(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 109120612 A
(43)申请公布日 2019.01.01

(21)申请号 201810882116.0

(22)申请日 2018.08.06

(71)申请人 浙江衣拿智能科技有限公司
地址 318000 浙江省台州市椒江区飞跃科创园32幢

(72)发明人 翁端文 吕新 褚如昶

(74)专利代理机构 杭州千克知识产权代理有限公司 33246
代理人 裴金华

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/62(2013.01)

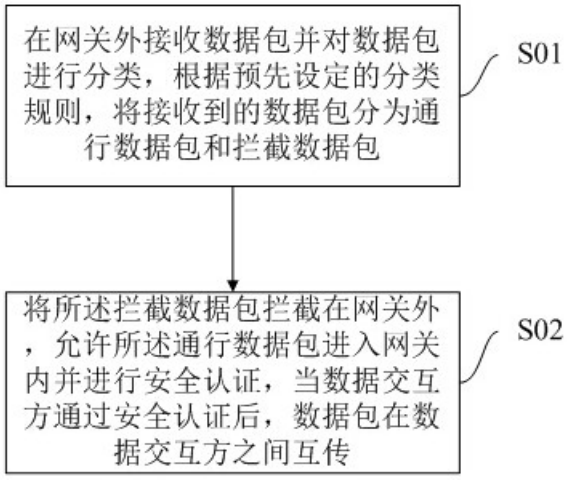
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种数据包过滤方法、系统及应用程序

(57)摘要

一种数据包过滤方法、系统及应用程序，属于应用程序技术领域。方法用于应用程序端；包括步骤S01，在网关外接收数据包并分类为通行数据包和拦截数据包；步骤S02，将拦截数据包拦截在网关外，允许通行数据包进入网关内并进行安全认证，当通过安全认证后，数据包在数据交互方之间互传。系统包括接收模块、分类模块、过滤模块、认证模块，分类模块在网关外对接收的数据包分为通行数据包和拦截数据包；过滤模块将拦截数据包拦截于网关外，并允许通行数据包进入网关；认证模块允许通过安全认证的数据包在数据交互方之间互传。应用程序采用上述系统。本发明辅助智能终端对来自与之交互的应用程序或浏览器的数据包进行数据过滤及认证，确保个人信息安全性。



CN 109120612 A

1.一种数据包过滤方法,其特征在于,用于应用程序端;方法包括:

步骤S01,在网关外接收数据包并对数据包进行分类,根据预先设定的分类规则,将接收到的数据包分为通行数据包和拦截数据包;

步骤S02,将所述拦截数据包拦截在网关外,允许所述通行数据包进入网关内并进行安全认证,当数据交互方通过安全认证后,数据包在数据交互方之间互传。

2.根据权利要求1所述的一种数据包过滤方法,其特征在于,步骤S01中预先设定的分类规则包括:

存在安全隐患的数据包和/或指定拦截的数据包被分类为拦截数据包;则其他数据包为通行数据包。

3.根据权利要求1所述的一种数据包过滤方法,其特征在于,步骤S02中将拦截数据包拦截在网关外的具体步骤包括:

当检测分类后的拦截数据包中数据包为存在安全隐患的数据包时,直接拦截数据包于网关外;

当检测分类后的拦截数据包中数据包为指定拦截的数据包时,确认当前需要拦截该指定拦截的数据包,则拦截数据包于网关外。

4.根据权利要求1所述的一种数据包过滤方法,其特征在于,步骤S02中通行数据包进入网关内进行安全认证的具体步骤包括:

所述通行数据包内的认证码在应用程序端进行安全认证,若认证通过,则应用程序发送反馈数据包经网关至数据包发送方,否则不发送反馈数据包。

5.一种数据包过滤系统,其特征在于,用于应用程序端;系统包括:

接收模块,用于在网关外接收数据包;

分类模块,用于在网关外对接收的数据包进行分类,根据预先设定的分类规则,将接收到的数据包分为通行数据包和拦截数据包;

过滤模块,用于将拦截数据包拦截于网关外,并允许通行数据包进入网关;

认证模块,用于对进入网关的通行数据包进行安全认证,当数据交互方通过安全认证后,数据包在数据交互方之间互传。

6.根据权利要求5所述的一种数据包过滤系统,其特征在于,所述预先设定的分类规则包括:存在安全隐患的数据包和/或指定拦截的数据包被分类为拦截数据包;则其他数据包为通行数据包。

7.根据权利要求6所述的一种数据包过滤系统,其特征在于,所述通行数据包根据发送数据包的来源方或者发送数据包的类型进行分类。

8.根据权利要求5所述的一种数据包过滤系统,其特征在于,所述过滤模块包括:

第一判断单元,用于判断数据包为通行数据包时,允许通行数据包进入网关,当判断数据包为拦截数据包时,触发第二判断单元;

第二判断单元,用于判断拦截数据包中数据包为存在安全隐患的数据包时,直接拦截数据包于网关外,而判断拦截数据包中数据包为指定拦截的数据包时,触发通知单元;

通知单元,用于确定当前是否需要拦截该指定拦截的数据包,若是则拦截数据包于网关外,否则允许数据包进入网关。

9.根据权利要求8所述的一种数据包过滤系统,其特征在于,所述认证模块包括:

认证单元，在应用程序端认证通行数据包内的认证码，若认证通过，则触发运行单元；

运行单元，接收通行数据包运行并发送反馈数据包经网关至数据包发送方。

10.一种应用程序，设于智能终端，其特征在于，采用上述权利要求5-9之一的数据包过滤系统。

一种数据包过滤方法、系统及应用程序

技术领域

[0001] 本发明涉及应用程序技术领域，尤其涉及一种数据包过滤方法、系统及应用程序。

背景技术

[0002] 现有智能设备，如手机、平板电脑等上的应用程序或浏览器在使用过程中，终端个人信息不经过智能设备端同意就被提取，个人信息安全性没有保证。现有智能设备的IOS系统或安卓系统通过设置通知的方式告知使用方，是否允许接收应用程序或浏览器发送的实时消息，是否允许应用程序保持后台运转状态。然而，这类通知是根据使用方的使用需要为基准设置的，当使用方需要/想要接收实时消息时，则开启通知，否则关闭；此方式并未对数据进行安全性过滤，甚至安全认证。并且，在使用应用程序或浏览器时，系统一般默认使用期间智能设备与应用程序或浏览器之间可以进行数据交互，而此过程中并未有对数据进行安全性过滤和安全认证。

发明内容

[0003] 本发明针对现有技术存在的问题，提出了一种能辅助智能设备对进行数据交互的应用程序或浏览器进行数据安全过滤、认证的数据包过滤方法、系统及应用程序。

[0004] 本发明是通过以下技术方案得以实现的：

本发明一种数据包过滤方法，用于应用程序端；方法包括：

步骤S01，在网关外接收数据包并对数据包进行分类，根据预先设定的分类规则，将接收到的数据包分为通行数据包和拦截数据包；

步骤S02，将所述拦截数据包拦截在网关外，允许所述通行数据包进入网关内并进行安全认证，当数据交互方通过安全认证后，数据包在数据交互方之间互传。

[0005] 本发明方法用于应用程序端，辅助智能终端在与其他应用程序或浏览器数据交互时，避免个人信息不经同意而随意泄露的问题发生，确保个人信息安全性。同时避免智能设备一直与后台开启的任何应用程序或浏览器进行数据交互，节约系统运行资源，提高智能终端系统运行效率。

[0006] 作为优选，步骤S01中预先设定的分类规则包括：

存在安全隐患的数据包和/或指定拦截的数据包被分类为拦截数据包；则其他数据包为通行数据包。

[0007] 作为优选，步骤S02中将拦截数据包拦截在网关外的具体步骤包括：

当检测分类后的拦截数据包中数据包为存在安全隐患的数据包时，直接拦截数据包于网关外；

当检测分类后的拦截数据包中数据包为指定拦截的数据包时，确认当前需要拦截该指定拦截的数据包，则拦截数据包于网关外。

[0008] 作为优选，步骤S02中通行数据包进入网关内进行安全认证的具体步骤包括：

所述通行数据包内的认证码在应用程序端进行安全认证，若认证通过，则应用程序发

送反馈数据包经网关至数据包发送方，否则不发送反馈数据包。

[0009] 一种数据包过滤系统，用于应用程序端；系统包括：

接收模块，用于在网关外接收数据包；

分类模块，用于在网关外对接收的数据包进行分类，根据预先设定的分类规则，将接收到的数据包分为通行数据包和拦截数据包；

过滤模块，用于将拦截数据包拦截于网关外，并允许通行数据包进入网关；

认证模块，用于对进入网关的通行数据包进行安全认证，当数据交互方通过安全认证后，数据包在数据交互方之间互传。

[0010] 作为优选，所述预先设定的分类规则包括：存在安全隐患的数据包和/或指定拦截的数据包被分类为拦截数据包；则其他数据包为通行数据包。

[0011] 作为优选，所述通行数据包根据发送数据包的来源方或者发送数据包的类型进行分类。

[0012] 作为优选，所述过滤模块包括：

第一判断单元，用于判断数据包为通行数据包时，允许通行数据包进入网关，当判断数据包为拦截数据包时，触发第二判断单元；

第二判断单元，用于判断拦截数据包中数据包为存在安全隐患的数据包时，直接拦截数据包于网关外，而判断拦截数据包中数据包为指定拦截的数据包时，触发通知单元；

通知单元，用于确定当前是否需要拦截该指定拦截的数据包，若是则拦截数据包于网关外，否则允许数据包进入网关。

[0013] 作为优选，所述认证模块包括：

认证单元，在应用程序端认证通行数据包内的认证码，若认证通过，则触发运行单元；

运行单元，接收通行数据包运行并发送反馈数据包经网关至数据包发送方。

[0014] 一种应用程序，设于智能终端，采用上述数据包过滤系统。

[0015] 该应用程序为智能终端上的app，采用数据包过滤系统实现，能确保数据交互信息安全，并提高智能终端系统运行效率。

[0016] 本发明具有以下有益效果：

本发明一种数据包过滤方法、系统及应用程序，辅助智能终端在与应用程序或浏览器进行数据交互时，对数据包进行安全性过滤，并对过滤通过的数据包进行安全认证，以使得智能终端的个人信息不会任意泄露，确保个人信息安全性。

附图说明

[0017] 图1为本发明一种数据包过滤方法的流程框图；

图2为本发明一种数据包过滤系统的系统框图；

图3为本发明一种数据包过滤系统中过滤模块的结构框图。

具体实施方式

[0018] 以下是本发明的具体实施例并结合附图，对本发明的技术方案作进一步的描述，但本发明并不限于这些实施例。

[0019] 本发明提供一种应用程序，即app，安装于智能终端，如智能手机、平板电脑等。该

应用程序可辅助智能终端过滤数据，将来自其他应用程序或浏览器的不安全数据包和/或不被选择通过的数据包滤除，进而使安全和/或选择通过的数据包通过网关。进一步对通过网关的数据包进行安全认证，认证通过后使得智能终端与其他应用程序/浏览器进行数据交互。

[0020] 本发明应用程序主要采用图2所示的数据包过滤系统。具体地，本发明一种数据包过滤系统包括接收模块、分类模块、过滤模块、认证模块。

[0021] 所述接收模块用于在网关外接收数据包，接收各种类型的数据包。如按发送数据包的来源方分类，包括来自购物app的数据包、来自浏览器的数据包、来自银行app的数据包等；如按发送数据包的类型进行分类，包括位置定位信息请求数据包、相册访问请求数据包、数据共享请求数据包等。

[0022] 所述分类模块用于在网关外对接收的数据包进行分类，根据预先设定的分类规则，将接收到的数据包分为通行数据包和拦截数据包。一实施方式下，所述预先设定的分类规则包括：存在安全隐患的数据包和/或指定拦截的数据包被分类为拦截数据包；则其他数据包为通行数据包。所述存在安全隐患的数据包为存在病毒、存在破坏智能终端系统问题的数据包。所述指定拦截的数据包为根据用户选择而设定待拦截的数据包，通过用户界面选择的方式对安装于智能终端的应用程序、浏览器进行选择，或通过用户界面选择数据包类型。另一实施方式下，所述预先设定的分类规则可以包括：所述通行数据包为指定通行数据包，如根据数据包的来源方或者发送数据包的类型来选择，而拦截数据包为除了指定通行数据包外的其他数据包。所述通行数据包可通过用户界面选择的方式对安装于智能终端的应用程序、浏览器进行选择，或通过用户界面选择数据包类型。另一实施方式下，所述预先设定的分类规则可以包括：存在安全隐患的数据包和/或指定拦截的数据包被分类为拦截数据包，指定通行的数据包被分类为通行数据包。指定拦截/通行的数据包括可通过用户界面选择的方式对安装于智能终端的应用程序、浏览器进行选择，或通过用户界面选择数据包类型。

[0023] 所述过滤模块用于将拦截数据包拦截于网关外，并允许通行数据包进入网关。如图3，所述过滤模块包括第一判断单元、第二判断单元和通知单元。所述第一判断单元用于判断数据包为拦截数据包还是通行数据包，当判断数据包为通行数据包时，允许通行数据包进入网关，而当判断数据包为拦截数据包时，通过第二判断单元进一步判断拦截数据包归属于哪一类，对拦截数据包进行分类处理。如，拦截数据包被设定为存在安全隐患的数据包和/或指定拦截的数据包时，对存在安全隐患的数据包直接进行拦截，拦截于网关外，而对于指定拦截的数据包进行再次确认，以便于用户确认当前是否需要拦截数据包，而不是永久性拦截。为此，所述第二判断单元用于判断拦截数据包中数据包为存在安全隐患的数据包时，直接拦截数据包于网关外，而判断拦截数据包中数据包为指定拦截的数据包时，触发通知单元。所述通知单元，以弹屏窗口或通知方式出现于智能终端的界面，用于确定当前是否需要拦截该指定拦截的数据包，当用户选择是，则拦截数据包于网关外，若用户选择否，允许原本被设定为指定拦截的数据包于当前进入网关内，当前被允许进入网关的指定拦截的数据包改变数据包类型，如可通过改变数据包标识符的方式将原先指定拦截的数据包改为通行数据包。当下一次接收到同样的数据包时，仍然通过第一判断单元、第二判断单元、通知单元进行判断，下一次用户又将利用通知单元重新选择。

[0024] 由此，智能终端利用采用数据包过滤系统的应用程序，可由用户主动设置拦截、通行数据包，也可由智能终端自动对数据包进行拦截，也可永久拦截或以通知的方式对数据包非永久拦截/通行。这样能更好地管理个人信息安全，以及智能终端系统运行。

[0025] 所述认证模块用于对进入网关的通行数据包进行安全认证，当数据交互方通过安全认证后，数据包在数据交互方之间互传。为了进一步确保个人信息安全，利用认证模块对删选入网关内的数据包进行再次安全认证。一方面提高了智能终端的安全性，另一方面约束了智能终端与应用程序/浏览器进行数据交互的范畴，即智能终端不再无条件响应同一数据交互方发送的任意类型的数据包，以限制数据交互安全程度。

[0026] 所述认证模块包括认证单元、运行单元。所述认证单元在应用程序端认证通行数据包内的认证码，若认证通过，则触发运行单元，否则，不做任何响应。所述运行单元，接收通行数据包运行并发送反馈数据包经网关至数据包发送方。该认证码为预先设定的认证码，当应用程序端收到该认证码进行比对。应用程序端也预存有认证码，将其与通行数据包的认证码进行比对，当两认证码一致时，则认证通过，即该通行数据包为可被应用程序端运行的数据包。运行单元根据通行数据包内的内容执行程序，当有执行结果时，发送带有执行结果的反馈数据包经网关发送至数据包发送方。当两认证码不一致时，则认证不通过，其他应用程序/浏览器无法接收到反馈数据包，则认为发送的数据包不被响应。或者，该认证码为当前利用加密算法基于请求命令生成的认证码，应用程序端根据接收到命令请求基于加密算法计算认证码，若认证单元判断发送来的认证码与生成的认证码一致时，认证通过，运行单元动作，反之认证失败。

[0027] 所述认证模块对通行数据包进行认证，此处通行数据包为原先设定的通行数据包和/或从原先设定的拦截数据包经过滤模块的通知单元临时改变类型的通行数据包。

[0028] 本发明利用过滤模块来验证智能终端接收数据包发送方发送的数据包的可靠性，进而开辟智能终端接收信息的通道；而利用认证模块来验证数据包发送方是否能够接收智能终端反馈数据包，进而开辟智能终端发送信息的通道。一旦通过过滤模块、认证模块，则智能终端与数据包发送方两者之间可以进行数据交互。该数据交互主要指当前发送数据包内容的交互，而不是说数据包发送方的任何一次数据交互都被允许，也不是说任意数据包发送方的某一类型的数据包内容能在智能终端与应用程序/浏览器之间运行。

[0029] 图1示出了本发明一种数据包过滤方法，用于应用程序端。该方法包括：

步骤S01，在网关外接收数据包并对数据包进行分类，根据预先设定的分类规则，将接收到的数据包分为通行数据包和拦截数据包；

步骤S02，将所述拦截数据包拦截在网关外，允许所述通行数据包进入网关内并进行安全认证，当数据交互方通过安全认证后，数据包在数据交互方之间互传。

[0030] 所述步骤S01中数据包的接收由接收模块执行，分类模块对接收的数据包进行分类。

[0031] 所述步骤S02中将拦截数据包拦截在网关外的具体步骤包括：

当检测分类后的拦截数据包中数据包为存在安全隐患的数据包时，直接拦截数据包于网关外；

当检测分类后的拦截数据包中数据包为指定拦截的数据包时，确认当前需要拦截该指定拦截的数据包，则拦截数据包于网关外。

[0032] 步骤S02通过第一判断单元、第二判断单元、通知单元对拦截数据包进行分情况拦截。

[0033] 步骤S02中通行数据包进入网关内进行安全认证的具体步骤包括：

所述述通行数据包内的认证码在应用程序端进行安全认证，若认证通过，则应用程序发送反馈数据包经网关至数据包发送方，否则不发送反馈数据包。

[0034] 安全认证利用认证单元进行，当认证通过时，由运行单元实现数据交互处理和反馈。

[0035] 本领域的技术人员应理解，上述描述及附图中所示的本发明的实施例只作为举例而并不限制本发明。本发明的目的已经完整有效地实现。本发明的功能及结构原理已在实施例中展示和说明，在没有背离所述原理下，本发明的实施方式可以有任何变形或修改。

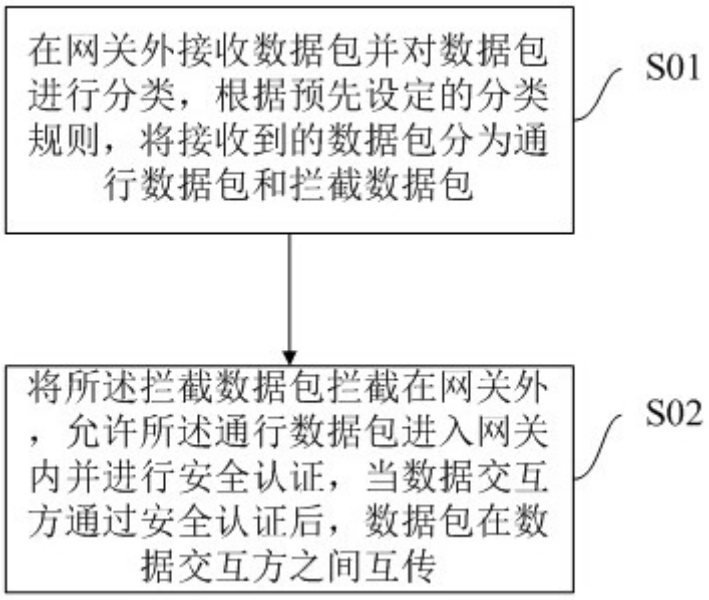

在网关外接收数据包并对数据包进行分类，根据预先设定的分类规则，将接收到的数据包分为通行数据包和拦截数据包
S01
将所述拦截数据包拦截在网关外，允许所述通行数据包进入网关内并进行安全认证，当数据交互方通过安全认证后，数据包在数据交互方之间互传
S02

图1

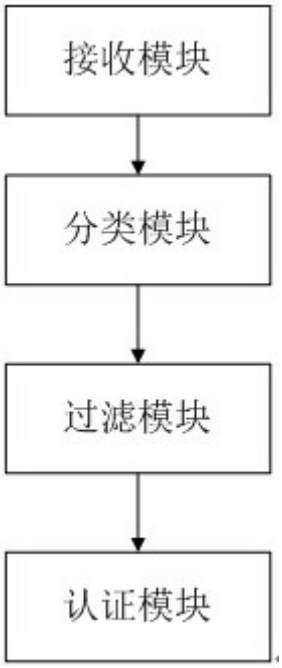

接收模块
分类模块
过滤模块
认证模块

图2

图3