(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 108154026 A
(43)申请公布日 2018.06.12

(21)申请号 201711464695.9

(22)申请日 2017.12.28

(71)申请人 成都卫士通信息产业股份有限公司
地址 610041 四川省成都市高新区云华路333号

(72)发明人 汪仕兵

(74)专利代理机构 成都市集智汇华知识产权代理事务所(普通合伙) 51237
代理人 李华 温黎娟

(51)Int.Cl.
G06F 21/44(2013.01)
G06F 9/445(2018.01)
H04M 1/725(2006.01)
H04L 29/06(2006.01)

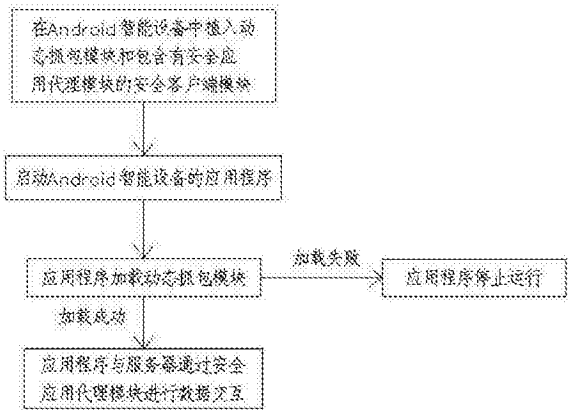
权利要求书2页 说明书5页 附图2页

(54)发明名称

基于Android系统的免Root无侵入的安全通信方法及系统

(57)摘要

本发明公开一种基于Android系统的免Root无侵入的安全通信方法，该方法用于实现Android智能设备与服务器之间的数据安全交互，包括：在Android智能设备中植入动态抓包模块和安全客户端模块；启动Android智能设备的应用程序；应用程序加载动态抓包模块，加载成功，则应用程序继续运行，加载失败，则应用程序停止运行；应用程序与服务器通过安全应用代理模块进行数据交互。本发明在整个数据交互过程中免Root无侵入，每一个应用程序都会加载一个动态抓包模块，不同的应用程序与服务器之间的信息通道是彼此独立的，可以有效隔离不同应用程序之间的数据，防止应用程序越权访问。



CN 108154026 A

1.基于Android系统的免Root无侵入的安全通信方法，该方法用于实现Android智能设备与服务器之间的数据安全交互，其特征在于，包括：

在Android智能设备中植入动态抓包模块和包含有安全应用代理模块的安全客户端模块；

启动Android智能设备的应用程序；

应用程序加载动态抓包模块，加载成功，则应用程序继续运行，加载失败，则应用程序停止运行；

应用程序与服务器通过安全应用代理模块进行数据交互。

2.根据权利要求1所述的基于Android系统的免Root无侵入的安全通信方法，其特征在于，所述应用程序加载动态抓包模块包括：

应用程序主动加载动态抓包模块；

动态抓包模块从安全客户端模块下载安全策略并解析；

动态抓包模块根据解析后的安全策略判别当前应用程序是否安全合法，如果是，则应用程序继续运行，如果不是，则应用程序停止运行；

动态抓包模块通过Android智能设备的AOP框架将当前应用程序使用的网络连接模块反射到安全代理模块，应用程序成功将动态抓包模块加载到应用程序网络框架中。

3.根据权利要求1所述的基于Android系统的免Root无侵入的安全通信方法，其特征在于，所述应用程序与服务器通过安全应用代理模块进行数据交互包括：

应用程序调用网络连接模块中的网络接口；

动态抓包模块调用安全客户端模块的安全应用代理模块；

Android智能设备的AOP框架将应用程序调用的网络接口自动发射给安全代理模块；

应用程序将数据发送给安全代理模块；

安全代理模块将从应用程序接收到的数据发送给服务器。

4.根据权利要求3所述的基于Android系统的免Root无侵入的安全通信方法，其特征在于，所述应用程序与服务器通过安全应用代理模块进行数据交互还包括：

服务器发送数据给安全代理模块；

安全代理模块将从服务器接收到的数据发送给Android智能设备的AOP框架；

应用程序自动通过Android智能设备的AOP框架接收数据。

5.根据权利要求1所述的基于Android系统的免Root无侵入的安全通信方法，其特征在于，在应用程序与服务器通过安全应用代理模块进行数据交互前还包括：通过安全客户端模块对服务器进行用户身份鉴别，如果服务器安全合法，则进行数据交互，反之，则不进行数据交互。

6.一种基于Android系统的免Root无侵入的安全通信系统，该系统通过权利要求1—5任意一项所述的安全通信方法在Android智能设备与服务器之间实现数据安全交互，其特征在于，所述安全通信系统包括：

动态抓包模块：植入于Android智能设备，用于供Android智能设备中的应用程序进行加载；

安全客户端模块：植入于Android智能设备，用于为所述动态抓包模块提供安全策略；

所述安全客户端模块内包含有安全应用代理模块，所述动态抓包模块自动调用所述安

全应用代理模块，所述安全应用代理模块用于为应用程序和服务端的数据交互提供安全通道。

7.根据权利要求6所述的一种基于Android系统的免Root无侵入的安全通信系统，其特征在于，所述动态抓包模块包括：

安全策略管理模块：用于从所述安全客户端模块下载安全策略并解析；

应用程序识别模块：用于根据解析后的安全策略判别当前应用程序是否安全合法；

网络框架动态加载模块：用于加载到Android智能设备的应用程序网路框架中。

8.根据权利要求6所述的一种基于Android系统的免Root无侵入的安全通信系统，其特征在于，所述安全客户端模块还设置有安全策略下发模块，所述安全策略下发模块用于为动态抓包模块提供安全策略。

9.根据权利要求8所述的一种基于Android系统的免Root无侵入的安全通信系统，其特征在于，所述安全客户端模块还设置有用户身份鉴别模块，所述用户身份鉴别模块用于鉴别服务器是否安全合法。

基于Android系统的免Root无侵入的安全通信方法及系统

技术领域

[0001] 本发明涉及通信安全领域，具体涉及一种基于Android系统的免Root无侵入的安全通信方法及系统。

背景技术

[0002] 随着Android手机、Android平板等Android智能设备大量涌入企业的办公环境中，企业员工通过这些智能设备处理公司相关业务，在享受移动办公带来便利性的同时，各种恶意攻击也在不知不觉中威胁着企业的信息安全，Android智能系统安全漏洞层出不穷，恶意软件铺天盖地，使企业急需使用安全设备在移动办公的环境下保护企业信息系统的安全性。现有的安全解决方案是在企业互联网入口部署传统VPN设备或安全网关设备，通过VPN设备或安全网关设备隔离功能对企业内部网络进行网络隔离及边界防护。

[0003] VPN设备在Android智能设备上使用虚拟网卡建立安全隧道，信息系统客户端通过虚拟网卡建立的安全隧道与信息系统服务器进行数据交互，但是这样的安全解决方案存在以下问题：使用安全隧道的应用程序身份不明确，恶意程序也可以使用安全通道访问企业内部网络，对企业内部网关进行攻击，窃取企业敏感信息；整个智能终端只能有一条安全隧道，各个应用系统间数据不能进行隔离，可能导致应用系统客户端越权访问其他应用系统服务器数据，存在安全隐患。

[0004] 传统安全网关在Android智能终端上采用获取Root权限，将网络数据包模块集成到操作系统中，通过接管系统相关功能实现应用系统网络数据包，该技术存在以下问题：需要获取Root权限，通过侵入接管系统相关功能，获取Root技术会根据不同的智能终端，采用不同Root方案，技术复杂且成功率低；获取Root权限后，恶意程序可以获取Root权限，导致整个智能终端被控制，进而对企业内部网络造成更大危害。

[0005] 因此，研究出一种基于Android系统的免Root无侵入并且具有独立安全通道的通信方法及系统具有非常重要的意义。

发明内容

[0006] 有鉴于此，本申请提供一种基于Android系统的免Root无侵入的安全通信方法及系统，通过在Android智能终端植入安全客户端和动态抓包模块，使Android智能终端的当前应用程序在和服务器进行数据交互前先进行动态抓包模块加载，加载成功后，当前应用程序再通过安全客户端和动态抓包模块共享的安全应用代理模块与服务器进行数据交互，整个数据交互过程免Root无侵入，既独立又安全。本发明通过以下技术方案实现：

[0007] 基于Android系统的免Root无侵入的安全通信方法，该方法用于实现Android智能设备与服务器之间的数据安全交互，包括：

[0008] 在Android智能设备中植入动态抓包模块和包含有安全应用代理模块的安全客户端模块；

[0009] 启动Android智能设备的应用程序；

[0010] 应用程序加载动态抓包模块，加载成功，则应用程序继续运行，加载失败，则应用程序停止运行；

[0011] 应用程序与服务器通过安全应用代理模块进行数据交互。

[0012] 进一步地，所述应用程序加载动态抓包模块包括：

[0013] 应用程序主动加载动态抓包模块；

[0014] 动态抓包模块从安全客户端模块下载安全策略并解析；

[0015] 动态抓包模块根据解析后的安全策略判别当前应用程序是否安全合法，如果是，则应用程序继续运行，如果不是，则应用程序停止运行；

[0016] 动态抓包模块通过Android智能设备的AOP框架将当前应用程序使用的网络连接模块反射到安全代理模块，应用程序成功将动态抓包模块加载到应用程序网络框架中。

[0017] 进一步地，所述应用程序与服务器通过安全应用代理模块进行数据交互包括：

[0018] 应用程序调用网络连接模块中的网络接口；

[0019] 动态抓包模块调用安全客户端模块的安全应用代理模块；

[0020] Android智能设备的AOP框架将应用程序调用的网络接口自动发射给安全代理模块；

[0021] 应用程序将数据发送给安全代理模块；

[0022] 安全代理模块将从应用程序接收到的数据发送给服务器。

[0023] 进一步地，所述应用程序与服务器通过安全应用代理模块进行数据交互还包括：

[0024] 服务器发送数据给安全代理模块；

[0025] 安全代理模块将从服务器接收到的数据发送给Android智能设备的AOP框架；

[0026] 应用程序自动通过Android智能设备的AOP框架接收数据。

[0027] 进一步地，在应用程序与服务器通过安全应用代理模块进行数据交互前还包括：通过安全客户端模块对服务器进行用户身份鉴别，如果服务器安全合法，则进行数据交互，反之，则不进行数据交互。

[0028] 一种基于Android系统的免Root无侵入的安全通信系统，该系统通过上述安全通信方法在Android智能设备与服务器之间实现数据安全交互，所述安全通信系统包括：

[0029] 动态抓包模块：植入于Android智能设备，用于供Android智能设备中的应用程序进行加载；

[0030] 安全客户端模块：植入于Android智能设备，用于为所述动态抓包模块提供安全策略；

[0031] 所述安全客户端模块内包含有安全应用代理模块，所述动态抓包模块自动调用所述安全应用代理模块，所述安全应用代理模块用于为应用程序和服务端的数据交互提供安全通道。

[0032] 进一步地，所述动态抓包模块包括：

[0033] 安全策略管理模块：用于从所述安全客户端模块下载安全策略并解析；

[0034] 应用程序识别模块：用于根据解析后的安全策略判别当前应用程序是否安全合法；

[0035] 网络框架动态加载模块：用于加载到Android智能设备的应用程序网路框架中。

[0036] 进一步地，所述安全客户端模块还设置有安全策略下发模块，所述安全策略下发

模块用于为动态抓包模块提供安全策略。

[0037] 进一步地，所述安全客户端模块还设置有用户身份鉴别模块，所述用户身份鉴别模块用于鉴别服务器是否安全合法。

[0038] 使用本发明时，首先，无需获取Root权限，可以实现免Root非侵入的数据交互，有效杜绝了获取系统Root权限带来的安全风险；其次，Android智能设备中每一个应用程序在都会加载一个动态抓包模块，并通过安全应用代理模块实现与服务器之间的通信。因此，不同的应用程序与服务器之间的信息通道是彼此独立的，可以有效隔离不同应用程序之间的数据，防止应用程序越权访问。另外，本发明能够准确识别应用程序是否安全合法，可以杜绝恶意软件对企业内部网络造成威胁。

附图说明

[0039] 图1为本发明实施例1提供的通信方法流程图。

[0040] 图2为本发明实施例1提供的应用程序加载动态抓包模块的具体流程图。

[0041] 图3为本发明实施例1提供的应用程序与服务器通过安全应用代理模块进行数据交互的具体流程图。

[0042] 图4为本发明实施例2提供的通信系统的结构框图。

具体实施方式

[0043] 为了使本领域的技术人员更好地理解本发明的技术方案，下面结合附图和具体实施例对本发明作进一步的详细说明。

[0044] 实施例1

[0045] 如图1所示，本实施例提供一种基于Android系统的免Root无侵入的安全通信方法，该方法用于实现Android智能设备与服务器之间的数据安全交互，包括：

[0046] 步骤S1：在Android智能设备中植入动态抓包模块和包含有安全应用代理模块的安全客户端模块；

[0047] 步骤S2：启动Android智能设备的应用程序；

[0048] 步骤S3：应用程序加载动态抓包模块，加载成功，则应用程序继续运行，加载失败，则应用程序停止运行；

[0049] 步骤S4：应用程序与服务器通过安全应用代理模块进行数据交互。

[0050] 具体地，如图2所示，步骤S4中所述应用程序加载动态抓包模块包括：

[0051] 步骤S301：应用程序主动加载动态抓包模块；

[0052] 步骤S302：动态抓包模块从安全客户端模块下载安全策略并解析；

[0053] 步骤S303：动态抓包模块根据解析后的安全策略判别当前应用程序是否安全合法，如果是，则应用程序继续运行，如果不是，则应用程序停止运行；

[0054] 步骤S304：动态抓包模块通过Android智能设备的AOP框架将当前应用程序使用的网络连接模块反射到安全代理模块，应用程序成功将动态抓包模块加载到应用程序网络框架中。

[0055] 具体地，如图3所示，步骤S4所述应用程序与服务器通过安全应用代理模块进行数据交互包括：

[0056] 步骤S401:应用程序调用网络连接模块中的网络接口;

[0057] 步骤S402:动态抓包模块调用安全客户端模块的安全应用代理模块;

[0058] 步骤S403:Android智能设备的AOP框架将应用程序调用的网络接口自动发射给安全代理模块;

[0059] 步骤S404:应用程序将数据发送给安全代理模块;

[0060] 步骤S405:安全代理模块将从应用程序接收到的数据发送给服务器。

[0061] 本实施例中,步骤S4还包括:

[0062] 步骤S406:服务器发送数据给安全代理模块;

[0063] 步骤S407:安全代理模块将从服务器接收到的数据发送给Android智能设备的AOP框架;

[0064] 步骤S408:应用程序自动通过Android智能设备的AOP框架接收数据。

[0065] 作为优选,在应用程序与服务器通过安全应用代理模块进行数据交互前还包括:通过安全客户端模块对服务器进行用户身份鉴别,如果服务器安全合法,则进行数据交互,反之,则不进行数据交互。

[0066] 其中,AOP是指针对业务处理过程中切面进行提取,它所面对的是处理过程中的某个步骤或阶段,以获得逻辑过程中各个部分之间的低耦合性的特殊功能。

[0067] 实施本实施例时,Android智能设备中的应用程序在使用网络连接时,可以获取指定应用程序的网络数据包,实现网络数据的安全透明代理,无需获取Android智能设备Root权限,无需侵入Android系统,能够精准识别不同应用程序,更重要的是,使用本发明时,Android智能设备的不同应用程序是通过不同的安全通道与服务器通信的,相互之间的数据完全隔离,保证了企业内部网络的安全性。

[0068] 实施例2

[0069] 如图4所示,本实施例提供一种基于Android系统的免Root无侵入的安全通信系统,该系统通过实施例1提供的安全通信方法在Android智能设备与服务器之间实现数据安全交互,通信系统包括:

[0070] 动态抓包模块:植入于Android智能设备,用于供Android智能设备中的应用程序进行加载;

[0071] 安全客户端模块:植入于Android智能设备,用于为所述动态抓包模块提供安全策略;

[0072] 所述安全客户端模块内包含有安全应用代理模块,所述动态抓包模块自动调用所述安全应用代理模块,所述安全应用代理模块用于为应用程序和服务端的数据交互提供安全通道。

[0073] 具体地,动态抓包模块包括:

[0074] 安全策略管理模块:用于从所述安全客户端模块下载安全策略并解析;

[0075] 应用程序识别模块:用于根据解析后的安全策略判别当前应用程序是否安全合法;

[0076] 网络框架动态加载模块:用于加载到Android智能设备的应用程序网路框架中。

[0077] 具体地,安全客户端模块包括安全策略下发模块,安全策略下发模块用于为动态抓包模块提供安全策略。

[0078] 作为优选，本实施例的安全客户端模块还包括用户身份鉴别模块，用户身份鉴别模块用于鉴别服务器是否安全合法。

[0079] 实施本实施例时，在Android智能设备的应用程序初始化时，加载动态抓包模块，动态抓包模块加载成功后，会通过Android系统AOP框架提供的类代理及反射功能，通过动态抓包模块内的类加载器，将动态抓包模块内的网络框架动态加载模块加载到当前应用程序中，当应用程序调用网络相关接口时，将会自动调用到网络框架动态加载模块，网络框架动态模块在被调用时，通过安全应用代理模块将网络数据转发到服务器，应用程序识别模块在运行中会对当前应用程序进行智能识别，判断当前应用程序是否合法，由于每个应用程序均单独加载了动态网络抓包模块，能够智能识别当前应用程序是否合法，并且通过不同的安全通道与服务器通信，不同应用程序之间的数据完全隔离，保证了企业内部网络的安全性。

[0080] 以上仅是本发明的优选实施方式，应当指出的是，上述优选实施方式不应视为对本发明的限制，本发明的保护范围应当以权利要求所限定的范围为准。对于本技术领域的普通技术人员来说，在不脱离本发明的精神和范围内，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

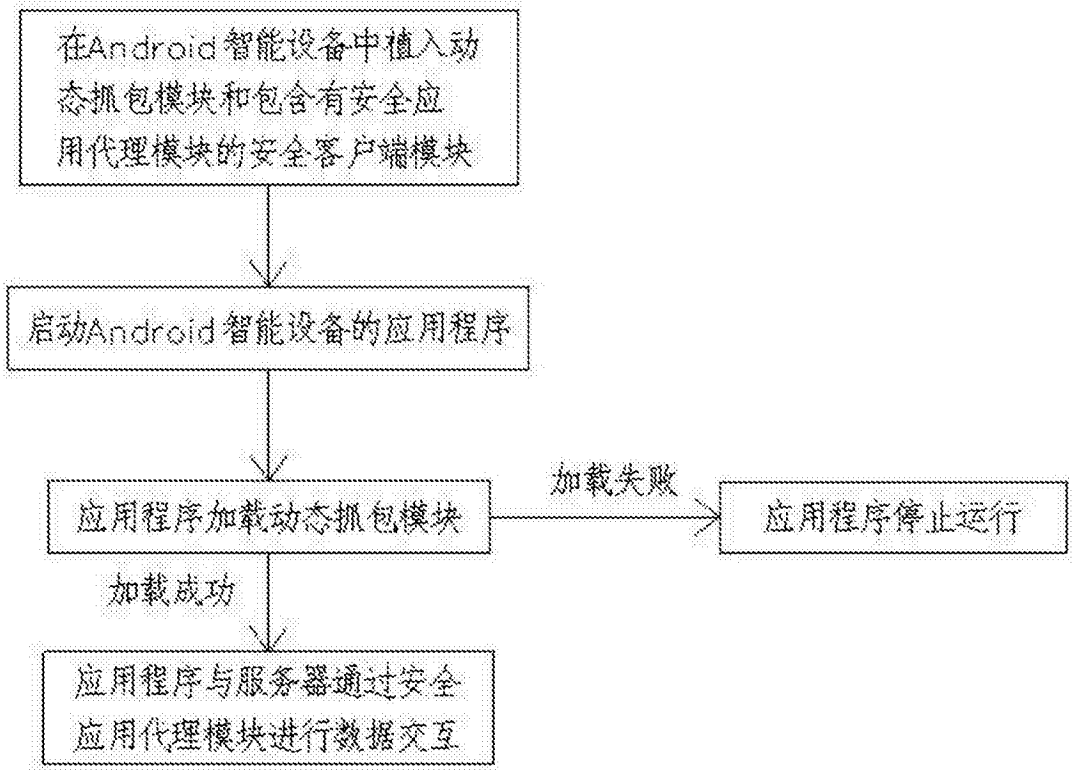

在Android智能设备中植入动态抓包模块和包含有安全应用代理模块的安全客户端模块
启动Android智能设备的应用程序
应用程序加载动态抓包模块
加载失败
应用程序停止运行
加载成功
应用程序与服务器通过安全应用代理模块进行数据交互

图1

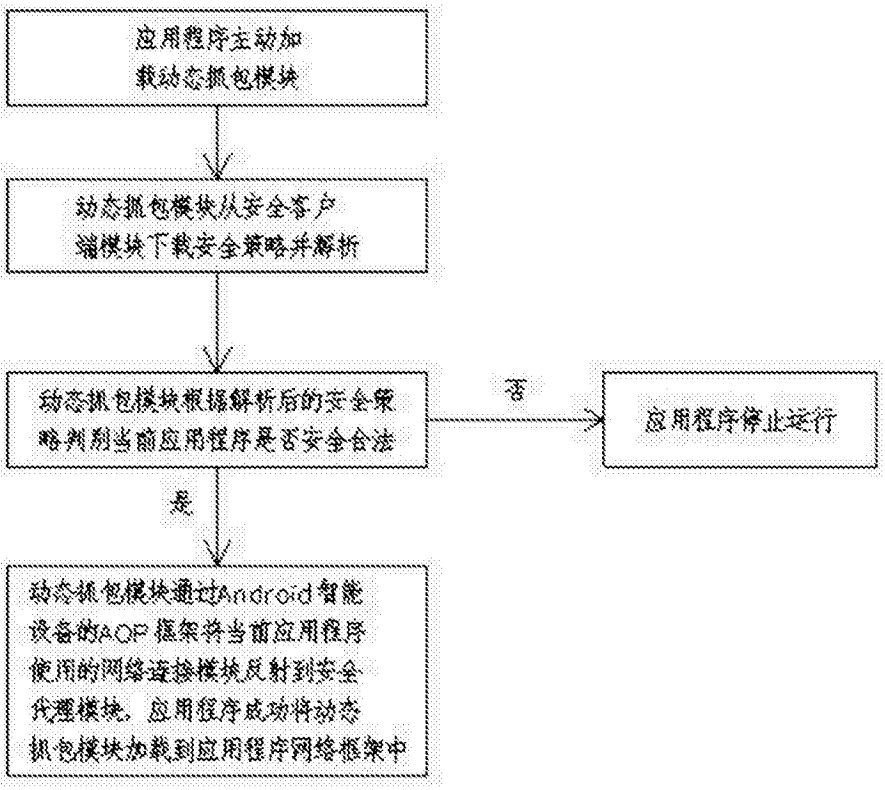

应用程序主动加载动态抓包模块
动态抓包模块从安全客户端模块下载安全策略并解析
动态抓包模块根据解析后的安全策略判别当前应用程序是否安全合法
否
应用程序停止运行
是
动态抓包模块通过Android智能设备的AOP框架将当前应用程序使用的网络连接模块反射到安全代理模块，应用程序成功将动态抓包模块加载到应用程序网络框架中

图2

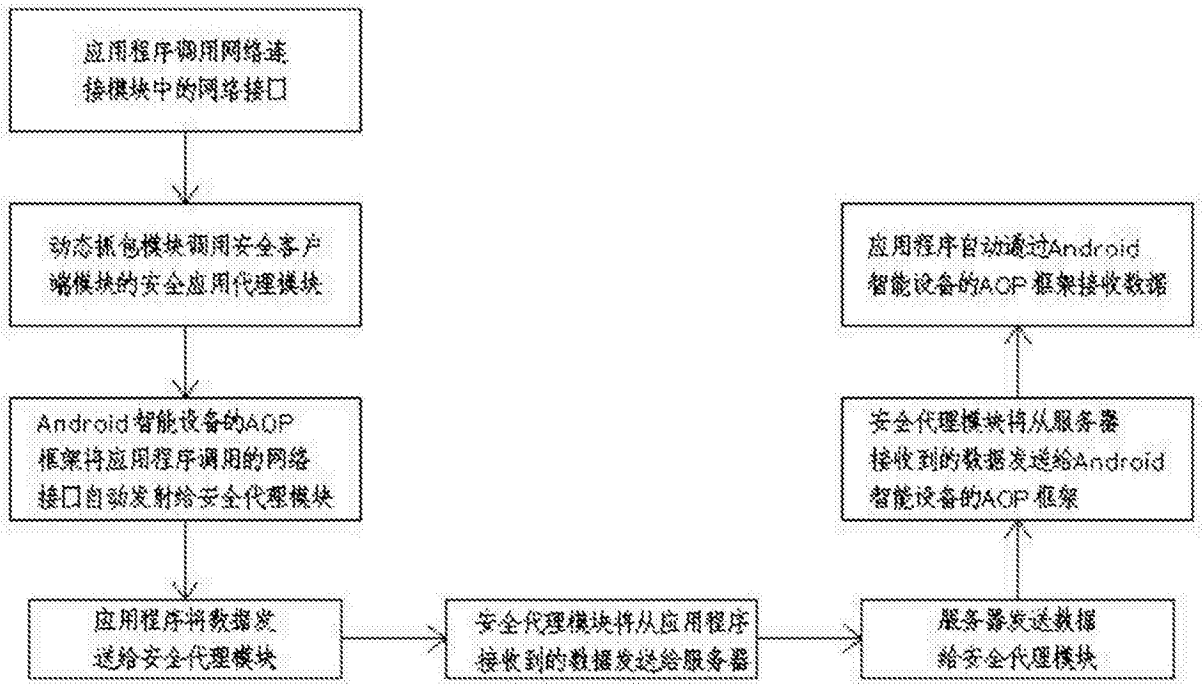

应用程序调用网络连接模块中的网络接口
动态抓包模块调用安全客户端模块的安全应用代理模块
Android智能设备的AOP框架将应用程序调用的网络接口自动发射给安全代理模块
应用程序将数据发送给安全代理模块
安全代理模块将从应用程序接收到的数据发送给服务器
服务器发送数据给安全代理模块
安全代理模块将从服务器接收到的数据发送给Android智能设备的AOP框架
应用程序自动通过Android智能设备的AOP框架接收数据

图3

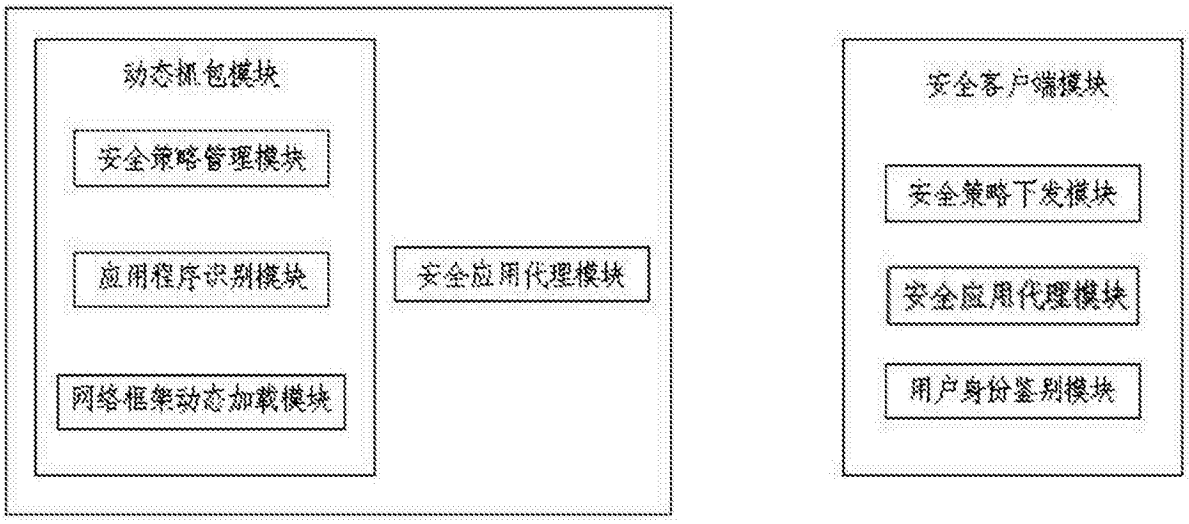

动态抓包模块
安全策略管理模块
应用程序识别模块
网络框架动态加载模块
安全应用代理模块
安全客户端模块
安全策略下发模块
安全应用代理模块
用户身份鉴别模块

图4