



(12) 发明专利申请

(10) 申请公布号 CN 105827565 A

(43) 申请公布日 2016. 08. 03

(21) 申请号 201510003988. 1

(22) 申请日 2015. 01. 05

(71) 申请人 中国移动通信集团江苏有限公司  
地址 210029 江苏省南京市虎踞路 59 号

(72) 发明人 冷志敏 金波 冯会彬 郑兴淦

(74) 专利代理机构 北京同达信恒知识产权代理  
有限公司 11291  
代理人 郭润湘

(51) Int. Cl.

H04L 29/06(2006. 01)

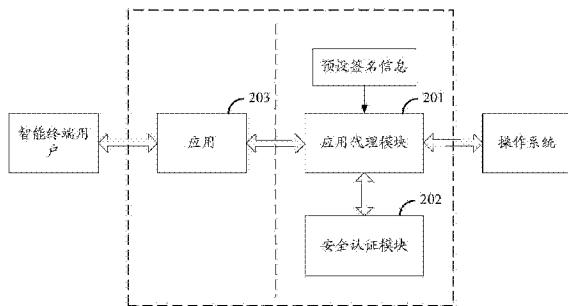
权利要求书2页 说明书7页 附图3页

(54) 发明名称

一种应用的安全认证系统、方法、及终端

(57) 摘要

本发明实施例提供了一种应用的安全认证系统、方法及终端，包括：应用代理模块，安全认证模块；应用代理模块，用于接收应用发送的系统调用请求，并将系统调用请求中携带的用于进行安全认证的信息发送给安全认证模块；以及基于应用通过安全认证的认证结果，为该应用调用系统调用请求所请求的系统功能，并向该应用反馈系统调用的结果；安全认证模块，用于基于接收的用于进行安全认证的信息，按照与该应用预先约定的安全认证方式，对该应用进行安全认证；并将得到安全认证的结果反馈应用代理模块。解决了现有技术中对应用进行安全认证时需要频繁修改固件导致系统稳定性差的问题。本发明涉及通信技术领域。



1. 一种应用的安全认证系统,其特征在于,包括:应用代理模块和安全认证模块;

所述应用代理模块,用于接收应用发送的系统调用请求,并将所述系统调用请求中携带的用于进行安全认证的信息发送给所述安全认证模块;以及基于所述应用通过安全认证的认证结果,为所述应用调用所述系统调用请求所请求的系统功能,并向所述应用反馈系统调用的结果;

所述安全认证模块,用于基于接收的所述用于进行安全认证的信息,按照与所述应用预先约定的安全认证方式,对所述应用进行安全认证;并将得到安全认证的结果反馈所述应用代理模块。

2. 如权利要求 1 所述的系统,其特征在于,所述应用代理模块,具体用于通过封装的系统调用接口接收应用发送的系统调用请求,

其中,所述封装的系统调用接口为所述应用代理模块预先将操作系统提供的系统调用接口进行封装,得到与所述系统调用接口对应的封装的系统调用接口,所述封装的系统调用接口用于提供给应用进行系统调用。

3. 如权利要求 1 或 2 所述的系统,其特征在于,所述应用代理模块,还用于在所在终端启动时,将预设签名信息提供给操作系统,并通过操作系统对所述应用代理模块的安全性验证;

其中,所述预设签名信息为所述应用代理模块预先使用操作系统提供的密钥对预设信息进行签名生成,并固化在操作系统中的。

4. 如权利要求 1 或 2 所述的系统,其特征在于,所述应用代理模块,还用于在接收应用发送的系统调用请求之后,并在将所述系统调用请求中携带的用于进行安全认证的信息发送给所述安全认证模块之前,从预先记录的合法应用列表中查找所述应用对应的应用标识,并从预先记录的合法系统调用列表中查找所述系统调用请求对应的系统调用;以及基于所述应用为合法应用且所述系统调用为合法系统调用的查找结果,触发安全认证模块对所述应用进行安全认证。

5. 一种应用的安全认证方法,其特征在于,包括:

终端中的应用代理模块接收应用发送的系统调用请求;

将所述系统调用请求中携带的用于进行安全认证的信息发送给所述终端中的安全认证模块;

所述安全认证模块基于接收的所述用于进行安全认证的信息,按照与所述应用预先约定的安全认证方式,对所述应用进行安全认证,并将得到安全认证的结果反馈所述应用代理模块;

所述应用代理模块基于所述应用通过安全认证的认证结果,为所述应用调用所述系统调用请求所请求的系统功能,并向所述应用反馈系统调用的结果。

6. 如权利要求 5 所述的方法,其特征在于,应用代理模块接收应用发送的系统调用请求,具体包括:

所述应用代理模块通过封装的系统调用接口接收应用发送的系统调用请求,

其中,所述封装的系统调用接口为所述应用代理模块预先将操作系统提供的系统调用接口进行封装,得到与所述系统调用接口对应的封装的系统调用接口,所述封装的系统调用接口用于提供给应用进行系统调用。

7. 如权利要求 5 或 6 所述的方法, 其特征在于, 还包括 :

在所在终端启动时, 所述应用代理模块将预设签名信息提供给操作系统, 并通过操作系统对所述应用代理模块的安全性验证;

其中, 所述预设签名信息为所述应用代理模块预先使用操作系统提供的密钥对预设信息进行签名生成, 并固化在操作系统中的。

8. 如权利要求 5 或 6 所述的方法, 其特征在于, 所述应用代理模块在接收应用发送的系统调用请求之后, 并在将所述系统调用请求中携带的用于进行安全认证的信息发送给所述安全认证模块之前, 还包括 :

从预先记录的合法应用列表中查找所述应用对应的应用标识, 并从预先记录的合法系统调用列表中查找所述系统调用请求对应的系统调用; 以及

基于所述应用为合法应用且所述系统调用为合法系统调用的查找结果, 触发安全认证模块对所述应用进行安全认证。

9. 如权利要求 5 或 6 所述的方法, 其特征在于, 所述用于进行安全认证的信息包括 : 应用的身份特征信息和 / 或预设扩展信息。

10. 一种终端, 其特征在于, 包括 : 如权利要求 1 ~ 4 任一项所述的一种应用的安全认证系统。

## 一种应用的安全认证系统、方法、及终端

### 技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种应用的安全认证系统、方法、及终端。

### 背景技术

[0002] 智能终端已经渗透到人们工作和生活的各个领域，人们可以利用智能终端的应用进行社交、娱乐、教育、生活、出行等诸多领域。在智能终端应用为王的时代，各种应用良莠不齐，其中不乏恶意的应用窃取用户隐私、破坏用户的智能终端系统等问题，给用户带来风险和隐患。

[0003] 由于终端系统中预设应用（例如：应用商城等）在使用时需要进行系统调用，为了防止恶意程序对系统的恶意调用，终端系统会生成自身的签名密钥，并对安装在自身的合法应用的当前版本进行安全签名，预置到终端系统固件中，各应用在使用中进行系统调用时，系统使用对应的系统固件对该应用的安全签名进行验证，通过验证的应用才能成功进行使用系统资源。因此，安装在各终端系统中的应用必须采用系统签名获取系统权限才能具备系统调用能力。

[0004] 但是，各个终端在安装或者预装应用程序的时候，由于采用 Android 系统的平台不统一，导致每个终端厂家具备自己的签名密钥，各应用必须依赖于各个终端厂家的实现分别签名，才能通过安全认证获取系统执行权限。

[0005] 以应用商城为例，应用商城是智能终端中的常见应用，可以为其他各种应用的安装、卸载提供统一入口。智能终端厂家众多，并且每个终端厂家可能采用不同的 Android 系统的版本，而应用商城作为一个独立的应用，需要对每个终端厂家每个 Android 版本单独进行系统签名，同时应用商城会不断存在新增需求，需要频繁升级，而应用商城的安全签名需要终端厂家才能实现，同时市场上存在多个应用商城，智能终端厂家亦会更换应用商城以获得最好的用户体验。因此，最终会导致两个主要问题，第一个问题是应用商城的版本繁多，版本管理困难，应用商城会根据市场需求不断迭代版本，每个终端厂家的每个产品采用的平台也不一样，终端厂家的每款产品最终需要对每个应用商城版本进行固件版本制作和集成；第二个问题是应用商城开发厂家和智能终端厂家的工作存在关联，导致工作效率低下，应用商城的版本最终需要终端厂家采用各自厂家的系统签名并进行预置才能正常工作。这两个问题最终影响终端厂家产品的研发、生产、上线和运营周期。

[0006] 图 1 为现有技术中操作系统对应用商城进行安全认证时存在的缺陷示意图，如图 1 所示，A1 厂家开发了应用商城，存在版本 1 ~ 版本 N 的 N 个版本，终端厂家 B 需要对 A1 厂家每个应用商城版本采用系统签名 B 进行处理，对应生成版本 B1 ~ 版本 BN 的 N 个签了名的加密数据，并均预置到终端系统固件中，可见，A1 厂家开发的应用商城，从版本 1 向版本 N 的发展过程中，终端厂家 B 一直针对每个版本的应用商城生成新的加密数据，并且每次生成的针对新版本的加密数据都需要预置到终端系统固件中，使得系统固件频繁修改。同样，终端厂家 C 开发 2 款产品，对每一款产品都存在类似问题。如果终端厂家还需要使用 A2、A3 等其他厂家开发的应用商城，那么对每个厂家的应用商城的使用都会存在上述问题。

## 发明内容

[0007] 本发明实施例提供了一种应用的安全认证系统、方法及终端，用以解决现有技术中对应用进行安全认证时需要频繁修改固件导致系统稳定性差的问题。

[0008] 基于上述问题，本发明实施例提供的一种安全认证系统，包括：应用代理模块和安全认证模块；

[0009] 所述应用代理模块，用于接收应用发送的系统调用请求，并将所述系统调用请求中携带的用于进行安全认证的信息发送给所述安全认证模块；以及基于所述应用通过安全认证的认证结果，为所述应用调用所述系统调用请求所请求的系统功能，并向所述应用反馈系统调用的结果；

[0010] 所述安全认证模块，用于基于接收的所述用于进行安全认证的信息，按照与所述应用预先约定的安全认证方式，对所述应用进行安全认证；并将得到安全认证的结果反馈所述应用代理模块。

[0011] 本发明实施例提供的一种应用的安全认证方法，包括：

[0012] 终端中的应用代理模块接收应用发送的系统调用请求；

[0013] 将所述系统调用请求中携带的用于进行安全认证的信息发送给所述终端中的安全认证模块；

[0014] 所述安全认证模块基于接收的所述用于进行安全认证的信息，按照与所述应用预先约定的安全认证方式，对所述应用进行安全认证，并将得到安全认证的结果反馈所述应用代理模块；

[0015] 所述应用代理模块基于所述应用通过安全认证的认证结果，为所述应用调用所述系统调用请求所请求的系统功能，并向所述应用反馈系统调用的结果。

[0016] 本发明实施例提供的一种终端，包括：上述的一种应用的安全认证系统。

[0017] 本发明实施例的有益效果包括：

[0018] 本发明实施例提供的一种应用的安全认证系统、方法及终端，包括：应用代理模块，安全认证模块；应用代理模块，用于接收应用发送的系统调用请求，并将系统调用请求中携带的用于进行安全认证的信息发送给安全认证模块；以及基于应用通过安全认证的认证结果，为该应用调用系统调用请求所请求的系统功能，并向该应用反馈系统调用的结果；安全认证模块，用于基于接收的用于进行安全认证的信息，按照与该应用预先约定的安全认证方式，对该应用进行安全认证；并将得到安全认证的结果反馈应用代理模块。本发明实施例提供的一种应用的安全认证系统，通过应用代理模块实现了应用的基本功能和系统调用的分离，针对应用的任何一个版本都不需要生成系统固件，而是通过应用代理模块接收应用的系统调用请求，并通过安全认证模块对应用的安全性进行检查，既保证了应用的安全性，又保证了不对系统固件进行频繁修改，解决了现有技术中对应用进行安全认证时需要频繁修改固件导致系统稳定性差的问题。

## 附图说明

[0019] 图 1 为现有技术中操作系统对应用商城进行安全认证时存在的缺陷示意图；

[0020] 图 2 为本发明实施例提供的一种应用的安全认证系统的结构示意图；

[0021] 图 3 为本发明实施例 2 提供的一种应用的安全认证方法的流程图；

[0022] 图 4 为本发明实施例提供的应用的安全认证方法，对应用商城这一应用进行安全认证的流程图。

## 具体实施方式

[0023] 本发明实施例提供了一种应用的安全认证系统、方法、及终端，以下结合说明书附图对本发明的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明。并且在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0024] 本发明实施例提供一种应用的安全认证系统，如图 2 所示，包括：应用代理模块 201 和安全认证模块 202；

[0025] 应用代理模块 201，用于接收应用 203 发送的系统调用请求，并将系统调用请求中携带的用于进行安全认证的信息发送给安全认证模块 202；以及基于应用 203 通过安全认证的认证结果，为应用 203 调用系统调用请求所请求的系统功能，并向应用 203 反馈系统调用的结果；

[0026] 安全认证模块 202，用于基于接收的用于进行安全认证的信息，按照与应用 203 预先约定的安全认证方式，对应用 203 进行安全认证；并将得到安全认证的结果反馈应用代理模块 201。

[0027] 进一步地，如图 2 所示，终端中包括多种应用，不同的应用需要通过系统调用来调用操作系统提供的不同的功能，图 2 应用 203 仅是以终端中多种应用中的某一个应用为例，其他应用也可以与应用代理模块 201 和安全认证模块 202 具有类似的连接关系，这里不再赘述。

[0028] 进一步地，本发明实施例中，终端可以为任何智能终端，例如：智能手机、智能路由器、OTT 终端、平板电脑等。

[0029] 下面结合附图，用具体实施例对本发明提供的方法及相关设备进行详细描述。

[0030] 实施例 1：

[0031] 本发明实施例 1 中，提供一种应用的安全认证系统，如图 2 所示，包括：应用代理模块 201 和安全认证模块 202；

[0032] 应用代理模块 201，用于接收应用 203 发送的系统调用请求，并将系统调用请求中携带的用于进行安全认证的信息发送给安全认证模块 202；以及基于应用 203 通过安全认证的认证结果，为应用 203 调用系统调用请求所请求的系统功能，并向应用 203 反馈系统调用的结果；

[0033] 安全认证模块 202，用于基于接收的用于进行安全认证的信息，按照与应用 203 预先约定的安全认证方式，对应用 203 进行安全认证；并将得到安全认证的结果反馈应用代理模块 201。

[0034] 进一步地，应用代理模块 201，具体用于通过封装的系统调用接口接收应用 203 发送的系统调用请求，

[0035] 其中，封装的系统调用接口为应用代理模块 201 预先将操作系统提供的系统调用接口进行封装，得到与系统调用接口对应的封装的系统调用接口，封装的系统调用接口用

于提供给应用 203 进行系统调用。

[0036] 进一步地，本发明实施例中，可以将应用代理模块 201 作为操作系统提供的服务，当操作系统启动之后就启动，并为上层应用提供服务。应用代理模块 201 为上层应用所提供的服务就是与安全认证模块 202 相配合，检查进行调用的各应用的安全性。为了使应用代理模块 201 能够接收到各应用发送的系统调用请求，可以预先将操作系统提供的系统调用接口进行封装，得到与系统调用接口对应的封装的系统调用接口，那么当应用 203 进行系统调用时，所调用的系统调用接口为应用代理模块 201 封装过的，提供给应用 203 进行系统调用的接口，这样，应用代理模块 201 就能够接收到应用 203 发送的系统调用请求。

[0037] 进一步地，应用代理模块 201 接收的应用 203 发送的系统调用请求中可以携带用于进行安全认证的信息，其中，用于安全认证的信息可以根据应用 203 与安全认证模块 202 预先约定的安全认证方式进行确定，例如：若应用 203 与安全认证模块 202 预先约定的安全认证方式为签名方式时，则用于安全认证的信息可以包括经过签名的预设信息，若应用 203 与安全认证模块 202 预先约定的安全认证方式为与白名单进行比对的方式时，则用于安全认证的信息可以包括应用 203 的身份特征信息（例如：可以包括：应用 203 的标识、应用 203 所调用的系统功能等），也就是说，用于进行安全认证的信息包括应用 203 的身份特征信息和 / 或预设扩展信息（例如：签名信息等）。

[0038] 进一步地，安全认证模块 202 与不同的应用 203 可以约定不同的安全认证方式，各应用 203 可以根据自身对应的不同安全认证方式，在系统调用请求中携带对应的用于进行安全认证的信息，具体的安全认证方式可以根据实际需要采用现有技术中任意安全认证方式，这里并不作限定。

[0039] 进一步地，应用代理模块 201，还用于在所在终端启动时，将预设签名信息提供给操作系统，并通过操作系统对应用代理模块 201 的安全性验证；

[0040] 其中，预设签名信息为应用代理模块 201 预先使用操作系统提供的密钥对预设信息进行签名生成，并固化在操作系统中的。

[0041] 进一步地，从操作系统的角度来看，应用代理模块 201 也是操作系统中的一个应用，只是与其他上层应用 203 相比，应用代理模块 201 是更加底层应用，可以看作应用代理模块 201 位于操作系统之上，位于上层应用之下。为了使应用代理模块 201 能够对上层应用 203 进行安全认证，需要确定应用代理模块 201 的可靠性。操作系统对应用代理模块 201 的签名是终端厂家保护终端系统的安全签名，应用代理模块 201 通过操作系统的签名验证后，具备操作系统的执行权限。又由于应用代理模块 201 与上层应用相比，可以不频繁的更新版本，甚至不更新版本，因此，对应用代理模块 201 可以采用生成签名并固化在操作系统中的方式进行安全认证。

[0042] 具体地，可以预先使用操作系统提供的密钥对应用代理模块 201 提供的预设信息进行签名生成，并将生成的签名固化在操作系统中，每次在所在终端启动时，应用代理模块 201 将预设签名信息提供给操作系统，并通过操作系统对应用代理模块 201 的安全性验证。通过了安全验证之后，应用代理模块 201 才能够作为操作系统中的服务为上层应用程序进行安全认证，否则，不能为上层应用程序进行安全认证。由于应用代理模块 201 与上层应用相比，可以不频繁的更新版本，甚至不更新版本，因此不会带来现有技术中存在的频谱更新固件导致操作系统不稳定的问题。而正是因为这样，首先保证了应用代理模块 201 的可靠

性,再在接收到应用 203 发送的系统调用请求时,由安全认证模块 202 按照与应用 203 预先预定的安全认证方式对应用 203 进行安全认证,又保证了应用 203 的安全性,避免了现有技术中频繁为应用 203 更新固件导致操作系统稳定性差的问题。

[0043] 进一步地,应用代理模块 201,还用于在接收应用发送的系统调用请求之后,并在将系统调用请求中携带的用于进行安全认证的信息发送给安全认证模块 202 之前,从预先记录的合法应用列表中查找应用 203 对应的应用标识,并从预先记录的合法系统调用列表中查找所述系统调用请求对应的系统调用;以及基于应用 203 为合法应用且系统调用为合法系统调用的查找结果,触发安全认证模块 202 对应用 203 进行安全认证。

[0044] 进一步地,应用代理模块 201 在接收到应用 203 发送的系统调用请求之后,可以对应用 203 进行初步检查,在应用 203 通过了初步检查之后,再由安全认证模块 202 对应用 203 进行更深层次的安全认证(例如:签名认证等),应用代理模块 201 可以预先存储合法应用对应的应用标识列表,以及合法系统调用对应的系统调用列表,从应用标识列表中查找应用 203 的标识,以及从系统调用列表中查找应用 203 发送的系统调用请求对应的系统调用,当应用 203 以及应用 203 进行的系统调用均合法时,确定应用 203 通过初步检查,可以触发安全认证模块 202 对应用 203 进行更进一步的安全认证。

[0045] 实施例 2:

[0046] 基于本发明实施例 1 提供的应用的安全认证系统,实施例 2 提供一种应用的安全认证方法,如图 3 所示,包括如下步骤:

[0047] S301、在应用代理模块所在终端启动时,应用代理模块将预设签名信息提供给操作系统,并通过操作系统对应用代理模块的安全性验证。

[0048] 其中,预设签名信息为应用代理模块预先使用操作系统提供的密钥对预设信息进行签名生成,并固化在操作系统中的。

[0049] 本步骤中,若应用代理模块未能通过操作系统对应用代理模块的安全性验证,则无法执行后续的步骤。

[0050] S302、应用代理模块通过封装的系统调用接口接收应用发送的系统调用请求,

[0051] 其中,封装的系统调用接口为应用代理模块预先将操作系统提供的系统调用接口进行封装,得到与系统调用接口对应的封装的系统调用接口,封装的系统调用接口用于提供给应用进行系统调用。

[0052] S303、从预先记录的合法应用列表中查找应用对应的应用标识,并从预先记录的合法系统调用列表中查找系统调用请求对应的系统调用。

[0053] S304、判断应用是否为合法应用且系统调用是否为合法系统调用,若是,则进入步骤 S305,否则,结束本流程。

[0054] 进一步地,本步骤中,当判断出应用为非法应用或者系统调用为非法系统调用时,则结束本流程。

[0055] S305、将 S302 中接收的系统调用请求中携带的用于进行安全认证的信息发送给终端中的安全认证模块。

[0056] S306、安全认证模块基于接收的用于进行安全认证的信息,按照与应用预先约定的安全认证方式,对应用进行安全认证,并将得到安全认证的结果反馈应用代理模块。

[0057] S307、应用代理模块基于应用通过安全认证的认证结果,为应用调用系统调用请

求所请求的系统功能，并向应用反馈系统调用的结果。

[0058] 下面以应用商城为例对本发明实施例提供的一种应用的安全认证方法进行举例说明。

[0059] 图 4 为本发明实施例提供的应用的安全认证方法，对应用商城这一应用进行安全认证的流程图，应用商城是用户智能终端上的应用入口，一方面提供应用的展示、介绍、下载、安装、升级、使用、下载等功能，另一方面根据用户的喜好，提供用户界别定制化的应用服务，比如使用时长统计、偏好分析等内容。在应用商城对应用进行安装或者卸载时需要通过相关的系统调用完成。如图 4 所示，包括如下步骤：

[0060] S401、应用商城根据用户指示启动。

[0061] S402、应用商城通过终端中的显示模块显示用户可以使用的各应用的列表，以及各应用的状态。

[0062] 进一步地，在应用商城的显示界面用户可以使用已经安装的应用。应用商城具有应用签名，应用签名是应用商城正式发布时候的签名，保证应用商城的合法性，由应用商城的开发者提供密钥并完成签名。

[0063] S403、当接收到用户发送的安装或者卸载应用的指示时，向应用代理模块发送对应的系统调用请求。

[0064] 进一步地，若用户发送安装应用的指示，则向应用代理模块发送安装应用的系统调用请求，若用户发送卸载应用的指示，则向应用代理模块发送卸载应用的系统调用请求。

[0065] 应用代理是连接外部应用商城到智能终端系统的内部操作系统的纽带。对于安全终端的实现，应用代理是实现终端应用内部操作的唯一通道。应用代理提供对外统一的接口，供应用商城调用。应用代理由终端厂家实现，具备系统执行权限。应用代理模块在终端产品实现之后，一般不会修改，并且可方便移植到其他终端产品。

[0066] S404、应用代理模块对应用商城进行初步检查。

[0067] 本步骤中，应用代理模块可以从预先记录的合法应用列表中查找应用商城对应的应用标识，并从预先记录的合法系统调用列表中查找安装或卸载的系统调用请求对应的系统调用；以及基于应用商城为合法应用且系统调用为合法系统调用的查找结果，触发安全认证模块对应用商城进行安全认证。

[0068] 基于应用商城为非法应用或者系统调用为非法系统调用的查找结果，拒绝未应用商城进行系统调用。

[0069] S405、在应用商城通过初步检查之后，将系统调用请求中携带的用于进行安全认证的信息发送给安全认证模块。

[0070] S406、安全认证模块根据接收的用于进行安全认证的信息，通过与应用商城预先约定的认证方式对应用商城进行安全认证。

[0071] 进一步地，本步骤中，可以通过白名单检查应用商城的安全性，此时，用于安全认证的信息可以为应用商城的身份特征信息，也可以通过签名认证等认证方式检查应用商城的安全性，此时，用于安全认证的信息可以为预设扩展信息。

[0072] S407、安全认证模块向应用代理模块反馈对应用商城进行安全认证的结果。

[0073] S408、当安全认证的结果为成功时，应用代理模块为应用商城调用上述系统调用请求所请求的操作系统的相关功能。

[0074] 进一步地,应用代理模块调用的操作系统的相关功能可以由操作管理模块实现,由操作管理模块对应用代理模块调用的相关功能进行操作管理。针对应用商城,对应用的安装和卸载,可调用系统内部的应用管理工具,例如:Android 系统用于各类应用(包)的安装、卸载、查询等管理的系统标准接口包管理应用(PM Utility, Package Management)实现应用的安装、卸载等功能。

[0075] S409、应用代理模块接收系统调用的结果。

[0076] S410、应用代理模块将系统调用的结果反馈给应用商城。

[0077] 进一步地,应用代理模块与应用商城进行的通信为进程间的通信,为了保证应用代理模块为应用商城进行安全认证时不会将应用商城挂起,可以通过广播将系统调用的结果反馈给应用商城。

[0078] S411、应用商城根据系统调用的结果,更新各应用的状态。

[0079] S412、根据用户的指示退出应用商城。

[0080] 本发明实施例提供的一种应用的安全认证系统、方法及终端,包括:应用代理模块,安全认证模块;应用代理模块,用于接收应用发送的系统调用请求,并将系统调用请求中携带的用于进行安全认证的信息发送给安全认证模块;以及基于应用通过安全认证的认证结果,为该应用调用系统调用请求所请求的系统功能,并向该应用反馈系统调用的结果;安全认证模块,用于基于接收的用于进行安全认证的信息,按照与该应用预先约定的安全认证方式,对该应用进行安全认证;并将得到安全认证的结果反馈应用代理模块。本发明实施例提供的一种应用的安全认证系统,通过应用代理模块实现了应用的基本功能和系统调用的分离,针对应用的任何一个版本都不需要生成系统固件,而是通过应用代理模块接收应用的系统调用请求,并通过安全认证模块对应用的安全性进行检查,既保证了应用的安全性,又保证了不对系统固件进行频繁修改,解决了现有技术中对应用进行安全认证时需要频繁修改固件导致系统稳定性差的问题。

[0081] 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实施例可以通过硬件实现,也可以借助软件加必要的通用硬件平台的方式来实现。基于这样的理解,本发明实施例的技术方案可以以软件产品的形式体现出来,该软件产品可以存储在一个非易失性存储介质(可以是 CD-ROM, U 盘, 移动硬盘等)中,包括若干指令用以使得一台计算机设备(可以是个人计算机,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。

[0082] 本领域技术人员可以理解附图只是一个优选实施例的示意图,附图中的模块或流程并不一定是实施本发明所必须的。

[0083] 本领域技术人员可以理解实施例中的装置中的模块可以按照实施例描述进行分布于实施例的装置中,也可以进行相应变化位于不同于本实施例的一个或多个装置中。上述实施例的模块可以合并为一个模块,也可以进一步拆分成多个子模块。

[0084] 上述本发明实施例序号仅仅为了描述,不代表实施例的优劣。

[0085] 显然,本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样,倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内,则本发明也意图包含这些改动和变型在内。

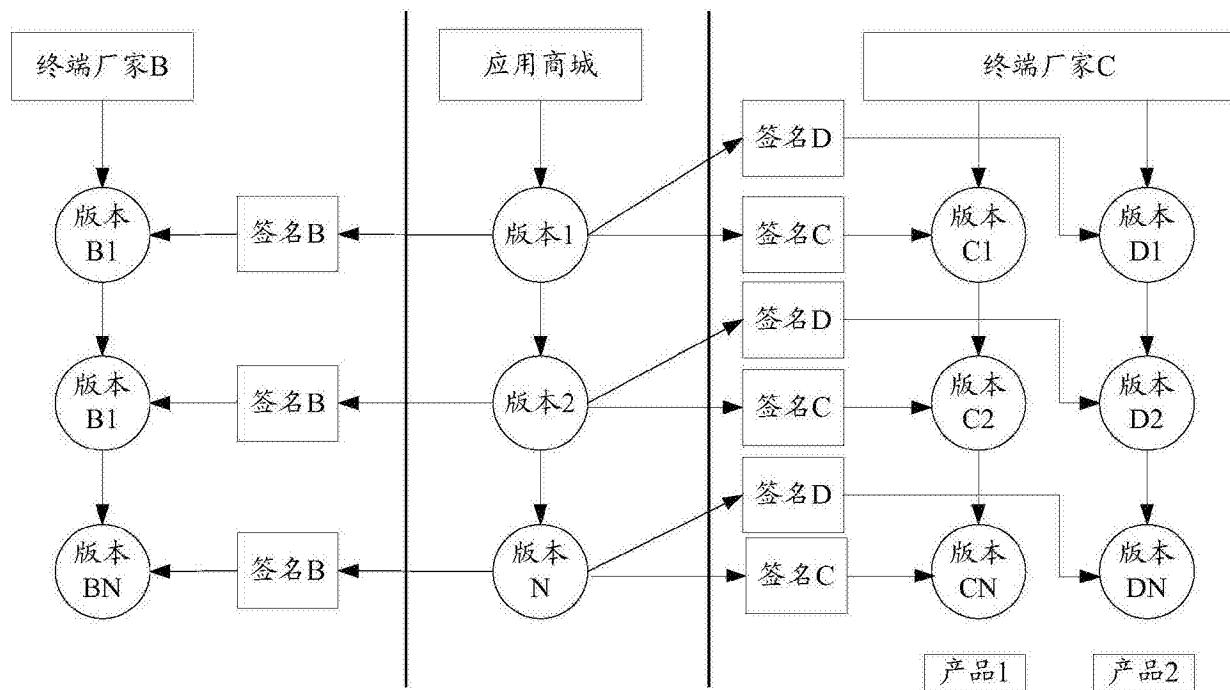


图 1

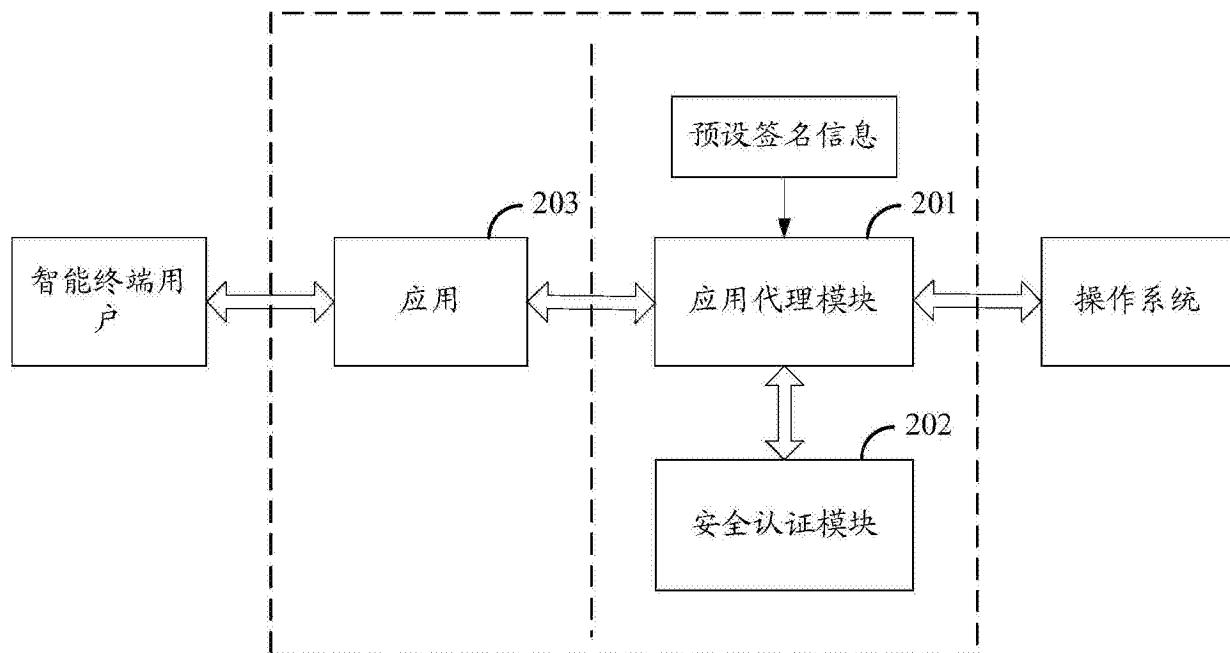


图 2

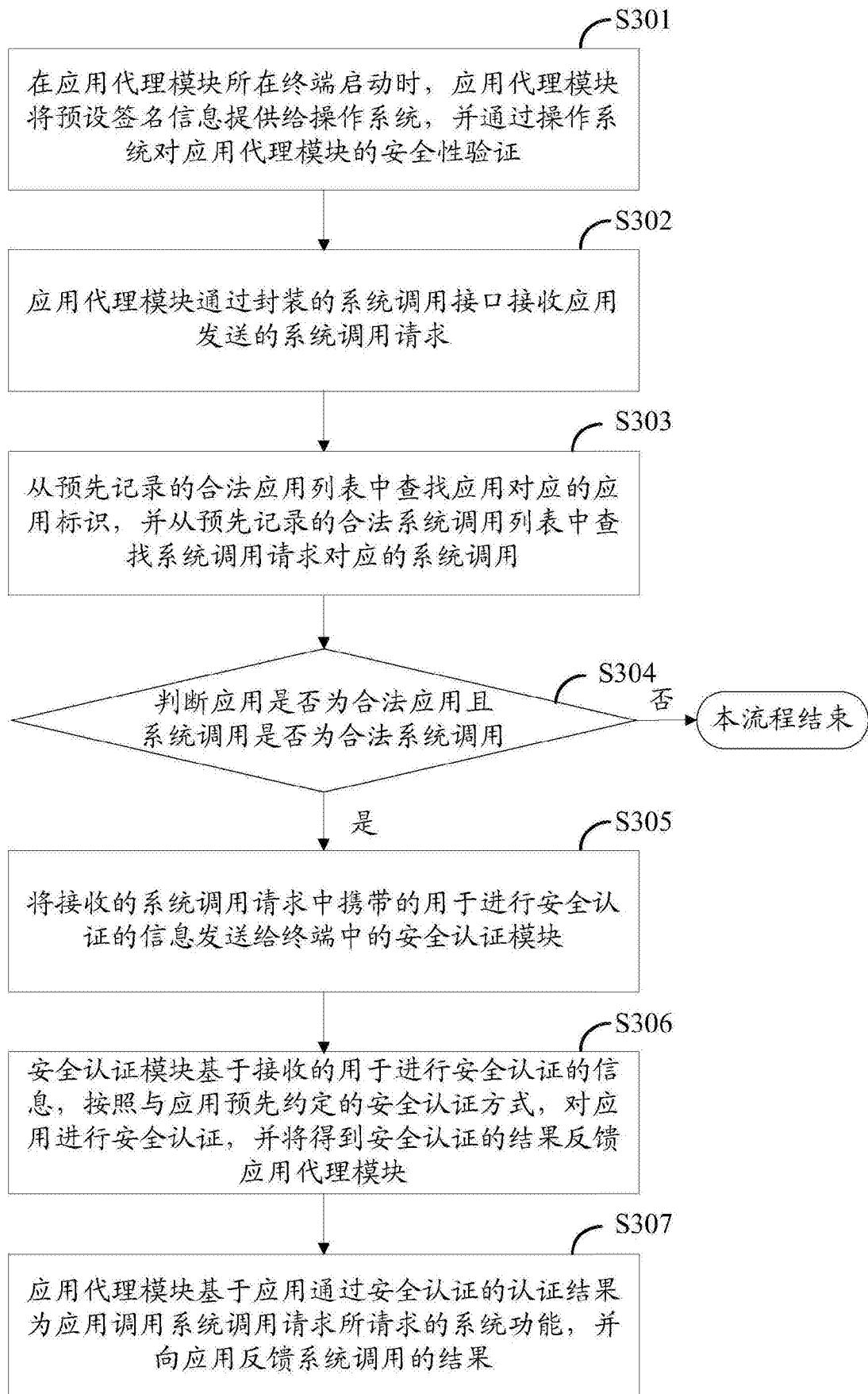


图 3

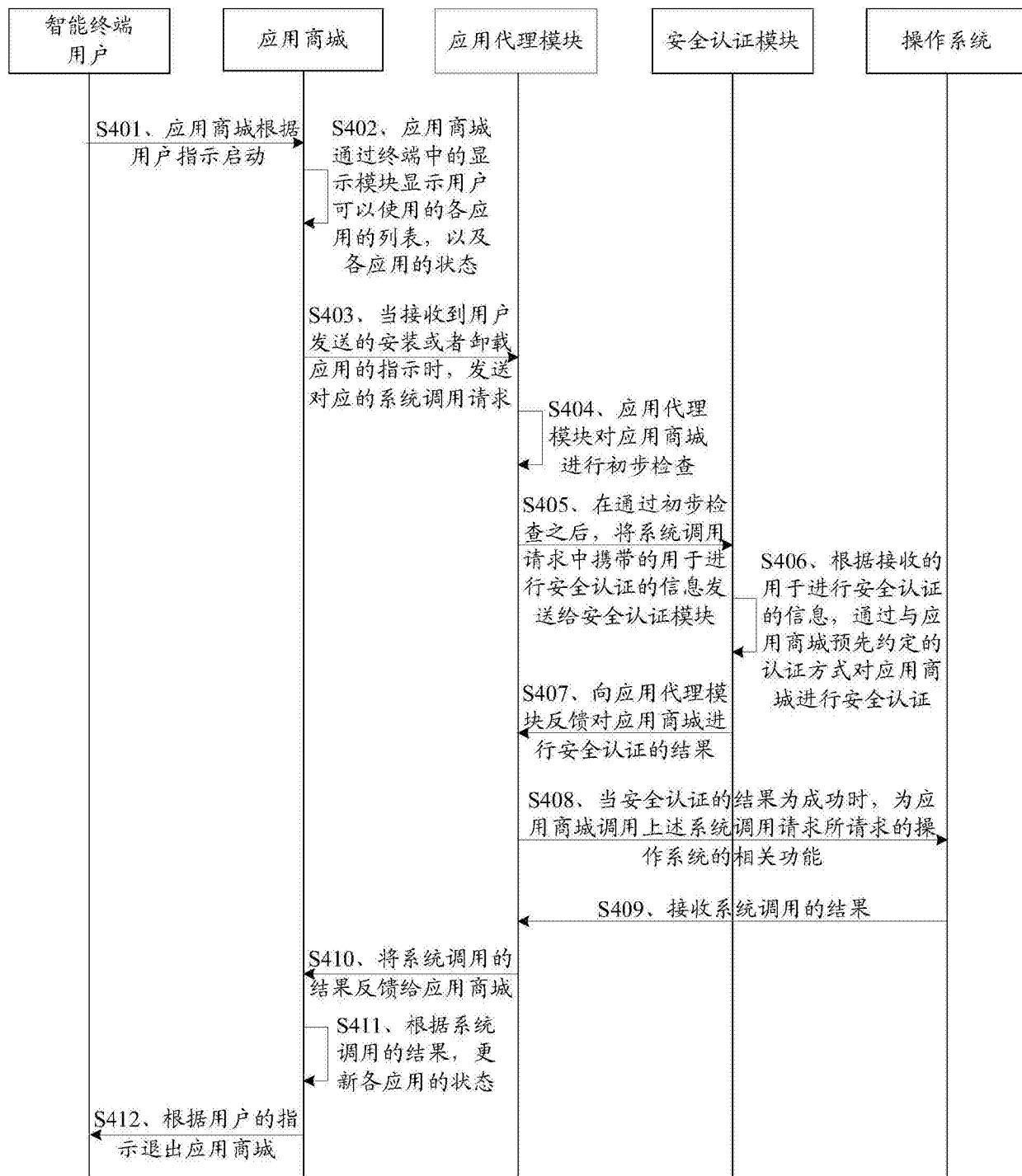


图 4