对应的域名,按照域名层级对上述域名进行分割,得到组成域名的多个字符串,将多个所述字符串按照数组格式组合,得到该通信接口对应的域名数组。

[0059] 本发明实施例提供的安卓应用的通信接口采集方法,获取安卓应用用于与服务器进行通信的各通信接口的接口信息,并对各通信接口的接口信息进行预处理,获得各通信接口对应的域名数组,便于下一步进行域名数组之间的基于字符串的相似度分析。

[0060] 在实际应用场景中,安卓应用用于与服务器进行通信的各通信接口的接口信息既可以通过对安卓应用的可执行程序进行动态分析获得,也可以通过对安卓应用的程序源码进行静态分析获得,下面通过图3所示的实施例,对如何获取各通信接口的接口信息进行详细说明。

[0061] 图3为本发明再一实施例提供的安卓应用的通信接口采集方法的流程示意图,本实施例在图2所述实施例的基础上,对步骤S201进行了优化。如图3所示,所述获取安卓应用用于与服务器进行通信的各通信接口的接口信息包括:

[0062] S301、运行所述安卓应用的应用程序,并逐一切换到所述安卓应用各运行页面上,针对每个运行页面,确定所述运行页面用于与服务器进行通信的第一通信接口,并获取

所述第一通信接口对应的接口信息。

[0063] 实际应用中,安卓应用与服务器的网络通信具有动态性的特征,随着用户访问安卓应用的不同的运行页面以及用户权限的变化,安卓应用与服务器之间具有不同的请求方式和接口信息参数,可通过在安卓应用端采用动态分析的方式对安卓应用与服务器之间的网络通信行为进行分析,跟随安卓应用运行的过程捕获各通信接口的接口信息。

[0064] 安卓应用用于与服务器进行通信的通信接口包括统一资源定位符(Uniform Resource Locator,URL)、参数和请求方式等,安卓应用开发人员为了保障服务器端通信接口保密性,通常采用HTTPS(Secure Hypertext Transfer Protocol,安全超文本传输协议)或者加密算法对安卓应用与服务器通信时的内容进行加密。

[0065] 鉴于目前应用市场中的安卓应用绝大多数都进行了代码混淆与加固,单独利用静态反编译smali分析无法达到预期效果,且经过混淆的代码很难找到所有网络通信接口的准确位置并进行修改,因此采用Hook技术,在不修改apk的情况下干预应用程序执行。为了获取这些隐藏在安卓应用中的服务器网络通信接口,可选地,在一种实施方式中,运行所述安卓应用的应用程序,并逐一切换到所述安卓应用的各运行页面,在每个运行页面上,确定所述运行页面用于与服务器进行通信的第一通信接口,在第一时刻对所述第一通信接口进行钩取,得到所述第一通信接口调用函数的传入参数,并从所述传入参数中获取所述第一通信接口对应的接口信息,其中,所述第一时刻为对所述第一通信接口发送的请求数据包进行封装之后,在对所述请求数据包进行加密之前的时刻。应理解的是,第一通信接口即为当前发送HTTP请求的通信接口。

[0066] 钩取(Hook)可以是消息处理中一个环节,主要用于监控消息在系统中的传递,并在消息最终处理前进行某些特定操作。Hook的本质是劫持API的函数调用,通过Hook技术获取想要进行动态行为分析的API函数地址,即可以对改地址进行重新定义,使得安卓应用运行时调用自定义API而不是系统原始API,也可以获取函数的传入参数,获得目标参数信息。

[0067] 可选地,采用Xposed框架对安卓网络通信的通信接口进行Hook,具体体现为利用Xposed框架对安卓应用在发送HTTP数据包和对HTTPS协议数据包加密之前进行Hook,获取HTTP/HTTPS数据包内容。

[0068] 安卓应用进行HTTP/HTTPS网络通信的方式较为集中,主要有HTTPClient、HTTPURLConnection、volley、OkHTTP四种,上述四种方式均为调用安卓API实现。本实施例中通过Xposed框架Hook上述四个安卓API,参考API的源码,根据其函数调用栈,分析出第一时刻,即HTTP/HTTPS请求组装headers参数和请求数据后(即HTTP请求包已经组装完成),HTTPS协议的tsl/ssl加密之前的时刻,捕捉第一时刻的函数调用栈,在当前调用栈正在执行的调用函数处进行Hook,获取未加密的HTTP/HTTPS数据包请求数据,得到调用函数的传入参数,并从上述传入参数中获取所述第一通信接口对应的接口信息,包括URL地址。上述方法第一可避免重打包技术中对安卓应用程序反编译smali代码的复杂修改,第二由于在HTTP/HTTPS请求组装headers参数和请求数据后(即HTTP请求包已经组装完成),HTTPS协议的tsl/ssl加密之前的第一时刻进行Hook,即获取到未加密的HTTP/HTTPS数据包请求数据,然后定义Hook成功后的回调方法,取出将要发送的请求包数据,分析请求包的headers、params、host、HTTP method等参数并打印,获得通信接口的接口信息,解决了现有技术中HTTPS数据包已经加密,无法获取接口信息的技术问题。

[0069] 实际应用中,对四种网络通信方式进行源码分析,四种网络通信发送网络请求时对应的安卓API分如下表1所示,其中volley和okHTTP3属于开源框架,在引用时可能会被开发者放入app开发包的lib中,可通过反编译smali文件查看其引入的类名。

[0070] 表1

[0071]	通信方式	安卓API
	HTTPURLConnection	java.net.URL.openConnection
	HTTPClient	org.apache.HTTP.impl.client.AbstractHttpClient.execute
	volley	com.android.volley.RequestQueue.add
	OkHTTP	com.squareup.okHTTP3.OkHttpClient.newCall

[0072] 进一步地,现有技术中通信接口采集后未进行分类,而在采集的过程中基于活动Activity页面功能的不同对于通信接口信息分类是接口分类最好的时机,这将对后续进行通信接口安全的研究提供更强的针对性。活动Activity代表了一个具有用户界面的单一屏幕。运行页面与活动Activity为一一对应关系,将用于与服务器进行通信的通信接口与活动Activity对应有利于快速识别敏感通信接口。

[0073] 鉴于安卓应用通信接口的特殊性,无论安卓应用的功能如何多样化,对于服务端来说,都是接收安卓应用终端的网络请求,请求方式包括下述中任一种:get、post、delete、put、head、option、trace、patch。即,无论安卓应用的前端应用页面如何变化,对于服务端来说,都是接收参数并进行数据处理,将处理结果以序列化形式返回给安卓应用终端,再由安卓应用将处理结果处理成能够显示在运行页面的形式。其中,参数的来源包括两种,一是用户填写,包括登录/注册/关键字搜索等其他涉及到服务器需要根据用户输入对数据库进行增删改查操作的,二是安卓应用通过调用安卓系统API或在程序内部获取请求所需参数而不需要通过用户自行输入的,如获取定位/当前日期进行搜索。实际应用中,第一种方式通常被恶意利用来攻击服务器,故对用户输入页面(活动Activity)用于与服务器进行通信的通信接口为敏感通信接口,对该敏感通信接口进行加固,有利于提高安卓应用的安全性。实际应用中,需要用户输入的页面(对应唯一的活动Activity)可以通过功能和界面上进行判断,故将用于与服务器进行通信的通信接口与安卓活动Activity对应有利于快速识别敏感通信接口。

[0074] 为了建立通信接口与安卓应用运行页面的对应关系,可选地,在一个具体实施方式中,在第一时刻对所述第一通信接口进行钩取,得到所述第一通信接口调用函数的传入参数的同时,获取所述运行页面调用所述第一通信接口的活动,建立所述第一通信接口与所述活动的对应关系。

[0075] 具体地,可基于ActivityManager获取安卓应用中正在运行的活动Activity,ActivityManager是Android系统自带的与系统中所有Activity交互的类,可用于获得系统里正在运行的Activities,包括进程(Process)、Package、Service、Task等信息。实际应用中,在对所述运行页面对应的第一通信接口在第一时刻运行的通信函数进行钩取,得到所述通信函数的传入参数同时,(即捕捉到HTTP请求的同时),运行ActivityManager打印获得当前安卓应用运行页面的活动,实现了当前发送HTTP请求的通信接口与当前页面活动的对应。

[0076] 另外,为了切换至安卓应用的各运行页面,可以采用自动化遍历的方式或人工遍

历的方式逐一切换至安卓应用的各运行页面上。可选地,在一个具体实施方式中,运行所述安卓应用的可执行安装包,通过自动遍历方式对所述安卓应用的可点击元素进行遍历点击,以切换到所述安卓应用的各运行页面上。

[0077] 具体地,自动化遍历运行页面工具为Droidbot。Droidbot是安卓的轻量级测试输入生成器,可以随机点击视图按钮或脚本输入事件发送到安卓应用程序,实现更快更高的测试覆盖率,并在测试后生成UI转换图(UTG)。目前市面上绝大多数安卓都有登录功能,为了能够成功绕过登录页面和其他表单填写页面,尽可能完全地遍历安卓应用的页面集合,本实施方式中基于Droidbot提供的可编写脚本验证功能,在检测到安卓应用时,预先注册账号,在Droidbot运行环境中添加账号和其他表单信息的脚本,在Droidbot遍历识别页面时加载预先设置的表单信息。Droidbot对安装应用完成运行页面自动化遍历后,生成活动Activity和各通信接口之间的跳转关系图。

[0078] 采用自动化遍历工具可以通过安卓应用运行点击事件遍历能够访问到的所有活动Activity和服务端通信接口的对应关系,但是安卓应用中存在部分不能通过页面可达性分析到达的、独立的和废弃接口,上述接口不能通过自动化遍历工具到达,但仍作为安卓应用与服务器通信的攻击点(即能够通过该部分口访问服务器),故该部分接口也应作为安卓应用用于与服务器通信的接口予以采集,以保障通信接口采集的完整性。下面通过步骤S302详细说明如何获取安卓应用中存在的不能通过页面可达性分析到达的、独立的和废弃的接口。应理解的是,步骤S302与步骤301可以并行进行,不分先后。

[0079] S302、对所述安卓应用的应用程序进行静态分析,确定所述安卓应用用于与所述服务器进行通信的多个第二通信接口,并获取各第二通信接口对应的接口信息。

[0080] 静态分析,是指在不执行程序的情况下对安卓应用进行的分析或基于程序的形式、结构或者文档评估安卓应用的过程。安卓应用apk文件格式通常都包含一个classes.dex文件,可选地,对安卓应用的应用程序进行静态分析包括对安卓应用的apk文件的反编译smali源码的静态分析和对安卓应用的apk文件的解压缩至dex文件的静态分析。

[0081] 为了获得安卓应用用于与服务器进行通信的多个第二通信接口,在一种实施方式中,对apk文件文件进行解压缩处理获得dex文件包,dex文件作为Dalvik虚拟机的可执行文件,文件结构包括文件头、索引区、数据区。而URL是以字符串的形式出现在代码之中,因此本文对dex文件分析的区域主要集中在索引区的string_ids和数据区的string_data_item。String_ids区域存放的是string_id_item的列表,string_id_item中存储的是一个名为string_data_off的uint类型值,这个值表示对应的string_data_item在文件中的位置。根据string_ids所指的字符串位置和String_data_item的值,编写正则匹配程序,过滤出静态URL。

[0082] 此外,由于Dex文件中的string是apk程序代码中所有定义的字符串,不局限于在类和方法中使用的字符串,这一部分被使用的字符串在smali文件集合中可以发现,同时也需要进一步在smali文件中获取尚在使用的URL请求的相关参数信息,具体见下述的实施方式。

[0083] 在另一种实施方式中,通过已知的第三方反编译工具,对上述dex文件进行反编译处理,得到一个包含smali源码的文件目录,里面存放着所有反编译获得的smali文件。首先

对smali文件中将字符串值赋值给寄存器的const-string语句进行分析,找出其中符合URL正则匹配的字符串或与上文dex文件分析结果匹配的字符串。应理解的是,此时URL的检索范围包括上随意实施方式中尚在使用的URL。然后记录符合条件字符串所属文件与位置,通过上下文语义分析,找出发送请求的语句,进而找到存放参数的寄存器,提取key,输入URL和参数。

[0084] 为了清楚的说明本实施方式,安卓应用apk中使用volley的情况为例,包括如下语句:

```

[0085]     invoke-static {v2, v1, v0, v3},
        Lcom/glavesoft/parking/volley/net/VolleyUtil;->
        postObjectApi(Ljava/lang/String;Ljava/util/Map;
        Ljava/lang/reflect/Type;Lcom/glavesoft/parking/volley/net/Respo
        nseListener;)

```

[0086] 根据postObjectApi方法的参数列表,第二个参数为HTTP请求的参数,即v1寄存器的值,继续向smali文件的上文寻找,可得出v1寄存器所存参数Map类型的key值,即HTTP请求的参数名。

[0087] 实际应用中,可以同时采用上述两种实施方式,获取安卓应用中存在的不能通过页面可达性分析到达的、独立的和废弃的接口。

[0088] S303、对所有第一通信接口的接口信息和所有第二通信接口的接口信息进行求并集处理,获得所述安卓应用用于与服务器进行通信的各通信接口的接口信息。

[0089] 第一通信接口为通过对运行安卓应用程序进行动态分析获取的,第二通信接口对安卓应用程序的源代码进行静态分析获取的,对第一通信接口和第二通信接口求并集处理,可以最大范围的获得安卓应用用于与服务器通信的通信接口。

[0090] 本发明实施例提供的安卓应用的通信接口采集方法,通过并行进行动态分析和静态分析的获取接口信息并求并集的方式,能够充分的采集通信接口的接口信息,保障通信接口采集的完整性;同时在对安卓应用的程序进行动态分析采集通信接口的同时,实现活动Activity页面和当前发送HTTP请求的通信接口的对应,以便根据活动Activity页面功能的不同对通信接口进行分类,大大提高了后续接口安全性分析的针对性。

[0091] 图4为本发明又一实施例提供的安卓应用的通信接口采集方法的流程示意图。在上述实施例的基础上,例如,在图1所示实施例的基础上,本实施例对步骤S102的具体实现过程进行了优化。如图4所示,所述针对每个通信接口,在所述域名数组和其他各域名数组之间进行相似性分析处理,获得所述域名数组与其他各域名数组之间的相似指标度包括:

[0092] S401、针对每个通信接口,将所述数组中的每个字符串与待对比域名数组的各字符串进行两两对比,获得所述字符串与所述待对比域名数组中各字符串相同位置的相同字符的相似个数;其中,所述待对比域名数组为其他各域名数组中的一个域名数组。

[0093] 通信接口对应的域名数组包含根据域名层级对该通信接口对应的域名进行分割后得到的多个字符串。实际应用中,针对每个通信接口,对通信接口的URL地址进行域名截取处理,获得截取后的域名;并根据域名层级对截取后的域名进行分割处理得到多个字符串;对多个所述字符串进行组合得到所述通信接口对应的域名数组。

[0094] 每个域名数组包括有多个字符串,相同位置的相同字符具体是指,在对比的两个字符串相同位置具有相同的字符,两个字符串的字符个数可以不同。具体地,以字符串weixin和字符串alipay为例,两个字符串第三个字符均为“i”,故两个字符串的相似个数为1。实际应用中,以字符串为对比单元,将所述域名数组中的每个字符串依次与待对比域名数组的各个字符串进行对比,获得每个字符串对应的相似个数。应理解的是,两个字符串分别属于带对比的不同域名数组。

[0095] S402、统计所述域名数组中的所有字符串的相似个数,将该相似个数确定为所述域名数组与待对比域名数组之间的相似指标度。

[0096] 每个域名数据包括有多个字符串,对每个字符串对应的相似个数求和,获得所述域名数组对应的相似个数,该相似个数即为所述域名数组与待对比域名数组之间的相似指标度k。

[0097] 重复步骤S401和步骤S402,直至获得所述域名数组和其他各域名属猪之间的相似指标度k。

[0098] 实际应用中,首先选择一个域名数组为第一域名数组,然后在除第一域名数组之外的其他各域名数组中选择一个域名数组为第二域名数组;针对第一域名数组的每个字符串,将所述字符串与第二域名数据的各字符串进行对比,获得所述字符串与第二域名数组中各字符串相同位置的相同字符的相似个数,直至第一域名数组中的所有字符串分别与第二域名数组中的各字符串两两对比完成,将每个字符串对应的相似个数求和即为第一域名数组与第一域名数组的相似指标度k;然后更换第二域名数组,直至获得第一域名数组与其他各域名数组之间的相似指标度k。然后更换第一域名数组,直至获得任意两个域名数组之间的相似指标度。

[0099] 本实施例提供的安卓应用的通信接口采集方法,基于通信接口的URL字符串的相似度进行两个通信接口的相似度分析,可准确快速的获取两个通信接口域名的相似度。

[0100] 实际应用中,具有完全相同或高度相似域名的两个通信接口可以判定为同一功能类别的通信接口,由于第三方服务器功能差异大、种类多,故第三方服务器通信接口与多个其他通信接口进行相似度分析后,高相似指标度的数量应远远小于低相似指标度的数量,故满足上述条件的通信接口为第三方服务器通信接口。下面对根据域名数组与其他各域名数组之间的各相似指标度确定所述域名数组是否为第三方服务器通信接口的步骤进行详细说明。

[0101] 图5为本发明下一实施例提供的安卓应用的通信接口采集方法的流程示意图。在上述实施例的基础上,例如,在图1所示实施例的基础上,本实施例对步骤S103的具体实现过程进行了优化。如图5所示,所述若在所述域名数组对应的所有相似指标度中,高于第一阈值的相似指标度的个数与低于所述第一阈值的相似指标度的个数之间符合预设的数量关系,则确定所述域名数组对应的通信接口为第三方服务器通信接口包括:

[0102] S501、针对每个域名数组,将所述域名数组对应的各相似指标度组合成所述域名数组对应的相似指标数组。

[0103] 实际应用中,针对每个域名数组,对所述域名数组和待对比域名数组进行相似性分析处理,即可得到所述域名数组和所述待对比域名数组的相似指标度。其中,所述待对比域名数组为其他各域名数组中的任意一个域名数组。

[0104] 针对每个域名数组,将所述域名数组和其他各域名数组进行相似性分析处理获得的各相似指标度进行组合处理,即可获得所述域名数组对应的相似指标数组。

[0105] S502、对所述相似指标数组中高于第一阈值的相似指标度进行聚类,获得第一相似指标类,对所述相似指标数组中低于第一阈值的相似指标度进行聚类,获得第二相似指标类。

[0106] 实际应用中,基于已知的聚类算法对相似指标数组中的相似指标度k进行聚类,将各相似指标度划分为第一相似指标类和第二相似指标类,其中,第一相似指标类中相似指标度k值均大于第一阈值,第二相似指标类中相似指标度k值均小于第一阈值,可选地,第一阈值预先设定。可选地,聚类算法包括K-means聚类算法。

[0107] S503、将所述第一相似指标类中相似指标度的个数与所述第二相似指标类中相似指标的个数求商值;若所述商值小于预设值,则确定所述域名数组对应的通信接口为第三方服务器通信接口。

[0108] 具体地,第一相似指标类中相似指标的个数远远小于第二相似指标类中相似指标的个数时,所述域名数组对应的通信接口为第三方服务器通信接口。

[0109] 本实施例提供的安卓应用的通信接口采集方法,针对每个通信接口,通过聚类将各通信接口对应的相似指标度分为高于第一阈值的第一相似指标类和低于第一阈值的第二相似指标类,并通过第一相似指标类和第二相似指标类的个数的商值与预设值进行比较,进而识别该通信接口是否为第三方服务器通信接口,与采用流量分析识别第三方服务器的方式相比,可有效排除同时段其他应用网络流量的干扰,大大提高了安卓应用第三方服务器接口识别的准确度。

[0110] 基于上述实施例所提供的安卓应用的通信接口采集方法,本发明实施例进一步给出实现上述方法实施例的装置实施例。

[0111] 图6为本发明一实施例提供的安卓应用的通信接口采集装置的结构示意图。如图6所示,该安卓应用的通信接口采集装置600包括获取模块610、相似性分析模块620以及确定模块630。

[0112] 获取模块610,获取安卓应用用于与服务器进行通信的各通信接口对应的域名数组。

[0113] 相似性分析模块620,用于针对每个域名数组,在所述域名数组和其他各域名数组之间进行相似性分析处理,获得所述域名数组与其他各域名数组之间的相似指标度。

[0114] 确定模块630,用于若在所述域名数组对应的所有相似指标度中,高于第一阈值的相似指标度的个数与低于所述第一阈值的相似指标度的个数之间符合预设的数量关系,则确定所述域名数组对应的通信接口为第三方服务器通信接口。

[0115] 本发明实施例提供的安卓应用的通信接口采集装置,获取安卓应用用于与服务器进行通信的各通信接口对应的域名数组;针对每个域名数组,在所述域名数组和其他各域名数组之间进行相似性分析处理,获得所述域名数组与其他各域名数组之间的相似指标度;若在所述域名数组对应的所有相似指标度中,高于第一阈值的相似指标度的个数与低于所述第一阈值的相似指标度的个数之间符合预设的数量关系,则确定所述域名数组对应的通信接口为第三方服务器通信接口。本发明实施例提供安卓应用的通信接口采集装置通过通信接口域名的相似度筛选出安卓应用中所有的第三方服务器通信接口,实现了第三方

服务器通信接口和安卓应用私有服务器通信接口的分类,以便剔除安卓应用的第三方服务器通信接口,准确度高,大大提高了安卓应用通信接口采集的纯净度。

[0116] 可选地,相似性分析模块620,还具体用于:将所述数组中的每个字符串与待对比域名数组的各字符串进行两两对比,获得所述字符串与所述待对比域名数组中各字符串相同位置的相同字符的相似个数;其中,所述待对比域名数组为其他各域名数组中的一个域名数组;统计所述域名数组中的所有字符串的相似个数,将该相似个数确定为所述域名数组与待对比域名数组之间的相似指标度。

[0117] 图7为本发明另一实施例提供的安卓应用的通信接口采集装置的结构示意图。本实施例是对图6实施例中获取模块610的优化,如图7所示,获取模块610包括接口信息获取子模块710以及域名截取子模块720。

[0118] 信息获取子模块710,用于获取安卓应用用于与服务器进行通信的各通信接口的接口信息,其中,所述接口信息中包括URL地址。

[0119] 域名截取子模块720,用于针对每个通信接口,对所述通信接口对应的URL地址进行域名截取处理,得到所述通信接口对应的域名数组;其中,所述通信接口对应的域名数组包含根据域名层级对该通信接口对应的域名进行分割后得到的多个字符串。

[0120] 本发明实施例提供的安卓应用的通信接口采集装置,获取安卓应用用于与服务器进行通信的各通信接口的接口信息,针对每个通信接口,对通信接口对应的URL地址进行域名截取处理,并根据域名层级对截取后的域名进行分割处理得到多个字符串,对多个所述字符串进行组合得到所述通信接口对应的域名数组。本实施例中的接口采集装置通过各通信接口的接口信息获取其对应的域名数组,保障域名各字符串的完整度。

[0121] 图8为本发明又一实施例提供的安卓应用的通信接口采集装置的结构示意图。本实施例是对图7实施例中接口信息获取子模块710的优化,如图8所示,接口信息获取子模块710包括到动态分析单元810、静态分析单元820以及并集单元830。

[0122] 动态分析单元810,用于运行所述安卓应用的应用程序,并逐一切换到所述安卓应用的各运行页面上,针对每个运行页面,确定所述运行页面用于与服务器进行通信的第一通信接口,并获取所述第一通信接口对应的接口信息;

[0123] 静态分析单元820,用于对所述安卓应用的应用程序进行静态分析,确定所述安卓应用用于与所述服务器进行通信的多个第二通信接口,并获取各第二通信接口对应的接口信息;

[0124] 并集单元830,用于对所有第一通信接口的接口信息和所有第二通信接口的接口信息进行求并集处理,获得所述安卓应用用于与服务器进行通信的各通信接口的接口信息。

[0125] 可选地,动态分析单元810还具体用于,运行所述安卓应用的可执行安装包,通过自动遍历方式对所述安卓应用的可点击元素进行遍历点击,以切换到所述安卓应用的各运行页面上。

[0126] 可选地,动态分析单元810还具体用于,针对每个运行页面,对所述运行页面对应的第一通信接口在第一时刻运行的通信函数进行钩取,得到所述通信函数的传入参数,并从所述传入参数中获取所述第一通信接口对应的接口信息,其中,所述第一时刻为对所述第一通信接口发送的请求数据包进行封装之后,在对所述请求数据包进行加密之前的时

刻。

[0127] 可选地,动态分析单元810还具体用于,在对所述运行页面对应的第一通信接口在第一时刻运行的通信函数进行钩取,得到所述通信函数的传入参数同时,获取所述运行页面调用所述第一通信接口的活动,建立所述第一通信接口与所述活动的对应关系。

[0128] 本发明实施例提供的安卓应用的通信接口采集装置,通过动态分析单元获取第一通信接口对应的接口信息,通过静态分析单元获取第二通信接口对应的接口信息,对所有第一通信接口的接口信息和所有第二通信接口的接口信息进行求并集处理,获得安卓应用用于与服务器进行通信的各通信接口的接口信息,通过动态分析和静态分析的并行处理,大大提高了通信接口采集的完整度。此外,在对安卓应用的程序进行动态分析采集通信接口的同时,实现活动Activity页面和通信接口的对应,以便根据活动Activity页面功能的不同对通信接口进行分类,大大提高了后续接口安全性分析的针对性。

[0129] 图6至图8所示实施例的安卓应用的通信接口采集装置可用于执行上述方法中的技术方案,其实现原理和技术效果类似,本实施例此处不再赘述。

[0130] 应理解以上图6至图8所示安卓应用的通信接口采集装置的各个模块的划分仅仅是一种逻辑功能的划分,实际实现时可以全部或部分集成到一个物理实体上,也可以物理上分开。且这些模块可以全部以软件通过处理元件调用的形式实现;也可以全部以硬件的形式实现;还可以部分模块以软件通过处理元件调用的形式实现,部分模块通过硬件的形式实现。此外这些模块全部或部分可以集成在一起,也可以独立实现。这里所述的处理元件可以是一种集成电路,具有信号的处理能力。在实现过程中,上述方法的各步骤或以上各个模块可以通过处理器元件中的硬件的集成逻辑电路或者软件形式的指令完成。

[0131] 图9为本发明一实施例提供的安卓应用的通信接口采集设备的硬件结构示意图。如图9所示,本实施例提供的安卓应用的通信接口采集设备900包括:至少一个存储器910、处理器920以及计算机程序;其中,计算机程序存储在存储器910中,并被配置为由处理器920执行以实现如上述安卓应用的通信接口采集方法。安卓应用的通信接口采集设备900还包括通信部件。其中,处理器920、存储器910以及通信部件通过总线连接。

[0132] 本领域技术人员可以理解,图9仅仅是安卓应用的通信接口采集设备的示例,并不构成对安卓应用的通信接口采集设备的限定,安卓应用的通信接口采集设备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,例如所述安卓应用的通信接口采集设备还可以包括输入输出设备、网络接入设备、总线等。

[0133] 此外,本发明实施例提供了一种可读存储介质,其上存储有计算机程序,该计算机程序被处理器执行以实现上述任一实现方式所述的方法。

[0134] 上述可读存储介质可以是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。可读存储介质可以是通用或专用计算机能够存取的任何可用介质。

[0135] 最后应说明的是:以上各实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述各实施例对本发明进行了详细的说明,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,或者对其中部分或者全部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发明各实施例技术

方案的范围。

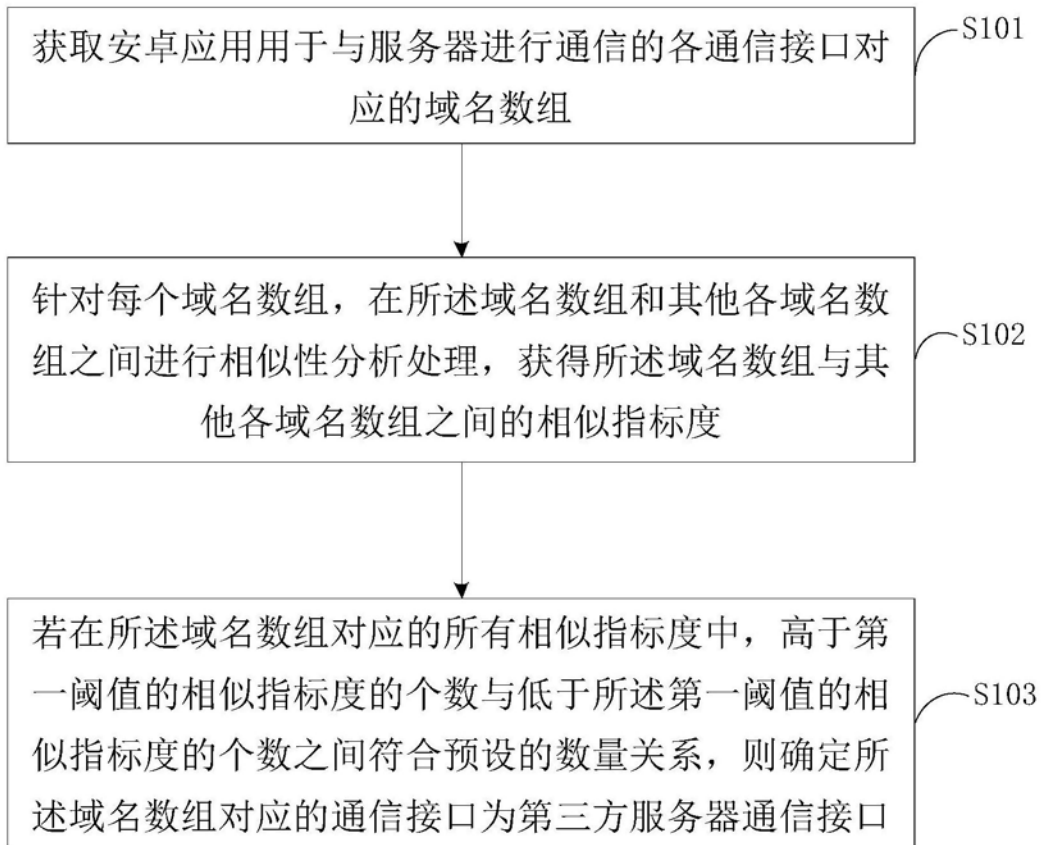


图1

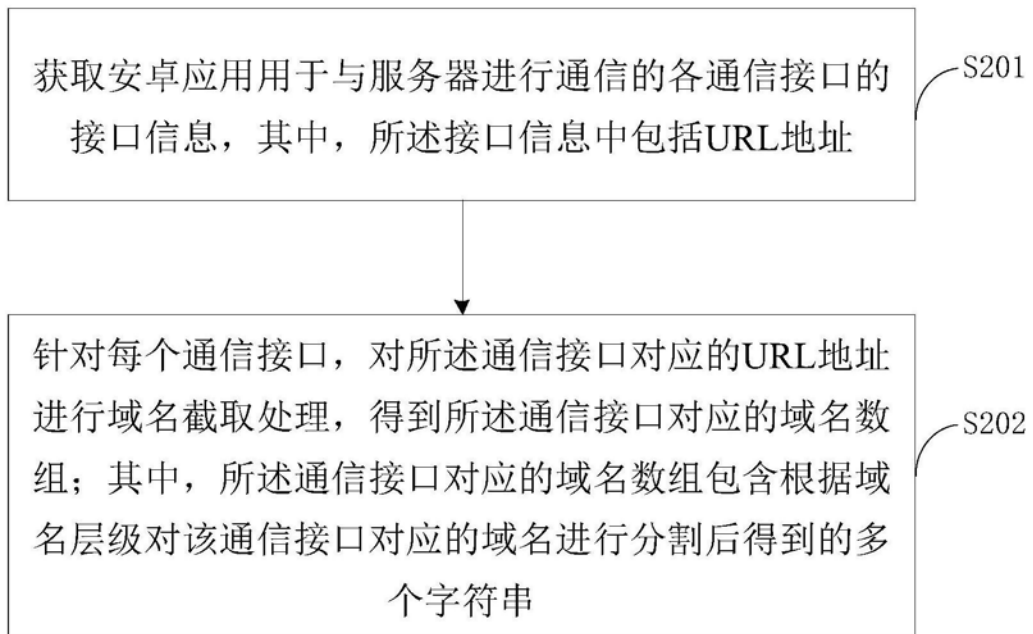


图2

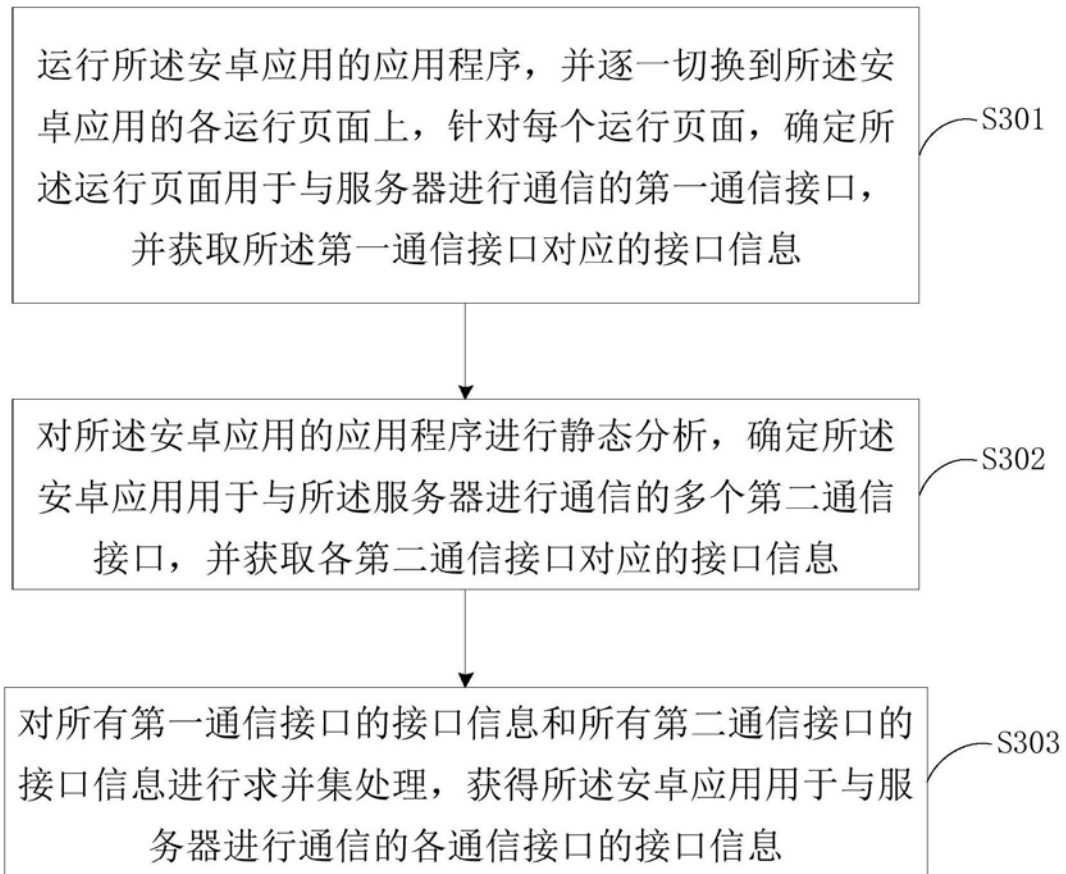


图3

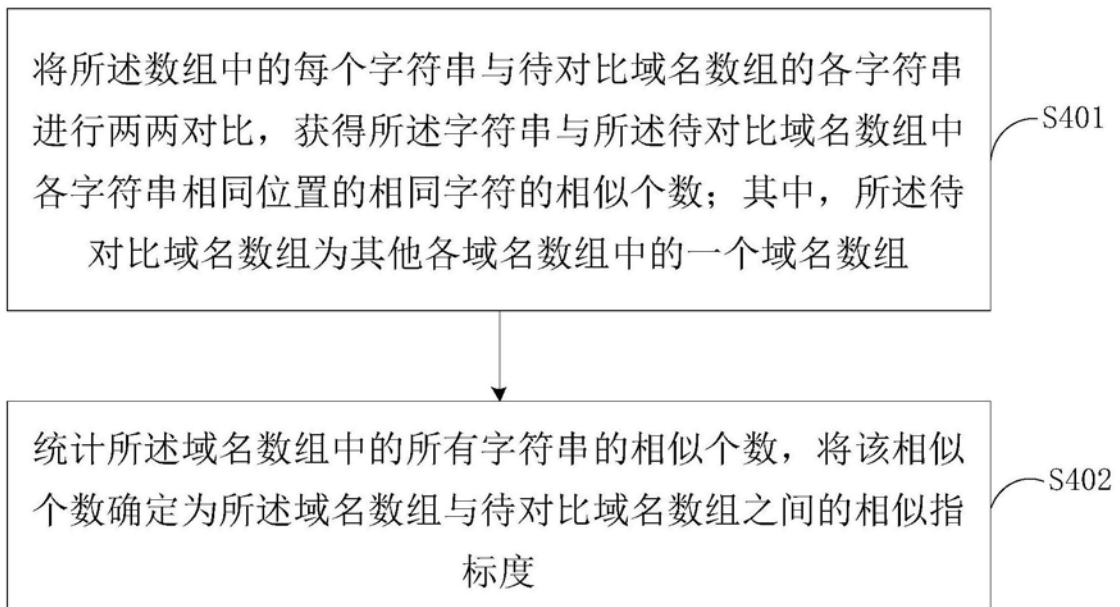


图4

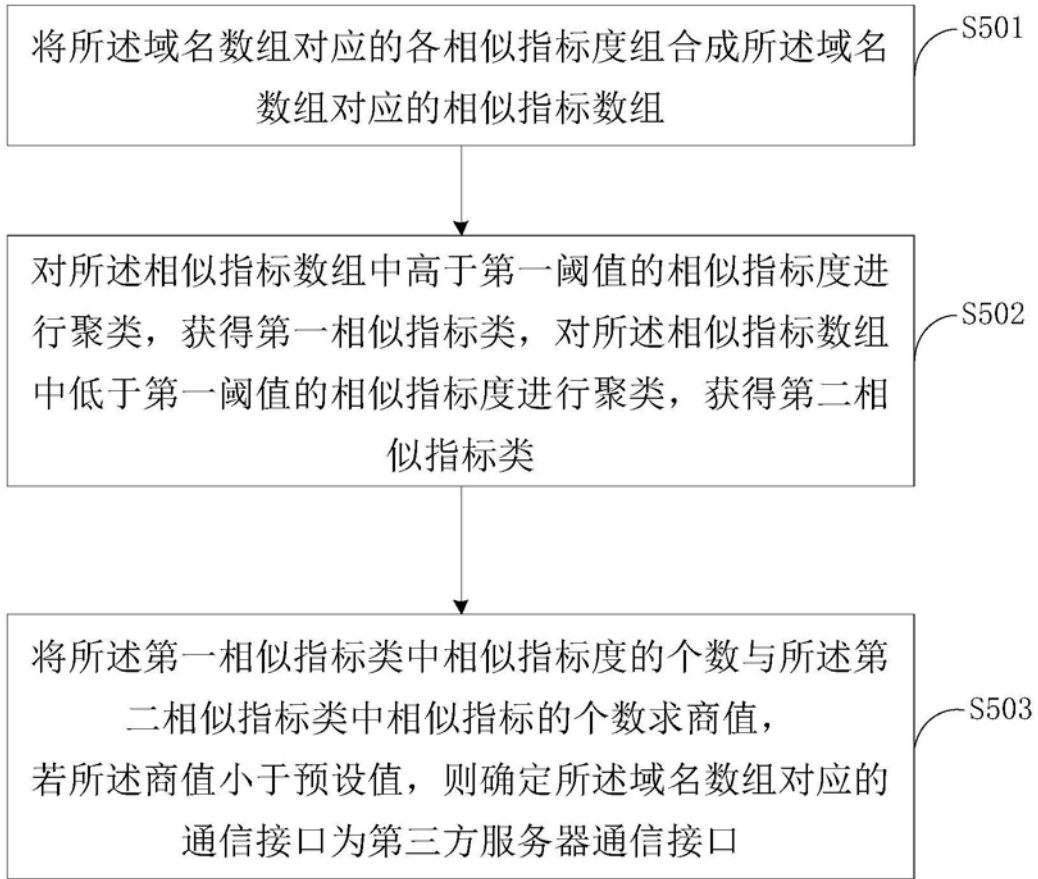


图5

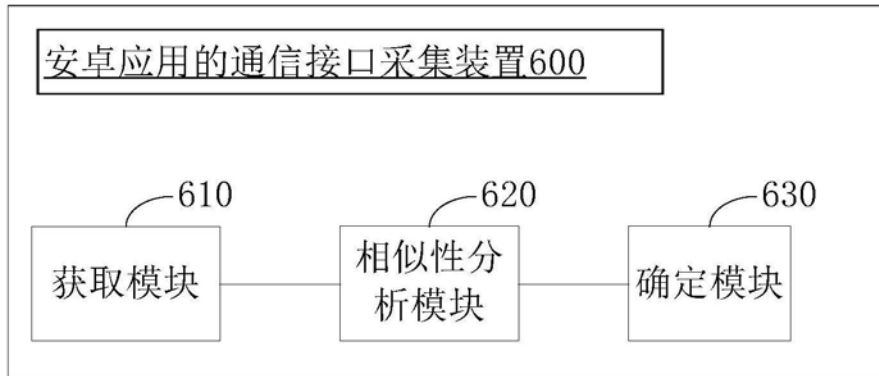


图6

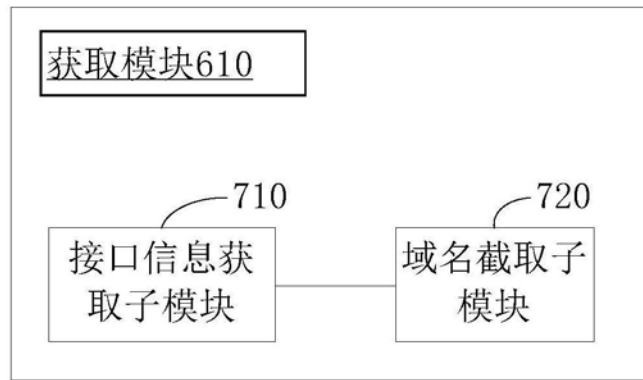


图7

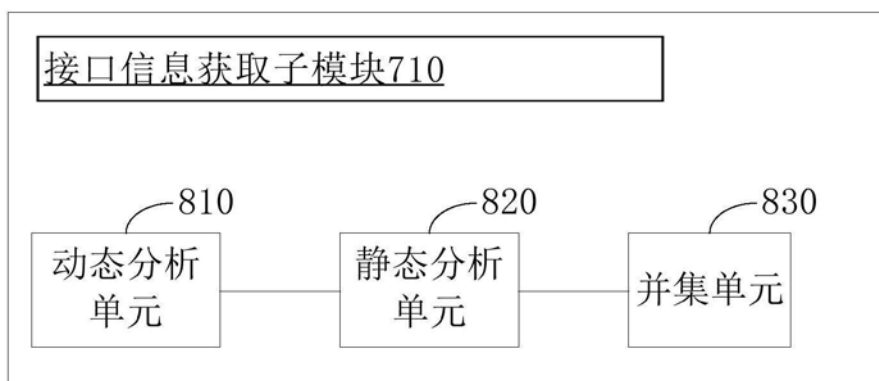


图8

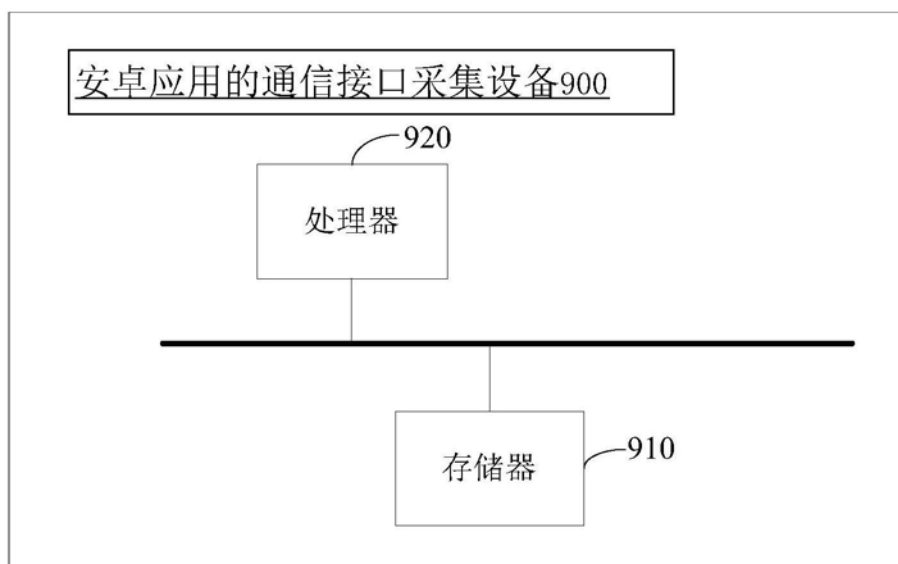


图9