(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 104683996 A
(43)申请公布日 2015.06.03

(21)申请号 201310631217.8

(22)申请日 2013.11.29

(71)申请人 中国移动通信集团公司
地址 100032 北京市西城区金融大街29号

(72)发明人 彭华熹

(74)专利代理机构 北京鑫媛睿博知识产权代理有限公司 11297
代理人 龚家骅

(51)Int.Cl.
H04W 24/00(2009.01)

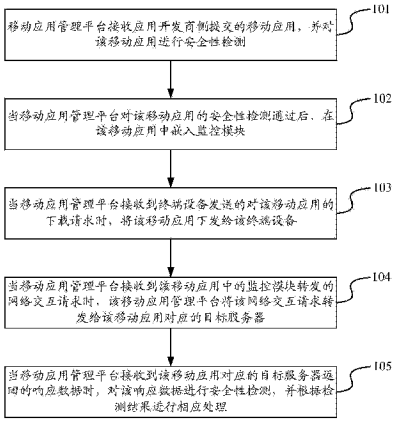
权利要求书3页 说明书7页 附图5页

(54)发明名称

一种移动应用安全管控方法和设备

(57)摘要

本发明公开了一种移动应用安全管控方法和设备，该方法包括：在安全性检测通过后的移动应用中嵌入监控代码，该监控代码用于监控并拦截该移动应用的所有网络操作；在该移动应用下发到终端设备后，当该移动应用发送网络交互请求时，该监控代码拦截该网络交互请求，并将该网络交互请求复制并转发给移动应用管理平台；移动应用管理平台接收到网络交互请求后，将该网络交互请求转发给该移动应用对应的目标服务器，并当接收到该目标服务器返回的响应数据时，对该响应数据进行安全性检测，并根据检测结果进行相应处理，实现了对发布后的移动应用进行安全管控。在本发明中，实现了对发布后的移动应用进行安全管控。



CN 104683996 A

1. 一种移动应用安全管控方法，其特征在于，包括：

当移动应用管理平台接收到应用开发商侧提交的移动应用，且对所述移动应用的安全性检测通过后，在所述移动应用中嵌入监控模块，该监控模块用于监控并拦截该移动应用的所有网络操作；

当所述移动应用管理平台接收到终端设备发送的对所述移动应用的下载请求时，将所述移动应用下发给所述终端设备；

当所述移动应用管理平台接收到所述移动应用中的监控模块转发的网络交互请求时，将该网络交互请求转发给所述移动应用对应的目标服务器；其中，所述网络交互请求是所述移动应用中的监控模块在拦截到所述移动应用的网络交互请求时，复制并转发给所述移动应用管理平台；

当所述移动应用管理平台接收到所述移动应用对应的目标服务器返回的响应数据时，对所述响应数据进行安全性检测，并根据检测结果进行相应处理。

2. 如权利要求 1 所述的方法，其特征在于，所述移动应用管理平台在所述移动应用中嵌入监控模块，具体为：

所述移动应用管理平台通过反编译嵌入的方式在所述移动应用中嵌入监控模块。

3. 如权利要求 1 所述的方法，其特征在于，所述移动应用管理平台将该网络交互请求转发给所述移动应用对应的目标服务器之后，还包括：

若所述移动应用管理平台在预设时间内未接收到所述移动应用对应的目标服务器返回的响应数据时，则保存所述网络交互请求。

4. 如权利要求 1 所述的方法，其特征在于，所述移动应用管理平台根据检测结果进行相应处理包括：

当所述检测结果为安全性检测不通过时，所述移动应用管理平台向所述监控模块发送告警消息。

5. 一种移动应用安全管控方法，其特征在于，所述移动应用中嵌入有监控模块，该方法包括：

移动应用中的监控模块拦截所述移动应用的网络交互请求；

所述监控模块将所述网络交互请求复制并转发给移动应用管理平台，以使所述移动应用管理平台将所述网络交互请求转发给所述移动应用对应的目标服务器，并当接收到所述移动应用对应的目标服务器的响应数据时，对该响应数据进行安全性检测。

6. 如权利要求 5 所述的方法，其特征在于，所述移动应用中的监控模块拦截所述移动应用的网络交互请求之后，还包括：

所述监控模块将所述移动应用转发给所述移动应用对应的目标服务器，并缓存接收到的响应数据；

所述监控模块将所述网络交互请求复制并转发给移动应用管理平台之后，还包括：

当所述监控模块在预设时间内接收到所述移动应用管理平台发送的告警消息时，所述监控模块禁止将所述响应数据在所述移动应用所在终端设备的显示界面上显示；其中，所述告警消息是所述移动应用管理平台在安全性检测的检测结果为安全性检测不通过时，向所述监控模块发送的。

7. 如权利要求 6 所述的方法，其特征在于，该方法还包括：

当所述监控模块在预设时间内未接收到所述移动应用管理平台发送的告警消息时，所述监控模块将所述响应数据在所述移动应用所在终端设备的显示界面上显示。

8. 如权利要求 5 所述的方法，其特征在于，所述移动应用中的监控模块拦截所述移动应用的网络交互请求之后，还包括：

所述监控模块缓存所述网络交互请求；

所述监控模块将所述网络交互请求复制并转发给移动应用管理平台之后，还包括：

当所述监控模块在预设时间内接收到所述移动应用管理平台发送的告警消息时，所述监控模块禁止将所述网络交互请求转发给所述移动应用对应的目标服务器；其中，所述告警消息是所述移动应用管理平台在安全性检测的检测结果为安全性检测不通过时，向所述监控模块发送的。

9. 如权利要求 8 所述的方法，其特征在于，该方法还包括：

当所述监控模块在预设时间内未接收到所述移动应用管理平台发送的告警消息时，所述监控模块将所述网络交互请求转发给所述移动应用对应的目标服务器。

10. 一种移动应用管理平台，其特征在于，包括：

嵌入模块，用于当所述移动管理平台接收到应用开发商侧提交的移动应用，且对所述移动应用的安全性检测通过后，在所述移动应用中嵌入监控模块，该监控模块用于监控并拦截该移动应用的所有网络操作；

发布模块，用于在所述移动应用管理平台接收到终端设备发送的对所述移动应用的下载请求时，将所述移动应用下发给所述终端设备；

发送模块，用于当所述移动应用管理平台接收到所述移动应用中的监控模块转发的网络交互请求时，将该网络交互请求转发给所述移动应用对应的目标服务器；

处理模块，用于当所述移动应用管理平台接收到所述移动应用对应的目标服务器返回的响应数据时，对所述响应数据进行安全性检测，并根据检测结果进行相应处理。

11. 如权利要求 10 所述的移动应用管理平台，其特征在于，

所述嵌入模块具体用于，通过反编译嵌入的方式在所述移动应用中嵌入监控模块。

12. 如权利要求 10 所述的移动应用管理平台，其特征在于，还包括：

缓存模块，用于在移动应用管理平台将该网络交互请求转发给所述移动应用对应的目标服务器之后，若所述移动应用管理平台在预设时间内未接收到所述移动应用对应的目标服务器返回的响应数据时，则保存所述网络交互请求。

13. 如权利要求 10 所述的移动应用管理平台，其特征在于，

所述处理模块具体用于，当所述检测结果为安全性检测不通过时，向所述监控模块发送告警消息。

14. 一种移动应用安全管控设备，其特征在于，所述移动应用安全管控设备的移动应用中嵌入有监控模块，其中，所述监控模块包括：

拦截单元，用于拦截所述移动应用的网络交互请求；

第一转发单元，用于将所述网络交互请求复制并转发给移动应用管理平台，以使所述移动应用管理平台将所述网络交互请求转发给所述移动应用对应的目标服务器，并当接收到所述移动应用对应的目标服务器的响应数据时，对该响应数据进行安全性检测。

15. 如权利要求 14 所述的移动应用安全管控设备，其特征在于，所述监控模块还包括：

第二转发单元，用于在所述监控模块拦截所述移动应用的网络交互请求之后，将所述移动应用转发给所述移动应用对应的目标服务器，并缓存接收到的响应数据；

第一处理单元，用于当所述监控模块在预设时间内接收到所述移动应用管理平台发送的告警消息时，禁止将所述响应数据在所述移动应用所在终端设备的显示界面上显示；其中，所述告警消息是所述移动应用管理平台在安全性检测的检测结果为安全性检测不通过时，向所述监控模块发送的。

16. 如权利要求 15 所述的移动应用安全管控设备，其特征在于，

所述第一处理单元还用于，当所述监控模块在预设时间内未接收到所述移动应用管理平台发送的告警消息时，将所述响应数据在所述移动应用所在终端设备的显示界面上显示。

17. 如权利要求 14 所述的移动应用安全管控设备，其特征在于，所述监控模块还包括：

缓存单元，用于在所述拦截单元拦截所述移动应用的网络交互请求之后，缓存所述网络交互请求；

第二处理单元，用于当所述监控模块在预设时间内接收到所述移动应用管理平台发送的告警消息时，禁止将所述网络交互请求转发给所述移动应用对应的目标服务器；其中，所述告警消息是所述移动应用管理平台在安全性检测的检测结果为安全性检测不通过时，向所述监控模块发送的。

18. 如权利要求 17 所述的移动应用安全管控设备，其特征在于，

所述第二处理单元还用于，当所述监控模块在预设时间内未接收到所述移动应用管理平台发送的告警消息时，将所述网络交互请求转发给所述移动应用对应的目标服务器。

一种移动应用安全管控方法和设备

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种移动应用安全管控方法和设备。

背景技术

[0002] 随着移动终端互联网的迅速发展，智能移动终端手机的增多，移动终端上相应的恶意代码威胁也逐渐增多。在目前主流的移动终端恶意代码中，大多数的恶意代码都存在主动的网络连接行为，通过网络连接，它们同远程控制服务器进行连接，可以下载和传播新的恶意代码，也可以接受远程服务器的指令进而触发相应的恶意行为，同时在这种情况下，其频繁的网络连接也造成了大量的无意义的网络流量，对网关设备造成了冲击。

[0003] 移动商城为了保证上线 app（应用程序）的安全，在 app 上线前均会做严格的 app 安全性检测，即使用相关技术手段，检测 app 中是否包含恶意代码，是否会动态下载恶意代码，是否会从服务器获取黄色、非法等内容的图片，文字等。只有通过安全性检测的 app 才能上线，供用户下载。

[0004] 但是，虽然通过上线前的 app 安全性检测，可以在一定程度上解决恶意软件泛滥的问题。但 app 上线后，用户在商城上下载 app 到自己的手机上使用，此时 app 基本上脱离了移动应用商城的安全管控，可以通过联网下载安装包自我更新，也可以通过联网从服务器获取黄色等非法内容，而不受应用商城的监管。目前对恶意软件的安全检测方法无法解决该问题。

发明内容

[0005] 本发明提供了一种移动应用安全管控方法和设备，用以实现对发布后的移动应用进行安全管控。

[0006] 为了达到以上目的，本发明实施例提供了一种移动应用安全管控方法，包括：

[0007] 当移动应用管理平台接收到应用开发商侧提交的移动应用，且对所述移动应用的安全性检测通过后，在所述移动应用中嵌入监控模块，该监控模块用于监控并拦截该移动应用的所有网络操作；

[0008] 当所述移动应用管理平台接收到终端设备发送的对所述移动应用的下载请求时，将所述移动应用下发给所述终端设备；

[0009] 当所述移动应用管理平台接收到所述移动应用中的监控模块转发的网络交互请求时，将该网络交互请求转发给所述移动应用对应的目标服务器；其中，所述网络交互请求是所述移动应用中的监控模块在拦截到所述移动应用的网络交互请求时，复制并转发给所述移动应用管理平台；

[0010] 当所述移动应用管理平台接收到所述移动应用对应的目标服务器返回的响应数据时，对所述响应数据进行安全性检测，并根据检测结果进行相应处理。

[0011] 本发明实施例还提供了一种移动应用安全管控方法，其特征在于，该方法包括：

[0012] 移动应用中的监控模块拦截所述移动应用的网络交互请求；

[0013] 所述监控模块将所述网络交互请求复制并转发给移动应用管理平台，以使所述移动应用管理平台将所述网络交互请求转发给所述移动应用对应的目标服务器，并当接收到所述移动应用对应的目标服务器的响应数据时，对该响应数据进行安全性检测。

[0014] 本发明实施例还提供了一种移动应用管理平台，包括：

[0015] 嵌入模块，用于当所述移动管理平台接收到应用开发商侧提交的移动应用，且对所述移动应用的安全性检测通过后，在所述移动应用中嵌入监控模块，该监控模块用于监控并拦截该移动应用的所有网络操作；

[0016] 发布模块，用于在所述移动应用管理平台接收到终端设备发送的对所述移动应用的下载请求时，将所述移动应用下发给所述终端设备；

[0017] 发送模块，用于当所述移动应用管理平台接收到所述移动应用中的监控模块转发的网络交互请求时，将该网络交互请求转发给所述移动应用对应的目标服务器；

[0018] 处理模块，用于当所述移动应用管理平台接收到所述移动应用对应的目标服务器返回的响应数据时，对所述响应数据进行安全性检测，并根据检测结果进行相应处理。

[0019] 本发明实施例还提供了一种移动应用安全管控设备，所述移动应用安全管控设备的移动应用中嵌入有监控模块，其中，所述监控模块包括：

[0020] 拦截单元，用于拦截所述移动应用的网络交互请求；

[0021] 第一转发单元，用于将所述网络交互请求复制并转发给移动应用管理平台，以使所述移动应用管理平台将所述网络交互请求转发给所述移动应用对应的目标服务器，并当接收到所述移动应用对应的目标服务器的响应数据时，对该响应数据进行安全性检测。

[0022] 本发明上述实施例中，通过在安全性检测通过后的移动应用中嵌入监控代码，该监控代码用于监控并拦截该移动应用的所有网络操作；在该移动应用下发到终端设备后，当该移动应用发送网络交互请求时，该监控代码拦截该网络交互请求，并将该网络交互请求复制并转发给移动应用管理平台；移动应用管理平台接收到网络交互请求后，将该网络交互请求转发给该移动应用对应的目标服务器，并当接收到该目标服务器返回的响应数据时，对该响应数据进行安全性检测，并根据检测结果进行相应处理，实现了对发布后的移动应用进行安全管控。

附图说明

[0023] 图 1 为本发明实施例提供的一种移动应用安全管控方法的流程示意图；

[0024] 图 2 为本发明实施例提供的移动应用安全管控技术方案在监控模块侧的处理流程；

[0025] 图 3 为本发明实施例提供的一种具体应用场景的系统架构图；

[0026] 图 4 为本发明实施例提供的一种移动应用管理平台的结构示意图；

[0027] 图 5 为本发明实施例提供的一种移动应用安全管控设备的结构示意图；

[0028] 图 6A 为本发明实施例提供的一种移动应用安全管控设备的结构示意图；

[0029] 图 6B 为本发明实施例提供的一种移动应用安全管控设备的结构示意图。

具体实施方式

[0030] 针对上述现有技术中的问题，本发明实施例提供了一种移动应用安全管控的技术

方案。在该技术方案中，通过在安全性检测通过后的移动应用中嵌入监控代码，该监控代码用于监控并拦截该移动应用的所有网络操作；在该移动应用下发到终端设备后，当该移动应用发送网络交互请求时，该监控代码拦截该网络交互请求，并将该网络交互请求复制并转发给移动应用管理平台；移动应用管理平台接收到网络交互请求后，将该网络交互请求转发给该移动应用对应的目标服务器，并当接收到该目标服务器返回的响应数据时，对该响应数据进行安全性检测，并根据检测结果进行相应处理，实现了对发布后的移动应用进行安全管控。

[0031] 下面将结合本申请中的附图，对本申请中的技术方案进行清楚、完整的描述，显然，所描述的实施例是本申请的一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0032] 如图 1 所示，为本发明实施例提供的一种移动应用安全管控方法的流程示意图，可以包括：

[0033] 步骤 101、移动应用管理平台接收应用开发商侧提交的移动应用，并对该移动应用进行安全性检测。

[0034] 具体的，移动应用管理平台接收到应用开发商侧提交的移动应用后，可以根据现有处理方式对其进行安全性检测。

[0035] 步骤 102、当移动应用管理平台对该移动应用的安全性检测通过后，在该移动应用中嵌入监控模块。

[0036] 具体的，在本发明实施例中，为了实现对发布后的移动应用的安全管控，对于安全性检测通过的移动应用，移动应用管理平台可以在该移动应用中嵌入监控模块，该监控模块用于监控并拦截该移动应用的所有网络操作。

[0037] 其中，移动应用管理平台可以通过反编译嵌入的方式在移动应用中嵌入监控模块。

[0038] 步骤 103、当移动应用管理平台接收到终端设备发送的对该移动应用的下载请求时，将该移动应用下发给该终端设备。

[0039] 具体的，终端设备可以通过向移动应用管理平台发送下载请求，请求下载相应的移动应用。

[0040] 步骤 104、当移动应用管理平台接收到该移动应用中的监控模块转发的网络交互请求时，该移动应用管理平台将该网络交互请求转发给该移动应用对应的目标服务器。

[0041] 具体的，终端设备下载到移动应用后，当该终端设备运行该移动应用时，该移动应用会向对应的目标服务器发送网络交互请求。

[0042] 在本发明实施例中，移动应用中的监控模块可以拦截该移动应用发送的网络交互请求，并将该网络交互请求复制并转发给移动应用管理平台，由移动应用管理平台将该网络交互请求转发给对应的目标服务器。

[0043] 步骤 105、当移动应用管理平台接收到该移动应用对应的目标服务器返回的响应数据时，对该响应数据进行安全性检测，并根据检测结果进行相应处理。

[0044] 具体的，在本发明实施例中，移动应用管理平台将网络交互请求转发给对应的目标服务器后，若接收到该目标服务器返回的响应数据，则可以对该响应数据进行安全性检

测，如检测该响应数据中是否包括恶意代码、黄色图片等非法信息等，当该响应数据中不包括恶意代码、黄色图片等非法信息时，确定检测结果为安全性检测通过；当该响应数据中包括恶意代码、黄色图片等非法信息时，确定检测结果为安全性检测不通过。

[0045] 若移动应用管理平台在预设时间内（可以根据具体场景设置）未接收到目标服务器返回的响应数据，则移动应用管理平台可以保存该网络交互请求，并在后续流程中，在特定情况下（如接收到对该移动应用的投诉、举报消息时）再次将该网络交互请求转发给目标服务器，并确定是否能接收到响应数据，并在接收到响应数据时，对响应数据进行安全性检测。

[0046] 其中，在本发明实施例中，当移动应用管理平台接收到目标服务器返回的响应数据，且对响应数据的安全性检测的检测结果为安全性检测不通过时，移动应用管理平台可以向监控模块发送告警消息。

[0047] 本发明实施例提供的移动应用安全管控技术方案在监控模块侧的处理流程可以如图 2 所示，可以包括以下步骤：

[0048] 步骤 201、移动应用中的监控模块拦截该移动应用的网络交互请求。

[0049] 步骤 202、监控模块将该网络交互请求复制并转发给移动应用管理平台，以使该移动应用管理平台将该网络交互请求转发给该移动应用对应的目标服务器，并当接收到该移动应用对应的目标服务器的响应数据时，对该响应数据进行安全性检测。

[0050] 其中，在本发明实施例中，当监控模块拦截了移动应用的网络交互请求后，一方面可以如以上描述的将该网络交互请求复制并转发给移动应用管理平台；另一方面，该监控模块还可以进行如方式一或方式二的处理：

[0051] 方式一、监控模块将该网络交互请求转发给该移动应用对应的目标服务器，并当接收到目标服务器返回的响应数据时，缓存该响应数据，而并不直接将该响应数据在该移动应用所在终端设备的显示界面上显示；当监控模块在将网络交互请求转发给移动应用管理平台之后的预设时间内，接收到移动应用管理平台的告警消息时，该监控模块禁止将该响应数据在该移动应用所在终端设备的显示界面上显示（即不将该响应数据在该移动应用所在终端设备的显示界面上显示）；当监控模块在将网络交互请求转发给移动应用管理平台之后的预设时间内，未接收到移动应用管理平台的告警消息时，该监控模块将该响应数据在该移动应用所在终端设备的显示界面上显示。

[0052] 方式二、监控模块缓存该网络交互请求，当监控模块在将网络交互请求转发给移动应用管理平台之后的预设时间内，接收到移动应用管理平台的告警消息时，该监控模块禁止将该网络交互请求转发给对应的目标服务器（即不将该网络交互请求转发给对应的目标服务器）；当监控模块在将网络交互请求转发给移动应用管理平台之后的预设时间内，未接收到移动应用管理平台的告警消息时，该监控模块将该网络交互请求转发给对应的目标服务器，并当接收到响应数据时，将该响应数据在该移动应用所在的终端设备的显示界面上显示。

[0053] 为了更好地理解本发明实施例提供的技术方案，下面结合具体的应用场景对本发明实施例提供的技术方案进行更加详细地描述。

[0054] 参见图 3，为该实施例提供的具体应用场景的系统架构图，基于该系统架构的移动应用安全管控方法的流程可以包括：

[0055] 1、开发者将 app 提交给移动应用管理平台，移动应用管理平台对 app 的安全性进行检测；

[0056] 2、确定 app 的安全性后，移动管理平台将监控模块通过反编译嵌入等手段嵌入 app，该监控模块的主要作用是可监管并拦截该 app 的所有网络操作；

[0057] 3、App 发布后，用户从应用管理平台下载 app 并运行，app 自有模块（即现有 app 原来就有的模块）进行网络交互操作时，网络交互请求均被监控模块监控拦截；

[0058] 4、监控模块一方面将该网络交互请求直接透明发送出去，即发送给目标服务器；另一方面，将网络交互请求复制并转发给移动应用管理平台；

[0059] 5、移动应用管理平台接收到网络交互请求后，将网络交互请求转发给 app 对应的目标服务器，以获取响应数据；

[0060] 6、若移动应用管理平台可获得响应数据，则分析其内容，主要包括（二进制代码、图片、文字等信息），通过相关安全性工具检测是否存在恶意代码，黄色图片等非法信息等。

[0061] 7、若移动应用管理平台无法获得响应数据，则将网络交互请求保存下来，以供事后追查。

[0062] 8、若移动应用管理平台检测到响应数据不安全（即安全性检测的检测结果为安全性检测不通过），则向监控模块发送告警消息，以供后续操作参考。

[0063] 其中，在该实施例中，步骤 4 中，监控模块将网络交互请求转发给目标服务器后，当接收到目标服务器返回的响应消息时，先缓存该响应消息，并当在将网络交互请求转发给移动应用管理平台后的预设时间内未接收到告警消息时，将该响应消息在移动应用所在的终端设备的显示界面显示；否则，不将该响应消息在移动应用所在终端设备的显示界面显示。

[0064] 通过以上描述可以看出，在本发明实施例提供的技术方案中，通过在安全性检测通过后的移动应用中嵌入监控代码，该监控代码用于监控并拦截该移动应用的所有网络操作；在该移动应用下发到终端设备后，当该移动应用发送网络交互请求时，该监控代码拦截该网络交互请求，并将该网络交互请求复制并转发给移动应用管理平台；移动应用管理平台接收到网络交互请求后，将该网络交互请求转发给该移动应用对应的目标服务器，并当接收到该目标服务器返回的响应数据时，对该响应数据进行安全性检测，并根据检测结果进行相应处理，在无需用户在终端设备上安装监控软件的情况下，实现了对发布后的移动应用进行安全管控。

[0065] 基于相同的技术构思，本发明实施例还提供了一种移动应用管理平台，可以应用于上述方法实施例。

[0066] 如图 4 所示，为本发明实施例提供的一种移动应用管理平台的结构示意图，可以包括：

[0067] 嵌入模块 41，用于当所述移动管理平台接收到应用开发商侧提交的移动应用，且对所述移动应用的安全性检测通过后，在所述移动应用中嵌入监控模块，该监控模块用于监控并拦截该移动应用的所有网络操作；

[0068] 发布模块 42，用于在所述移动应用管理平台接收到终端设备发送的对所述移动应用的下载请求时，将所述移动应用下发给所述终端设备；

[0069] 发送模块 43，用于当所述移动应用管理平台接收到所述移动应用中的监控模块转

发的网络交互请求时，将该网络交互请求转发给所述移动应用对应的目标服务器；

[0070] 处理模块 44，用于当所述移动应用管理平台接收到所述移动应用对应的目标服务器返回的响应数据时，对所述响应数据进行安全性检测，并根据检测结果进行相应处理。

[0071] 其中，所述嵌入模块 41 具体用于，通过反编译嵌入的方式在所述移动应用中嵌入监控模块。

[0072] 其中，本发明实施例提供的移动应用管理平台还包括：

[0073] 缓存模块 45，用于在移动应用管理平台将该网络交互请求转发给所述移动应用对应的目标服务器之后，若所述移动应用管理平台在预设时间内未接收到所述移动应用对应的目标服务器返回的响应数据时，则保存所述网络交互请求。

[0074] 其中，所述处理模块 44 具体用于，当所述检测结果为安全性检测不通过时，向所述监控模块发送告警消息。

[0075] 基于相同的技术构思，本发明实施例还提供了一种移动应用安全管控设备，可以应用于上述方法实施例。

[0076] 如图 5 所示，为本发明实施例提供的一种移动应用安全管控设备的结构示意图，该移动应用安全管控设备的移动应用中嵌入有监控模块，该监控模块可以包括：

[0077] 拦截单元 51，用于拦截所述移动应用的网络交互请求；

[0078] 第一转发单元 52，用于将所述网络交互请求复制并转发给移动应用管理平台，以使所述移动应用管理平台将所述网络交互请求转发给所述移动应用对应的目标服务器，并当接收到所述移动应用对应的目标服务器的响应数据时，对该响应数据进行安全性检测。

[0079] 其中，参见图 6A 在本发明的一实施例中，该监控模块还可以包括：

[0080] 第二转发单元 53，用于在所述监控模块拦截所述移动应用的网络交互请求之后，将所述移动应用转发给所述移动应用对应的目标服务器，并缓存接收到的响应数据；

[0081] 第一处理单元 54，用于当所述监控模块在预设时间内接收到所述移动应用管理平台发送的告警消息时，禁止将所述响应数据在所述移动应用所在终端设备的显示界面上显示；其中，所述告警消息是所述移动应用管理平台在安全性检测的检测结果为安全性检测不通过时，向所述监控模块发送的。

[0082] 其中，所述第一处理单元 54 还用于，当所述监控模块在预设时间内未接收到所述移动应用管理平台发送的告警消息时，将所述响应数据在所述移动应用所在终端设备的显示界面上显示。

[0083] 其中，参见图 6B，在本发明另一实施例中，该监控模块还可以包括：

[0084] 缓存单元 55，用于在所述拦截单元拦截所述移动应用的网络交互请求之后，缓存所述网络交互请求；

[0085] 第二处理单元 56，用于当所述监控模块在预设时间内接收到所述移动应用管理平台发送的告警消息时，禁止将所述网络交互请求转发给所述移动应用对应的目标服务器；其中，所述告警消息是所述移动应用管理平台在安全性检测的检测结果为安全性检测不通过时，向所述监控模块发送的。

[0086] 其中，所述第二处理单元 56 还用于，当所述监控模块在预设时间内未接收到所述移动应用管理平台发送的告警消息时，将所述网络交互请求转发给所述移动应用对应的目标服务器。

[0087] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台终端设备(可以是手机，个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述的方法。

[0088] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视本发明的保护范围。

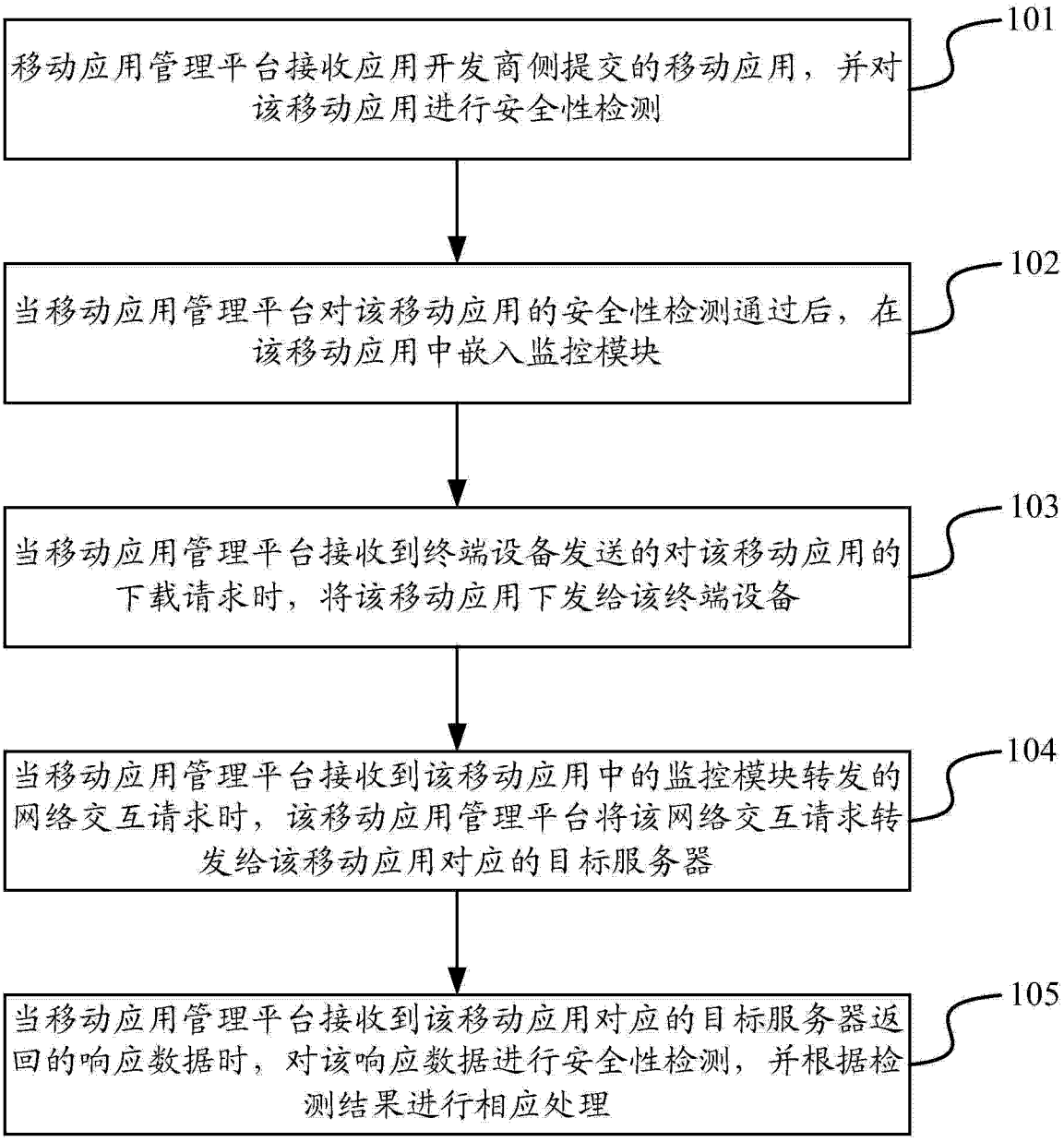

移动应用管理平台接收应用开发商侧提交的移动应用，并对该移动应用进行安全性检测
101
当移动应用管理平台对该移动应用的安全性检测通过后，在该移动应用中嵌入监控模块
102
当移动应用管理平台接收到终端设备发送的对该移动应用的下载请求时，将该移动应用下发给该终端设备
103
当移动应用管理平台接收到该移动应用中的监控模块转发的网络交互请求时，该移动应用管理平台将该网络交互请求转发给该移动应用对应的目标服务器
104
当移动应用管理平台接收到该移动应用对应的目标服务器返回的响应数据时，对该响应数据进行安全性检测，并根据检测结果进行相应处理
105

图 1

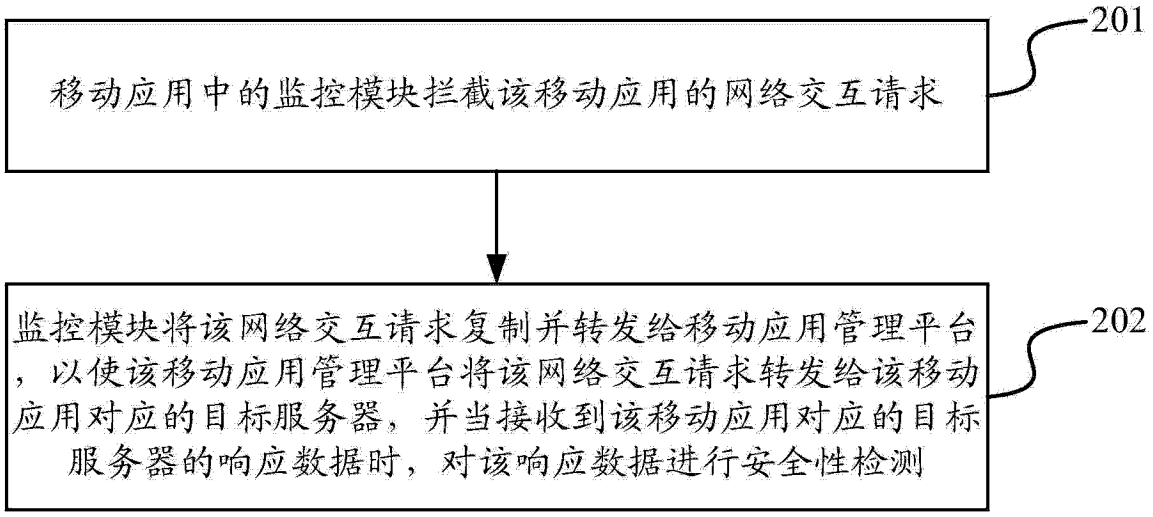

移动应用中的监控模块拦截该移动应用的网络交互请求
201
监控模块将该网络交互请求复制并转发给移动应用管理平台，以使该移动应用管理平台将该网络交互请求转发给该移动应用对应的目标服务器，并当接收到该移动应用对应的目标服务器的响应数据时，对该响应数据进行安全性检测
202

图 2

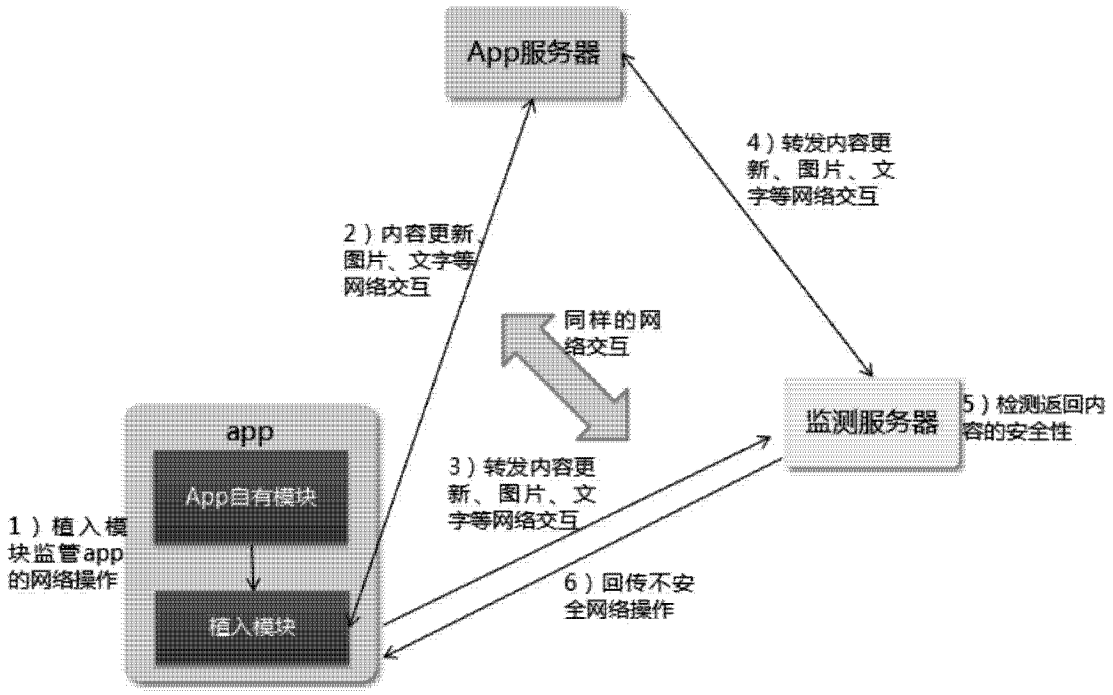

App服务器
4）转发内容更新、图片、文字等网络交互
2）内容更新、图片、文字等网络交互
同样的网络交互
监测服务器
5）检测返回内容的安全性
app
App自有模块
植入模块
1）植入模块监管app的网络操作
3）转发内容更新、图片、文字等网络交互
6）回传不安全网络操作

图 3

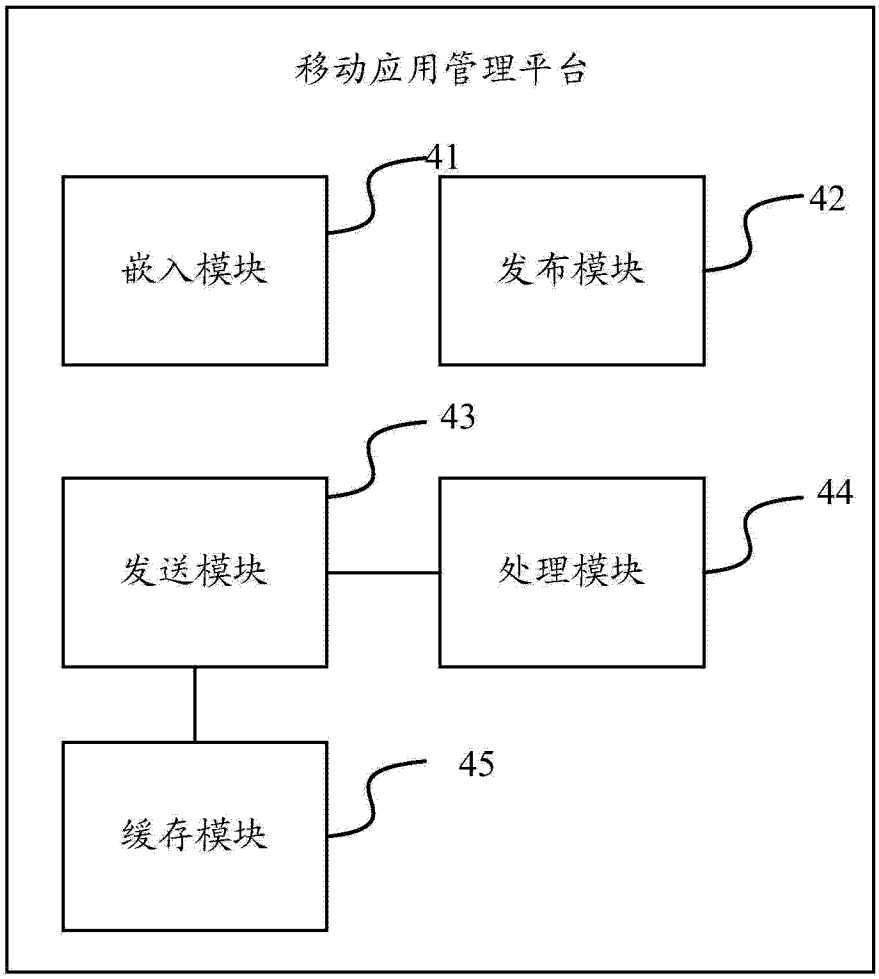

移动应用管理平台
41
嵌入模块
42
发布模块
43
发送模块
44
处理模块
45
缓存模块

图 4

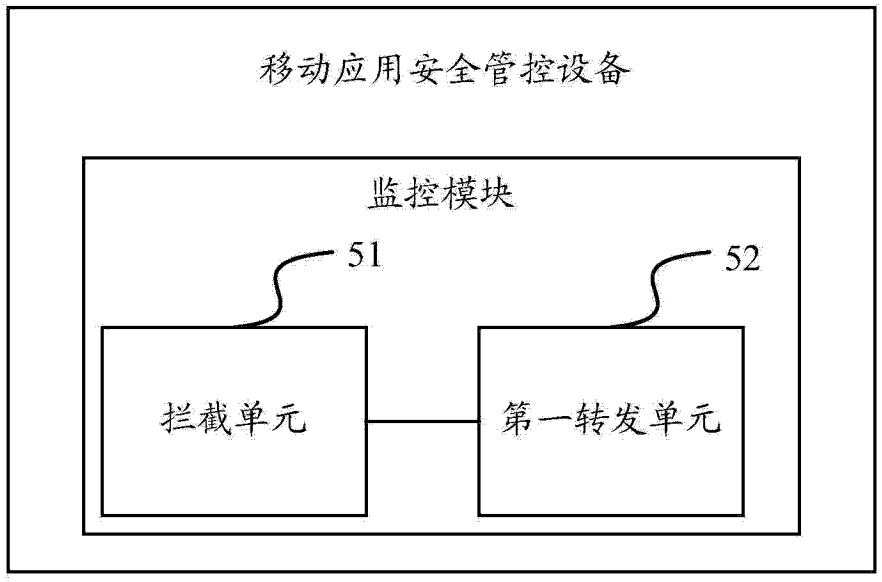

移动应用安全管控设备
监控模块
51
拦截单元
52
第一转发单元

图 5

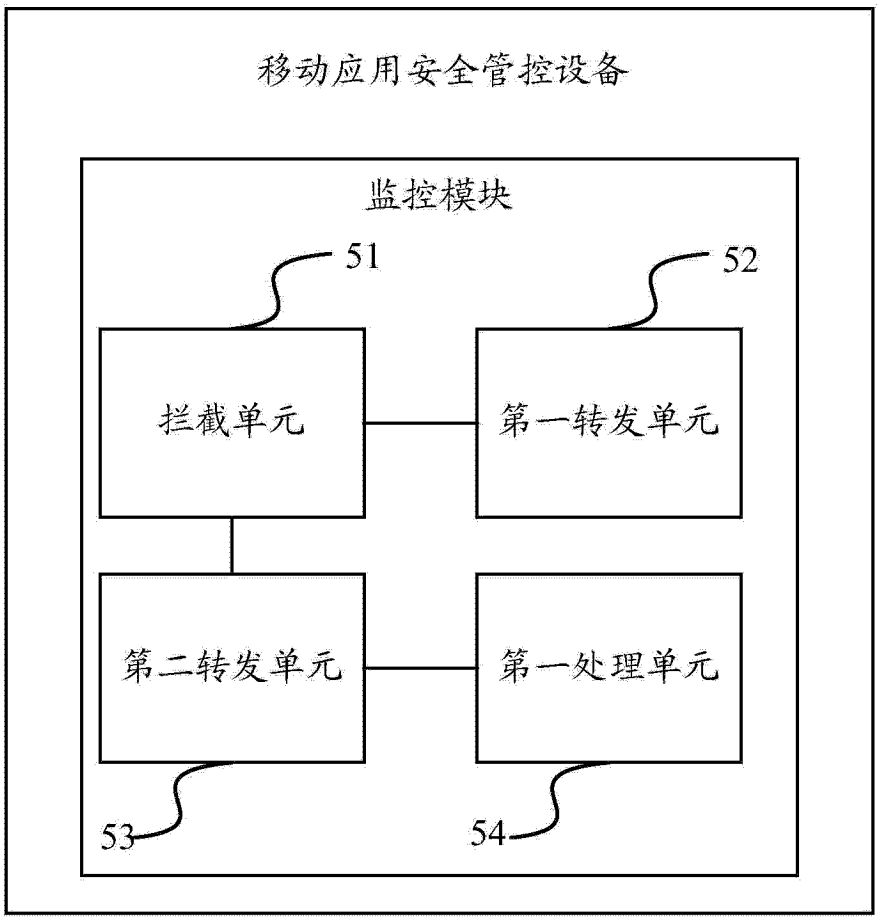


图 6A

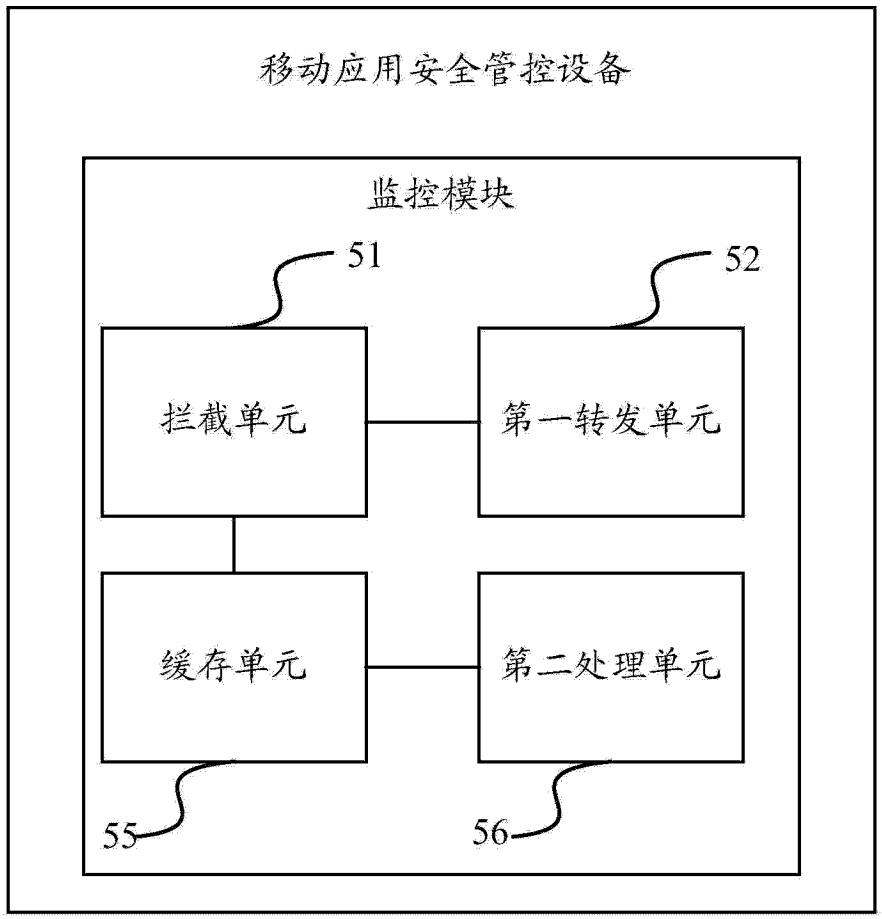


图 6B