



# (12) 发明专利申请

(10) 申请公布号 CN 104123120 A

(43) 申请公布日 2014. 10. 29

(21) 申请号 201310142674. 0

(22) 申请日 2013. 04. 23

(71) 申请人 腾讯科技(深圳)有限公司

地址 518031 广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室

(72) 发明人 童磊

(74) 专利代理机构 深圳市深佳知识产权代理事

务所(普通合伙) 44285

代理人 唐华明

(51) Int. Cl.

G06F 9/44(2006. 01)

G06F 17/30(2006. 01)

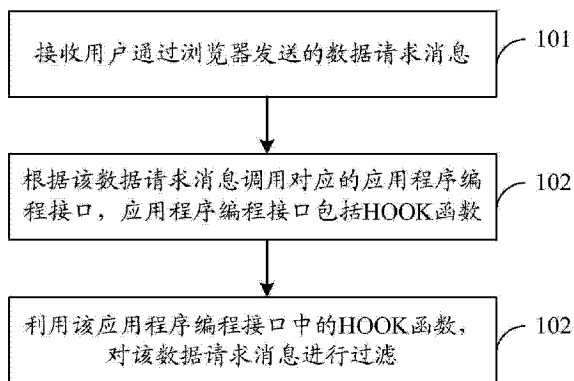
权利要求书2页 说明书15页 附图5页

## (54) 发明名称

一种浏览器页面数据过滤方法、装置和系统

## (57) 摘要

本发明实施例公开了一种浏览器页面数据过滤方法、装置和系统。本发明实施例采用接收用户通过浏览器发送的数据请求消息,根据该数据请求消息调用对应的应用程序编程接口,其中,该应用程序编程接口包括钩子函数,利用该应用程序编程接口中的钩子函数,对所述数据请求消息进行过滤;由于基本上所有浏览器在请求数据时都会使用应用程序编程接口,因此,该方案兼容性较好,不会存在兼容性问题,无需特意为不同的浏览器开发特定的插件,不仅无需后期维护,而且开发量较小,实现灵活。



1. 一种浏览器页面数据过滤方法,其特征在于,包括:  
接收用户通过浏览器发送的数据请求消息;  
根据所述数据请求消息调用对应的应用程序编程接口,所述应用程序编程接口包括钩子函数;  
利用所述应用程序编程接口中的钩子函数,对所述数据请求消息进行过滤。
2. 根据权利要求1所述的方法,其特征在于,所述利用所述应用程序编程接口中的钩子函数,对所述数据请求消息进行过滤,包括:  
利用所述应用程序编程接口中的钩子函数,确定所述数据请求消息即将请求的数据为预置的需要拦截的数据时,阻止所述数据请求消息。
3. 根据权利要求1所述的方法,其特征在于,所述利用所述应用程序编程接口中的钩子函数,对所述数据请求消息进行过滤,包括:  
利用所述应用程序编程接口中的钩子函数,确定所述数据请求消息即将请求的数据为预置的需要拦截的数据时,根据所述数据请求消息返回一个空白文件,作为所述数据请求消息所请求的数据。
4. 根据权利要求1所述的方法,其特征在于,所述利用所述应用程序编程接口中的钩子函数,对所述数据请求消息进行过滤,包括:  
利用所述应用程序编程接口中的钩子函数,确定所述数据请求消息即将请求的数据为预置的需要拦截的第一类数据时,阻止所述数据请求消息;  
利用所述应用程序编程接口中的钩子函数,确定所述数据请求消息即将请求的数据为预置的需要拦截的第二类数据时,根据所述数据请求消息返回一个空白文件,作为所述数据请求消息所请求的数据。
5. 根据权利要求4所述的方法,其特征在于,  
所述利用所述应用程序编程接口中的钩子函数,确定所述数据请求消息即将请求的数据为预置的需要拦截的第一类数据时,阻止所述数据请求消息,具体为:利用所述应用程序编程接口中的钩子函数,确定所述数据请求消息即将请求的数据为广告链接且为非图片链接时,阻止所述数据请求消息;  
所述利用所述应用程序编程接口中的钩子函数,确定所述数据请求消息即将请求的数据为预置的需要拦截的第二类数据时,根据所述数据请求消息返回一个空白文件,作为所述数据请求消息所请求的数据,具体为:利用所述应用程序编程接口中的钩子函数,确定所述数据请求消息即将请求的数据为广告链接且为图片链接时,根据所述数据请求消息返回一个空白图片文件,作为所述数据请求消息所请求的数据。
6. 根据权利要求1至5任一项所述的方法,其特征在于,所述利用所述应用程序编程接口中的钩子函数,对所述数据请求消息进行过滤之后,还包括:  
返回过滤结果给用户。
7. 一种浏览器页面数据过滤装置,其特征在于,包括:  
接收单元,用于接收用户通过浏览器发送的数据请求消息;  
调用单元,用于根据所述数据请求消息调用对应的应用程序编程接口,所述应用程序编程接口包括钩子函数;  
过滤单元,用于利用所述应用程序编程接口中的钩子函数,对所述数据请求消息进行

过滤。

8. 根据权利要求7所述的浏览器页面数据过滤装置,其特征在于,

所述过滤单元,具体用于利用所述应用程序编程接口中的钩子函数,确定所述数据请求消息即将请求的数据为预置的需要拦截的数据时,阻止所述数据请求消息。

9. 根据权利要求7所述的浏览器页面数据过滤装置,其特征在于,

所述过滤单元,具体用于利用所述应用程序编程接口中的钩子函数,确定所述数据请求消息即将请求的数据为预置的需要拦截的数据时,根据所述数据请求消息返回一个空白文件,作为所述数据请求消息所请求的数据。

10. 根据权利要求7所述的浏览器页面数据过滤装置,其特征在于,所述过滤单元包括第一过滤子单元和第二过滤子单元;

第一过滤子单元,用于利用所述应用程序编程接口中的钩子函数,确定所述数据请求消息即将请求的数据为预置的需要拦截的第一类数据时,阻止所述数据请求消息;

第二过滤子单元,用于利用所述应用程序编程接口中的钩子函数,确定所述数据请求消息即将请求的数据为预置的需要拦截的第二类数据时,根据所述数据请求消息返回一个空白文件,作为所述数据请求消息所请求的数据。

11. 根据权利要求10所述的浏览器页面数据过滤装置,其特征在于,

第一过滤子单元,具体用于利用所述应用程序编程接口中的钩子函数,确定所述数据请求消息即将请求的数据为广告链接且为非图片链接时,阻止所述数据请求消息;

第二过滤子单元,具体用于利用所述应用程序编程接口中的钩子函数,确定所述数据请求消息即将请求的数据为广告链接且为图片链接时,据所述数据请求消息返回一个空白图片文件,作为所述数据请求消息所请求的数据。

12. 根据权利要求7至11任一项所述的浏览器页面数据过滤装置,其特征在于,还包括通知单元;

通知单元,用于返回过滤结果给用户。

13. 一种通信系统,其特征在于,包括权利要求7至12任一项所述的浏览器页面数据过滤装置。

## 一种浏览器页面数据过滤方法、装置和系统

### 技术领域

[0001] 本发明涉及通信技术领域,具体涉及一种浏览器页面数据过滤方法、装置和系统。

### 背景技术

[0002] 浏览器(Browser),是万维网服务的客户端浏览程序,它可以通过向万维网服务器发送各种请求,然后对万维网服务器根据这些请求返回的数据,如超文本信息和各种多媒体数据进行解释、显示和播放。通过浏览器,用户可以浏览万维网服务的各种数据,比如网页、视频等等,在此过程中,除了用户自身需求的数据之外,往往还会夹杂有其他的一些数据,比如一些恶意网页广告或弹窗广告等,这些数据常常会对用户的浏览造成干扰,特别是一些投放不规范的网页广告或弹窗广告等,更会对用户造成骚扰,极大影响到用户的浏览体验,因此,如果对浏览器页面数据进行过滤,是一个值得关注的问题。

[0003] 在现有技术中,一般通过在浏览器中加载插件来实现对浏览器页面数据进行过滤,比如加载一个广告拦截插件,等等。但是,由于目前浏览器的种类较多,各种浏览器的特性也截然不同,因此,很难将同一种插件移植到不同的浏览器下,也就是说,针对不同的浏览器,一般需要开发不同的插件。

[0004] 在对现有技术的研究和实践过程中,本发明的发明人发现,由于现有方案中每个浏览器内核都需要额外地去维护一个插件,因此后期维护较为麻烦,而且需要针对不同的浏览器开发不同的插件,开发量也较大,实现不够灵活。

### 发明内容

[0005] 本发明实施例提供一种浏览器页面数据过滤方法、装置和系统,不仅无需后期维护,而且开发量较小,实现灵活。

[0006] 一种浏览器页面数据过滤方法,包括:

[0007] 接收用户通过浏览器发送的数据请求消息;

[0008] 根据所述数据请求消息调用对应的应用程序编程接口(API, Application Programming Interface),所述应用程序编程接口包括钩子(HOOK)函数;

[0009] 利用所述应用程序编程接口中的钩子函数,对所述数据请求消息进行过滤。

[0010] 一种浏览器页面数据过滤装置,包括:

[0011] 接收单元,用于接收用户通过浏览器发送的数据请求消息;

[0012] 调用单元,用于根据所述数据请求消息调用对应的应用程序编程接口,所述应用程序编程接口包括钩子函数;

[0013] 过滤单元,用于利用所述应用程序编程接口中的钩子函数,对所述数据请求消息进行过滤。

[0014] 一种通信系统,包括本发明实施例提供的任一种浏览器页面数据过滤装置。

[0015] 本发明实施例采用接收用户通过浏览器发送的数据请求消息,根据该数据请求消息调用对应的应用程序编程接口,其中,该应用程序编程接口包括钩子函数,利用该应用程

序编程接口中的钩子函数,对所述数据请求消息进行过滤;由于基本上所有浏览器在请求数据时都会使用应用程序编程接口,因此,该方案兼容性较好,不会存在兼容性问题,无需特意为不同的浏览器开发特定的插件,不仅无需后期维护,而且开发量较小,实现灵活。

### 附图说明

[0016] 为了更清楚地说明本发明实施例中的技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0017] 图 1 是本发明实施例提供的浏览器页面数据过滤方法的流程图;

[0018] 图 2a 是本发明实施例提供的浏览器页面数据过滤方法的场景示意图;

[0019] 图 2b 是本发明实施例提供的浏览器页面数据过滤方法的另一流程图;

[0020] 图 3 是本发明实施例提供的浏览器页面数据过滤方法的又一流程图;

[0021] 图 4 是本发明实施例提供的浏览器页面数据过滤方法的再一流程图;

[0022] 图 5 是本发明实施例提供的浏览器页面数据过滤装置的结构示意图;

[0023] 图 6 是本发明实施例提供的终端的结构示意图。

### 具体实施方式

[0024] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0025] 本发明实施例提供一种浏览器页面数据过滤方法、装置和系统。以下分别进行详细说明。

[0026] 实施例一、

[0027] 本发明实施例将从浏览器页面数据过滤装置的角度进行描述,该浏览器页面数据过滤装置具体可以集成在客户端中,该客户端可以装载在终端中,该终端具体可以为智能手机、平板电脑、电子书阅读器、MP3 播放器(Moving Picture Experts Group Audio Layer III,动态影像专家压缩标准音频层面 3)、MP4 (Moving Picture Experts Group Audio Layer IV,动态影像专家压缩标准音频层面 3) 播放器、膝上型便携计算机和台式计算机等等。

[0028] 一种浏览器页面数据过滤方法,包括:接收用户通过浏览器发送的数据请求消息;根据该数据请求消息调用对应的应用程序编程接口,其中,应用程序编程接口包括钩子(HOOK)函数;利用该应用程序编程接口中的 HOOK 函数,对该数据请求消息进行过滤。

[0029] 如图 1 所示,具体流程可以如下:

[0030] 101、接收用户通过浏览器发送的数据请求消息;其中,该数据请求消息可以请求网页展现各种资源文件。

[0031] 该数据请求消息具体可以为链接地址,比如统一资源定位符(URL, Uniform Resource Locator)等。

[0032] 102、根据步骤 101 中接收到的数据请求消息调用对应的应用程序编程接口(API, Application Programming Interface),比如 send 或 recv 等等。

[0033] 其中,应用程序编程接口包括 HOOK 函数,例如,具体可以在应用程序编程接口的代码的头部添加 HOOK 函数的代码。

[0034] 需说明的是,应用程序编程接口是一些预先定义的函数,其目的在于提供应用程序与开发人员基于某软件或硬件的以访问一组例程的能力,而又无需访问源码,或理解内部工作机制的细节。而 HOOK 函数是消息处理机制的一部分,通过设置“钩子”,应用程序可以各种消息和事件进行过滤,在此不再赘述。

[0035] 103、利用该应用程序编程接口中的 HOOK 函数,对该数据请求消息进行过滤。

[0036] 其中,过滤的方式可以有多种,比如,如果检测到该数据请求消息即将请求的数据为预置的需要拦截的数据时,则可以直接阻止该数据请求消息或者返回一个空白文件,以替换掉该数据请求消息原来所请求的数据,等等。例如,具体可以如下:

[0037] (1) 利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为预置的需要拦截的数据时,阻止该数据请求消息。

[0038] 其中,该需要拦截的数据可以根据实际应用的需求进行设置,比如,可以设置为广告链接、游戏链接或不明插件安装链接等等。

[0039] 例如,以广告拦截为例,当利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为广告链接时,则可以直接阻止该数据请求消息。

[0040] (2) 利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为预置的需要拦截的数据时,根据该数据请求消息返回一个空白文件,作为该数据请求消息所请求的数据。

[0041] 其中,该需要拦截的数据可根据以实际应用的需求进行设置,比如,可以设置为广告链接、游戏链接或不明插件安装链接等等。

[0042] 例如,以广告拦截为例,当利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为广告链接(比如 js 文件, swf 文件等)时,则可以根据该数据请求消息返回一个空白文件,作为该数据请求消息所请求的数据,即替换掉该数据请求消息原来所请求的广告数据,这样,浏览器就会以为已经下载到了该广告数据,从而起到拦截该广告数据的作用。

[0043] (3) 可选的,为了提高其灵活性和用户体验质量,还可以根据数据请求消息具体所请求的数据的类型而采用不同的过滤方式,例如,还可以如下方式来进行过滤:

[0044] A、利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为预置的需要拦截的第一类数据时,阻止该数据请求消息;

[0045] B、利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为预置的需要拦截的第二类数据时,根据该数据请求消息返回一个空白文件,作为该数据请求消息所请求的数据。

[0046] 其中,该需要拦截的数据可以根据实际应用的需求进行设置,比如,可以设置为广告链接、游戏链接或不明插件安装链接等等。

[0047] 例如,还是以广告拦截为例,其中,需要拦截的第一类数据可以设置为“广告链接且为非图片链接”,需要拦截的第二类数据可以设置为“广告链接且为图片链接”,则上述步

骤具体可以如下：

[0048] 利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为广告链接且为非图片链接时,阻止所述数据请求消息；

[0049] 利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为广告链接且为图片链接时,据所述数据请求消息返回一个空白图片文件,作为该数据请求消息所请求的数据,即用该空白图片文件替换掉该数据请求消息原来所请求的广告图片,这样,浏览器就会以为已经下载到了该广告图片,从而起到拦截该广告图片的作用。

[0050] 需说明的是,如果检测到该数据请求消息即将请求的数据不是预置的需要拦截的数据,则继续根据该数据请求消息获取需要请求的数据,在此不再赘述。

[0051] 此外,可选的,为了提高用户体验质量,还可以将过滤结果通知给用户,比如,可以告知用户过滤对象,过滤的详细信息等等。即在步骤“利用该应用程序编程接口中的 HOOK 函数,对该数据请求消息进行过滤”之后,该浏览器页面数据过滤方法还可以包括：

[0052] 返回过滤结果给用户。

[0053] 例如,以广告拦截为例,具体可以返回拦截结果和拦截的详细信息等过滤结果给用户,以使用户判断这些拦截是否合适,此后,用户还可以通过查看日志等方式来查看这些过滤结果,在此不再赘述。

[0054] 由上可知,本实施例采用接收用户通过浏览器发送的数据请求消息,根据该数据请求消息调用对应的应用程序编程接口,其中,该应用程序编程接口包括钩子函数,利用该应用程序编程接口中的钩子函数,对所述数据请求消息进行过滤;由于基本上所有浏览器在请求数据时都会使用应用程序编程接口,因此,该方案兼容性较好,不会存在兼容性问题,无需专门为不同的浏览器开发特定的插件,不仅无需后期维护,而且开发量较小,实现灵活。

[0055] 根据实施例一所描述的方法,以下将在实施例二、三和四中举例作进一步详细说明。

[0056] 实施例二、

[0057] 在本实施例中,将以广告拦截为例进行说明。

[0058] 如图 2a 所示,该浏览器页面数据过滤装置具体可以为客户端,比如浏览器,该客户端可以装载在终端中,该客户端可以包括浏览器注入模块、检测拦截模块和用户通知模块。在本实施例中,各个模块的功能可以如下：

[0059] (1) 浏览器注入模块；

[0060] 浏览器注入模块,主要用于在接收到浏览器的数据请求消息之后,立即暂停浏览器的请求,并将该数据请求消息转发给检测拦截模块,以确定该数据请求消息所请求的数据是否为一个广告的连接,并等待检测拦截模块返回检测结果,如果返回的检测结果指示该数据请求消息即将请求的数据是一个广告链接(比如 js 文件或 swf 文件)等,则直接阻止该数据请求消息。

[0061] (2) 检测拦截模块；

[0062] 检测拦截模块,主要用于接收浏览器注入模块转发的数据请求消息,比如 URL,然后调用对应的应用程序编程接口,利用广告规则库对该数据请求消息进行检测,以判断是否是一个广告链接,并返回检测结果给浏览器注入模块。

[0063] 需说明的是,由于判断的标准都在广告规则库里,因此在系统启动时,该检测拦截模块需要去解析广告规则库,以及探测该广告规则库的更新情况,即请求新的广告规则库,这样,才能更精确地对广告进行拦截。

[0064] 其中,广告规则库可以保存在服务端,由服务端进行维护,例如,具体可以在服务端设置一个“后台广告规则库搜集模块”,用于日常的 URL 源代码分析工作,提取这些 URL 里面的广告链接,生成广告规则下发到客户端供检测拦截模块使用。

[0065] (3) 用户通知模块;

[0066] 用户通知模块,主要用于在检测拦截模块拦截到广告之后,告知用户拦截结果和拦截的详细信息,以使用户判断这些拦截是否合适,此后,用户还可以通过查看日志等方式来查看这些拦截信息。

[0067] 基于上述客户端的结构,如图 2b 所示,一种浏览器页面数据过滤方法,具体流程可以如下:

[0068] 201、浏览器注入模块接收用户通过浏览器发送的数据请求消息,比如 URL 等,并将该数据请求消息转发给检测拦截模块。

[0069] 其中,该数据请求消息可以请求网页展现各种资源文件。

[0070] 例如,浏览器注入模块接收用户通过浏览器发送的数据请求消息后,立即暂停该数据请求消息的请求,并将该数据请求消息转发给检测拦截模块,以确定该数据请求消息所请求的数据是否为一个广告链接,并等待检测拦截模块返回检测结果。

[0071] 202、检测拦截模块根据步骤 201 中接收到的数据请求消息调用对应的应用程序编程接口。

[0072] 其中,应用程序编程接口包括 HOOK 函数,比如,具体可以在应用程序编程接口的代码的头部添加 HOOK 函数的代码。

[0073] 203、检测拦截模块利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据是否为广告链接,若是,则返回指示该数据请求消息即将请求的数据为广告链接的检测结果给浏览器注入模块;若否,则返回指示该数据请求消息即将请求的数据不是广告链接的检测结果给浏览器注入模块。

[0074] 204、浏览器注入模块接收检测结果,若该检测结果指示该数据请求消息即将请求的数据为广告链接,则直接阻止该数据请求消息,此时,还可以将该拦截结果和拦截的详细信息发送给用户通知模块;否则,若该检测结果指示该数据请求消息即将请求的数据不是广告链接,则继续执行该数据请求消息的请求。

[0075] 205、可选的,用户通知模块可以接收浏览器注入模块发送的拦截结果和拦截的详细信息,并将该拦截结果和拦截的详细信息通知给用户,以使用户判断这些拦截是否合适。

[0076] 此后,用户还可以通过查看日志等方式来查看这些拦截信息。

[0077] 由上可知,由上可知,本实施例采用接收用户通过浏览器发送的数据请求消息,根据该数据请求消息调用对应的应用程序编程接口,其中,该应用程序编程接口包括钩子函数,利用该应用程序编程接口中的钩子函数,确定该数据请求消息即将请求的数据为广告链接时,直接阻止该数据请求消息,从而实现对广告的拦截;由于基本上所有浏览器在请求数据时都会使用应用程序编程接口,因此,该方案兼容性较好,不会存在兼容性问题,无需特意为不同的浏览器开发特定的广告拦截插件,不仅无需后期维护,而且开发量较小,实现



灵活。

[0078] 实施例三、

[0079] 与实施例二相同的是,在本实施例中,同样以广告拦截为例进行说明。与实施二不同的是,在实施例二中,当发现数据请求消息所请求的数据为广告链接时,采用的是直接阻止该数据请求消息的方式,而在本实施例中,将采用另一种方式,即根据该数据请求消息返回一个空白文件,作为该数据请求消息所请求的数据,以下将进行详细说明。

[0080] 与实施例二中的客户端结构相同,如图 2a 所示,该客户端可以包括浏览器注入模块、检测拦截模块和用户通知模块。在本实施例中,各个模块的功能可以如下:

[0081] (1) 浏览器注入模块;

[0082] 浏览器注入模块,主要用于在接收到浏览器的数据请求消息之后,立即暂停浏览器的请求,并将该数据请求消息转发给检测拦截模块,以确定该数据请求消息所请求的数据是否为一个广告链接,并等待检测拦截模块返回检测结果,如果返回的检测结果指示该数据请求消息即将请求的数据是一个广告链接(比如 js 文件或 swf 文件)等,则返回一个数据量较小的空白文件给浏览器,作为该数据请求消息所请求的数据。

[0083] (2) 检测拦截模块;

[0084] 检测拦截模块,主要用于接收浏览器注入模块转发的数据请求消息,比如 URL,然后调用对应的应用程序编程接口,利用广告规则库对该数据请求消息进行检测,以判断是否是一个广告链接,并返回检测结果给浏览器注入模块。

[0085] 需说明的是,由于判断的标准都在广告规则库里,因此在系统启动时,该检测拦截模块需要去解析广告规则库,以及探测该广告规则库的更新情况,即请求新的广告规则库,这样,才能更精确地对广告进行拦截。

[0086] 其中,广告规则库可以保存在服务端,由服务端进行维护,例如,具体可以在服务端设置一个“后台广告规则库搜集模块”,用于日常的 URL 源代码分析工作,提取这些 URL 里面的广告链接,生成广告库规则下发到客户端供检测拦截模块使用。

[0087] (3) 用户通知模块;

[0088] 用户通知模块,主要用于在检测拦截模块拦截到广告之后,告知用户拦截结果和拦截的详细信息,以使用户判断这些拦截是否合适,此后,用户还可以通过查看日志等方式来查看这些拦截信息。

[0089] 基于上述客户端的结构,如图 3 所示,一种浏览器页面数据过滤方法,具体流程可以如下:

[0090] 301、浏览器注入模块接收用户通过浏览器发送的数据请求消息,比如 URL 等,并将该数据请求消息转发给检测拦截模块。

[0091] 其中,该数据请求消息可以请求网页展现各种资源文件。

[0092] 例如,浏览器注入模块接收用户通过浏览器发送的数据请求消息后,立即暂停该数据请求消息的请求,并将该数据请求消息转发给检测拦截模块,以确定该数据请求消息所请求的数据是否为一个广告链接,并等待检测拦截模块返回检测结果。

[0093] 302、检测拦截模块根据步骤 301 中接收到的数据请求消息调用对应的应用程序编程接口。

[0094] 其中,应用程序编程接口包括 HOOK 函数,比如,具体可以在应用程序编程接口的

代码的头部添加 HOOK 函数的代码。

[0095] 303、检测拦截模块利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据是否为广告链接,若是,则返回指示该数据请求消息即将请求的数据为广告链接的检测结果显示给浏览器注入模块;若否,则返回指示该数据请求消息即将请求的数据不是广告链接的检测结果显示给浏览器注入模块。

[0096] 304、浏览器注入模块接收检测结果,若该检测结果指示该数据请求消息即将请求的数据为广告链接,则返回一个数据量较小的空白文件(比如具体可以是一个空白的图片文件)给浏览器,以作为该数据请求消息所请求的数据,此时,还可以将该拦截结果和拦截的详细信息发送给用户通知模块;否则,若该检测结果指示该数据请求消息即将请求的数据不是广告链接,则继续执行该数据请求消息的请求。

[0097] 305、可选的,用户通知模块可以接收浏览器注入模块发送的拦截结果和拦截的详细信息,并将该拦截结果和拦截的详细信息通知给用户,以使用户判断这些拦截是否合适。

[0098] 此后,用户还可以通过查看日志等方式来查看这些拦截信息。

[0099] 由上可知,由上可知,本实施例采用接收用户通过浏览器发送的数据请求消息,根据该数据请求消息调用对应的应用程序编程接口,其中,该应用程序编程接口包括钩子函数,利用该应用程序编程接口中的钩子函数,确定该数据请求消息即将请求的数据为广告链接时,返回一个空白的文件给浏览器,以替换掉原数据请求消息所要请求的数据,从而实现拦截广告的目的;由于基本上所有浏览器在请求数据时都会使用应用程序编程接口,因此,该方案兼容性较好,不会存在兼容性问题,无需特意为不同的浏览器开发特定的广告拦截插件,不仅无需后期维护,而且开发量较小,实现灵活。

[0100] 实施例四、

[0101] 在实施例二和三的基础上,进一步的,为了提高其灵活性和用户体验质量,还可以根据数据请求消息具体所请求的数据的类型而采用不同的过滤方式,以下将同样以广告拦截为例作详细说明。

[0102] 与实施例二和三中的客户端结构相同,如图 2a 所示,该客户端可以包括浏览器注入模块、检测拦截模块和用户通知模块。在本实施例中,各个模块的功能可以如下:

[0103] (1) 浏览器注入模块;

[0104] 浏览器注入模块,主要用于在接收到浏览器的数据请求消息之后,立即暂停浏览器的请求,并将该数据请求消息转发给检测拦截模块,以确定该数据请求消息所请求的数据是否为一个广告链接,并等待检测拦截模块返回检测结果,如果返回的检测结果指示该数据请求消息即将请求的数据是一个广告链接且为非图片链接,则直接阻止该数据请求消息;而如果返回的检测结果指示该数据请求消息即将请求的数据是一个广告链接且为图片链接,则返回一个数据量较小的空白图片文件给浏览器,作为该数据请求消息所请求的数据。

[0105] (2) 检测拦截模块;

[0106] 检测拦截模块,主要用于接收浏览器注入模块转发的数据请求消息,比如 URL,然后调用对应的应用程序编程接口,利用广告规则库对该数据请求消息进行检测,以判断是否是一个广告链接,且确定该广告链接的类型,比如是图片链接还是非图片链接等,然后返回检测结果给浏览器注入模块。

[0107] 需说明的是,由于判断的标准都在广告规则库里,因此在系统启动时,该检测拦截模块需要去解析广告规则库,以及探测该广告规则库的更新情况,即请求新的广告规则库,这样,才能更精确地对广告进行拦截。

[0108] 其中,广告规则库可以保存在服务端,由服务端进行维护,例如,具体可以在服务端设置一个“后台广告规则库搜集模块”,用于日常的 URL 源代码分析工作,提取这些 URL 里面的广告链接,生成广告库规则下发到客户端供检测拦截模块使用。

[0109] (3) 用户通知模块;

[0110] 用户通知模块,主要用于在检测拦截模块拦截到广告之后,告知用户拦截结果和拦截的详细信息,以使用户判断这些拦截是否合适,此后,用户还可以通过查看日志等方式来查看这些拦截信息。

[0111] 基于上述客户端的结构,如图 4 所示,一种浏览器页面数据过滤方法,具体流程可以如下:

[0112] 401、浏览器注入模块接收用户通过浏览器发送的数据请求消息,比如 URL 等,并将该数据请求消息转发给检测拦截模块。

[0113] 其中,该数据请求消息可以请求网页展现各种资源文件。

[0114] 例如,浏览器注入模块接收用户通过浏览器发送的数据请求消息后,立即暂停该数据请求消息的请求,并将该数据请求消息转发给检测拦截模块,以确定该数据请求消息所请求的数据是否为一个广告链接,并等待检测拦截模块返回检测结果。

[0115] 402、检测拦截模块根据步骤 401 中接收到的数据请求消息调用对应的应用程序编程接口。

[0116] 其中,应用程序编程接口包括 HOOK 函数,比如,具体可以在应用程序编程接口的代码的头部添加 HOOK 函数的代码。

[0117] 403、检测拦截模块利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据是否为广告链接,若是,则返回指示该数据请求消息即将请求的数据为广告链接的检测结果给浏览器注入模块,并在该检测结果中指示该广告链接的类型,比如是图片链接或非图片链接等;若否,则返回指示该数据请求消息即将请求的数据不是广告链接的检测结果给浏览器注入模块。

[0118] 404、浏览器注入模块接收检测结果,若该检测结果指示该数据请求消息即将请求的数据为广告链接且为非图片链接,则直接阻止该数据请求消息;若该检测结果指示该数据请求消息即将请求的数据为广告链接且为图片链接,则返回一个数据量较小的空白图片文件给浏览器,以作为该数据请求消息所请求的数据;此时,还可以将该拦截结果和拦截的详细信息发送给用户通知模块;否则,若该检测结果指示该数据请求消息即将请求的数据不是广告链接,则继续执行该数据请求消息的请求。

[0119] 405、可选的,用户通知模块可以接收浏览器注入模块发送的拦截结果和拦截的详细信息,并将该拦截结果和拦截的详细信息通知给用户,以使用户判断这些拦截是否合适。

[0120] 此后,用户还可以通过查看日志等方式来查看这些拦截信息。

[0121] 由上可知,由上可知,本实施例采用接收用户通过浏览器发送的数据请求消息,根据该数据请求消息调用对应的应用程序编程接口,其中,该应用程序编程接口包括钩子函数,利用该应用程序编程接口中的钩子函数,确定该数据请求消息即将请求的数据为广告

链接且为非图片链接时,直接阻止该数据请求消息,而确定该数据请求消息即将请求的数据为广告链接且为图片链接时,则返回一个空白的文件给浏览器,以替换掉原数据请求消息所要请求的数据,从而实现对拦截广告的目的;由于基本上所有浏览器在请求数据时都会使用应用程序编程接口,因此,该方案兼容性较好,不会存在兼容性问题,无需特意在不同的浏览器开发特定的广告拦截插件,不仅无需后期维护,而且开发量较小,实现灵活。

[0122] 进一步的,由于该方案可以根据数据请求消息具体所请求的数据的类型而采用不同的过滤方式,所以可以更好地提高灵活性和用户体验质量。

[0123] 实施例五、

[0124] 为了更好地实现以上方法,本发明实施例还提供一种浏览器页面数据过滤装置,如图 5 所示,该浏览器页面数据过滤装置包括接收单元 501、调用单元 502 和过滤单元 503;

[0125] 接收单元 501,用于接收用户通过浏览器发送的数据请求消息;

[0126] 该数据请求消息具体可以为链接地址,比如 URL 等。

[0127] 调用单元 502,用于根据接收单元 501 接收到的数据请求消息调用对应的应用程序编程接口,比如调用 send 或 recv 等等;

[0128] 其中,应用程序编程接口包括 HOOK 函数,例如,具体可以在应用程序编程接口的代码的头部添加 HOOK 函数的代码。

[0129] 过滤单元 503,用于利用调用单元 502 调用的应用程序编程接口中的钩子函数,对该数据请求消息进行过滤。

[0130] 其中,过滤的方式可以有多种,比如,如果检测到该数据请求消息即将请求的数据为预置的需要拦截的数据时,则可以直接阻止该数据请求消息或者返回一个空白文件,以替换掉该数据请求消息原来所请求的数据,等等。例如,具体可以如下:

[0131] 过滤单元 503,具体可以用于利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为预置的需要拦截的数据时,阻止该数据请求消息。

[0132] 其中,该需要拦截的数据可以根据实际应用的需求进行设置,比如,可以设置为广告链接、游戏链接或不明插件安装链接等等。

[0133] 例如,以广告拦截为例,当过滤单元 503 利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为广告链接时,则可以直接阻止该数据请求消息。

[0134] 或者,过滤单元 503,具体可以用于利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为预置的需要拦截的数据时,根据该数据请求消息返回一个空白文件,作为该数据请求消息所请求的数据。

[0135] 其中,该需要拦截的数据可根据以实际应用的需求进行设置,比如,可以设置为广告链接、游戏链接或不明插件安装链接等等。

[0136] 例如,以广告拦截为例,当过滤单元 503 利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为广告链接(比如 js 文件, swf 文件等)时,则可以根据该数据请求消息返回一个空白文件,作为该数据请求消息所请求的数据,即替换掉该数据请求消息原来所请求的广告数据,这样,浏览器就会以为已经下载到了该广告数据,从而起到拦截该广告数据的作用。

[0137] 可选的,为了提高其灵活性和用户体验质量,还可以根据数据请求消息具体所请求的数据的类型而采用不同的过滤方式,即,过滤单元 503 可以包括第一过滤子单元和第

二过滤子单元；

[0138] 第一过滤子单元,用于利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为预置的需要拦截的第一类数据时,阻止该数据请求消息；

[0139] 第二过滤子单元,用于利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为预置的需要拦截的第二类数据时,根据该数据请求消息返回一个空白文件,作为该数据请求消息所请求的数据。

[0140] 其中,该需要拦截的数据可以根据实际应用的需求进行设置,比如,可以设置为广告链接、游戏链接或不明插件安装链接等等。

[0141] 例如,还是以广告拦截为例,其中,需要拦截的第一类数据可以设置为“广告链接且为非图片链接”,需要拦截的第二类数据可以设置为“广告链接且为图片链接”,则：

[0142] 第一过滤子单元,具体用于利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为广告链接且为非图片链接时,阻止所述数据请求消息；

[0143] 第二过滤子单元,具体用于利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为广告链接且为图片链接时,据所述数据请求消息返回一个空白图片文件,作为该数据请求消息所请求的数据,即用该空白图片文件替换掉该数据请求消息原来所请求的广告图片,这样,浏览器就会以为已经下载到了该广告图片,从而起到拦截该广告图片的作用。

[0144] 需说明的是,如果检测到该数据请求消息即将请求的数据不是预置的需要拦截的数据,则过滤单元 503 可以继续根据该数据请求消息获取需要请求的数据,在此不再赘述。

[0145] 此外,可选的,为了提高用户体验质量,还可以将过滤结果通知给用户,比如,可以告知用户过滤对象,过滤的详细信息等等。即该浏览器页面数据过滤装置还可以包括通知单元；

[0146] 通知单元,用于返回过滤结果给用户。

[0147] 例如,以广告拦截为例,通知单元具体可以用于返回拦截结果和拦截的详细信息等过滤结果给用户,以使用户判断这些拦截是否合适,此后,用户还可以通过查看日志等方式来查看这些过滤结果,在此不再赘述。

[0148] 具体实施时,以上各个单元可以作为独立实体来实现,也可以进行任意组合,作为同一或若干个实体来实现,比如以实施例二、三和四中的浏览器注入模块、检测拦截模块和用户通知模块的形式来实现,等等,在此不再赘述。

[0149] 该浏览器页面数据过滤装置具体可以集成在客户端中,该客户端可以装载在终端中,该终端具体可以为智能手机、平板电脑、电子书阅读器、MP3 播放器、MP4 播放器、膝上型便携计算机和台式计算机等等。

[0150] 由上可知,本实施例的浏览器页面数据过滤装置中的接收单元 501 可以接收用户通过浏览器发送的数据请求消息,并由调用单元 502 根据该数据请求消息调用对应的应用程序编程接口,其中,该应用程序编程接口包括钩子函数,然后由过滤单元 503 利用该应用程序编程接口中的钩子函数,对该数据请求消息进行过滤；由于基本上所有浏览器在请求数据时都会使用应用程序编程接口,因此,该方案兼容性较好,不会存在兼容性问题,无需特意为不同的浏览器开发特定的插件,不仅无需后期维护,而且开发量较小,实现灵活。

[0151] 实施例六、

[0152] 相应的,本发明实施例还提供一种通信系统,包括本发明实施例提供的任一种浏览器页面数据过滤装置,其中,该浏览器页面数据过滤装置具体可参见实施例五,例如,该浏览器页面数据过滤装置具体可以集成在客户端中,如下:

[0153] 客户端,用于接收用户通过浏览器发送的数据请求消息;根据该数据请求消息调用对应的应用程序编程接口,其中,应用程序编程接口包括 HOOK 函数;利用该应用程序编程接口中的 HOOK 函数,对该数据请求消息进行过滤,具体可参见前面的实施例,在此不再赘述。

[0154] 此外,该通信系统还可以包括服务端,如下:

[0155] 服务端,用于为客户端提供过滤的规则。

[0156] 则客户端,具体可以用于从服务端获取过滤规则,利用该应用程序编程接口中的 HOOK 函数,按照该过滤规则对该数据请求消息进行过滤。

[0157] 比如,以广告拦截为例,该服务端可以保存和维护广告规则库,并将该广告规则库提供给客户端使用,而客户端,则可以利用调用的应用程序编程接口中的 HOOK 函数,根据广告规则库对数据请求消息进行检测,以确定该数据请求消息即将请求的数据是否为广告链接,并根据检测结果对该数据请求消息进行处理,具体可参见前面的实施例,在此不再赘述。

[0158] 该通信系统可以实现本发明实施例所提供的浏览器页面数据过滤装置同样的有益效果,在此不再赘述。

[0159] 实施例七、

[0160] 相应的,本发明实施例还提供一种终端,如图 6 所示,该终端可以包括射频(RF, Radio Frequency)电路 601、包括有一个或一个以上计算机可读存储介质的存储器 602、输入单元 603、显示单元 604、传感器 605、音频电路 606、无线保真(WiFi, Wireless Fidelity)模块 607、包括有一个或者一个以上处理核心的处理器 608、以及电源 609 等部件。本领域技术人员可以理解,图 6 中示出的终端结构并不构成对终端的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件布置。其中:

[0161] RF 电路 601 可用于收发信息或通话过程中,信号的接收和发送,特别地,将基站的下行信息接收后,交由一个或者一个以上处理器 608 处理;另外,将涉及上行的数据发送给基站。通常,RF 电路 601 包括但不限于天线、至少一个放大器、调谐器、一个或多个振荡器、用户身份模块(SIM, Subscriber Identity Module)卡、收发信机、耦合器、低噪声放大器(LNA, Low Noise Amplifier)、双工器等。此外,RF 电路 601 还可以通过无线通信与网络和其他设备通信。所述无线通信可以使用任一通信标准或协议,包括但不限于全球移动通讯系统(GSM, Global System of Mobile communication)、通用分组无线服务(GPRS, General Packet Radio Service)、码分多址(CDMA, Code Division Multiple Access)、宽带码分多址(WCDMA, Wideband Code Division Multiple Access)、长期演进(LTE, Long Term Evolution)、电子邮件、短消息服务(SMS, Short Messaging Service)等。

[0162] 存储器 602 可用于存储软件程序以及模块,处理器 608 通过运行存储在存储器 602 的软件程序以及模块,从而执行各种功能应用以及数据处理。存储器 602 可主要包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需的应用程序(比如声音播放功能、图像播放功能等)等;存储数据区可存储根据终端的使用所创建的

数据(比如音频数据、电话本等)等。此外,存储器 602 可以包括高速随机存取存储器,还可以包括非易失性存储器,例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。相应地,存储器 602 还可以包括存储器控制器,以提供处理器 608 和输入单元 603 对存储器 602 的访问。

[0163] 输入单元 603 可用于接收输入的数字或字符信息,以及产生与用户设置以及功能控制有关的键盘、鼠标、操作杆、光学或者轨迹球信号输入。具体地,在一个具体的实施例中,输入单元 603 可包括触敏表面以及其他输入设备。触敏表面,也称为触摸显示屏或者触控板,可收集用户在其上或附近的触摸操作(比如用户使用手指、触笔等任何适合的物体或附件在触敏表面上或在触敏表面附近的操作),并根据预先设定的程式驱动相应的连接装置。可选的,触敏表面可包括触摸检测装置和触摸控制器两个部分。其中,触摸检测装置检测用户的触摸方位,并检测触摸操作带来的信号,将信号传送给触摸控制器;触摸控制器从触摸检测装置上接收触摸信息,并将它转换成触点坐标,再送给处理器 608,并能接收处理器 608 发来的命令并加以执行。此外,可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触敏表面。除了触敏表面,输入单元 603 还可以包括其他输入设备。具体地,其他输入设备可以包括但不限于物理键盘、功能键(比如音量控制按键、开关按键等)、轨迹球、鼠标、操作杆等中的一种或多种。

[0164] 显示单元 604 可用于显示由用户输入的信息或提供给用户的信息以及终端的各种图形用户接口,这些图形用户接口可以由图形、文本、图标、视频和其任意组合来构成。显示单元 604 可包括显示面板,可选的,可以采用液晶显示器(LCD, Liquid Crystal Display)、有机发光二极管(OLED, Organic Light-Emitting Diode)等形式来配置显示面板。进一步的,触敏表面可覆盖显示面板,当触敏表面检测到在其上或附近的触摸操作后,传送给处理器 608 以确定触摸事件的类型,随后处理器 608 根据触摸事件的类型在显示面板上提供相应的视觉输出。虽然在图 6 中,触敏表面与显示面板是作为两个独立的部件来实现输入和输出功能,但是在某些实施例中,可以将触敏表面与显示面板集成而实现输入和输出功能。

[0165] 终端还可包括至少一种传感器 605,比如光传感器、运动传感器以及其他传感器。具体地,光传感器可包括环境光传感器及接近传感器,其中,环境光传感器可根据环境光线的明暗来调节显示面板的亮度,接近传感器可在终端移动到耳边时,关闭显示面板和/或背光。作为运动传感器的一种,重力加速度传感器可检测各个方向上(一般为三轴)加速度的大小,静止时可检测出重力的大小及方向,可用于识别手机姿态的应用(比如横竖屏切换、相关游戏、磁力计姿态校准)、振动识别相关功能(比如计步器、敲击)等;至于终端还可配置的陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器,在此不再赘述。

[0166] 音频电路 606、扬声器,传声器可提供用户与终端之间的音频接口。音频电路 606 可将接收到的音频数据转换后的电信号,传输到扬声器,由扬声器转换为声音信号输出;另一方面,传声器将收集的声音信号转换为电信号,由音频电路 606 接收后转换为音频数据,再将音频数据输出处理器 608 处理后,经 RF 电路 601 以发送给比如另一终端,或者将音频数据输出至存储器 602 以便进一步处理。音频电路 606 还可能包括耳塞插孔,以提供外设耳机与终端的通信。

[0167] WiFi 属于短距离无线传输技术,终端通过 WiFi 模块 607 可以帮助用户收发电子邮

件、浏览网页和访问流式媒体等,它为用户提供了无线的宽带互联网访问。虽然图 6 示出了 WiFi 模块 607,但是可以理解的是,其并不属于终端的必须构成,完全可以根据需要在不改变发明的本质的范围内而省略。

[0168] 处理器 608 是终端的控制中心,利用各种接口和线路连接整个手机的各个部分,通过运行或执行存储在存储器 602 内的软件程序和 / 或模块,以及调用存储在存储器 602 内的数据,执行终端的各种功能和处理数据,从而对手机进行整体监控。可选的,处理器 608 可包括一个或多个处理核心;优选的,处理器 608 可集成应用处理器和调制解调处理器,其中,应用处理器主要处理操作系统、用户界面和应用程序等,调制解调处理器主要处理无线通信。可以理解的是,上述调制解调处理器也可以不集成到处理器 608 中。

[0169] 终端还包括给各个部件供电的电源 609 (比如电池),优选的,电源可以通过电源管理系统与处理器 608 逻辑相连,从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。电源 609 还可以包括一个或一个以上的直流或交流电源、再充电系统、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。

[0170] 尽管未示出,终端还可以包括摄像头、蓝牙模块等,在此不再赘述。具体在本实施例中,终端中的处理器 608 会按照如下的指令,将一个或一个以上的应用程序的进程对应的可执行文件加载到存储器 602 中,并由处理器 608 来运行存储在存储器 602 中的应用程序,从而实现各种功能:

[0171] 尽管未示出,终端还可以包括摄像头、蓝牙模块等,在此不再赘述。具体在本实施例中,终端的显示单元是触摸屏显示器,终端还包括有存储器,以及一个或者一个以上的程序,其中一个或者一个以上程序存储于存储器中,且经配置以由一个或者一个以上处理器执行述一个或者一个以上程序包含用于进行以下操作的指令:

[0172] 接收用户通过浏览器发送的数据请求消息;根据该数据请求消息调用对应的应用程序编程接口,其中,应用程序编程接口包括 HOOK 函数;利用该应用程序编程接口中的 HOOK 函数,对该数据请求消息进行过滤。

[0173] 其中,过滤的方式可以有多种,比如,如果检测到该数据请求消息即将请求的数据为预置的需要拦截的数据时,则可以直接阻止该数据请求消息或者返回一个空白文件,以替换掉该数据请求消息原来所请求的数据,等等。例如,具体可以如下:

[0174] (1) 利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为预置的需要拦截的数据时,阻止该数据请求消息。

[0175] 其中,该需要拦截的数据可以根据实际应用的需求进行设置,比如,可以设置为广告链接、游戏链接或不明插件安装链接等等。

[0176] 例如,以广告拦截为例,当利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为广告链接时,则可以直接阻止该数据请求消息。

[0177] (2) 利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为预置的需要拦截的数据时,根据该数据请求消息返回一个空白文件,作为该数据请求消息所请求的数据。

[0178] 其中,该需要拦截的数据可根据以实际应用的需求进行设置,比如,可以设置为广告链接、游戏链接或不明插件安装链接等等。

[0179] 例如,以广告拦截为例,当利用该应用程序编程接口中的 HOOK 函数,确定该数据



请求消息即将请求的数据为广告链接(比如 js 文件, swf 文件等)时,则可以根据该数据请求消息返回一个空白文件,作为该数据请求消息所请求的数据,即替换掉该数据请求消息原来所请求的广告数据,这样,浏览器就会以为已经下载到了该广告数据,从而起到拦截该广告数据的作用。

[0180] (3)可选的,为了提高其灵活性和用户体验质量,还可以根据数据请求消息具体所请求的数据的类型而采用不同的过滤方式,例如,还可以如下方式来进行过滤:

[0181] A、利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为预置的需要拦截的第一类数据时,阻止该数据请求消息;

[0182] B、利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为预置的需要拦截的第二类数据时,根据该数据请求消息返回一个空白文件,作为该数据请求消息所请求的数据。

[0183] 其中,该需要拦截的数据可以根据实际应用的需求进行设置,比如,可以设置为广告链接、游戏链接或不明插件安装链接等等。

[0184] 例如,还是以广告拦截为例,其中,需要拦截的第一类数据可以设置为“广告链接且为非图片链接”,需要拦截的第二类数据可以设置为“广告链接且为图片链接”,则上述步骤具体可以如下:

[0185] 利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为广告链接且为非图片链接时,阻止所述数据请求消息;

[0186] 利用该应用程序编程接口中的 HOOK 函数,确定该数据请求消息即将请求的数据为广告链接且为图片链接时,据所述数据请求消息返回一个空白图片文件,作为该数据请求消息所请求的数据,即用该空白图片文件替换掉该数据请求消息原来所请求的广告图片,这样,浏览器就会以为已经下载到了该广告图片,从而起到拦截该广告图片的作用。

[0187] 需说明的是,如果检测到该数据请求消息即将请求的数据不是预置的需要拦截的数据,则继续根据该数据请求消息获取需要请求的数据,在此不再赘述。

[0188] 此外,可选的,还可以返回过滤结果给用户,例如,以广告拦截为例,具体可以返回拦截结果和拦截的详细信息等过滤结果给用户,以使用户判断这些拦截是否合适,此后,用户还可以通过查看日志等方式来查看这些过滤结果,在此不再赘述。

[0189] 由上可知,本实施例的终端采用接收用户通过浏览器发送的数据请求消息,根据该数据请求消息调用对应的应用程序编程接口,其中,该应用程序编程接口包括钩子函数,利用该应用程序编程接口中的钩子函数,对所述数据请求消息进行过滤;由于基本上所有浏览器在请求数据时都会使用应用程序编程接口,因此,该方案兼容性较好,不会存在兼容性问题,无需特意为不同的浏览器开发特定的插件,不仅无需后期维护,而且开发量较小,实现灵活。

[0190] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通程序来指令相关的硬件来完成,该程序可以存储于一计算机可读存储介质中,存储介质可以包括:只读存储器(ROM, Read Only Memory)、随机存取记忆体(RAM, Random Access Memory)、磁盘或光盘等。

[0191] 以上对本发明实施例所提供的一种浏览器页面数据过滤方法、装置和系统进行了详细介绍,本文中应用了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的

说明只是用于帮助理解本发明的方法及其核心思想 ;同时,对于本领域的技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

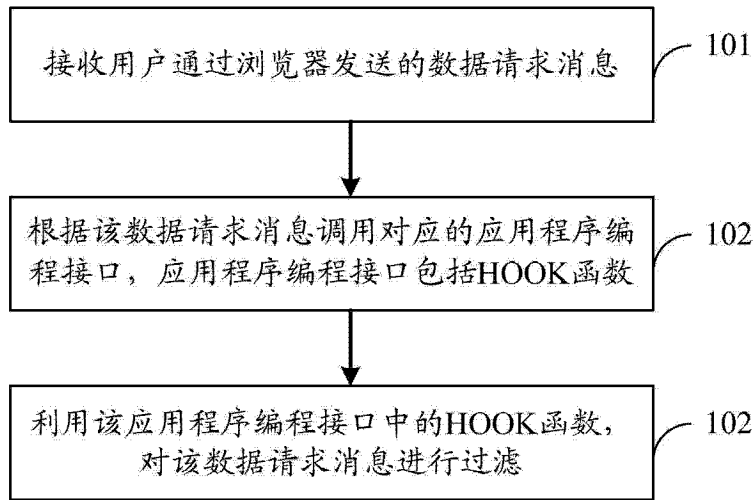


图 1

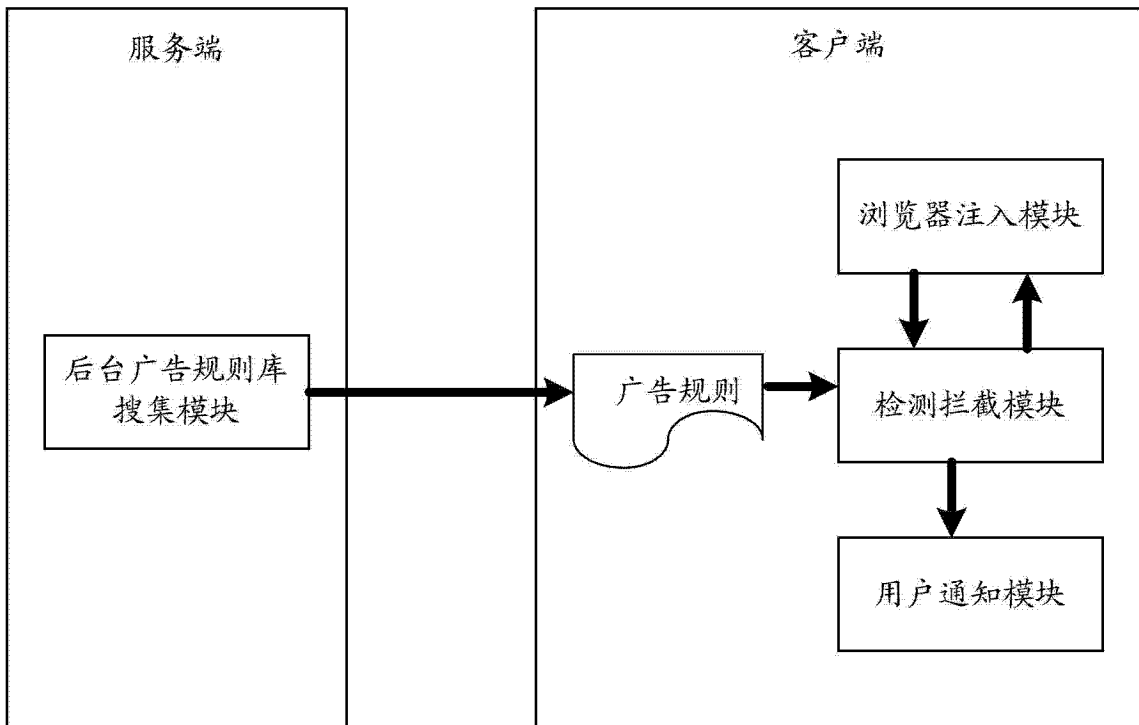


图 2a

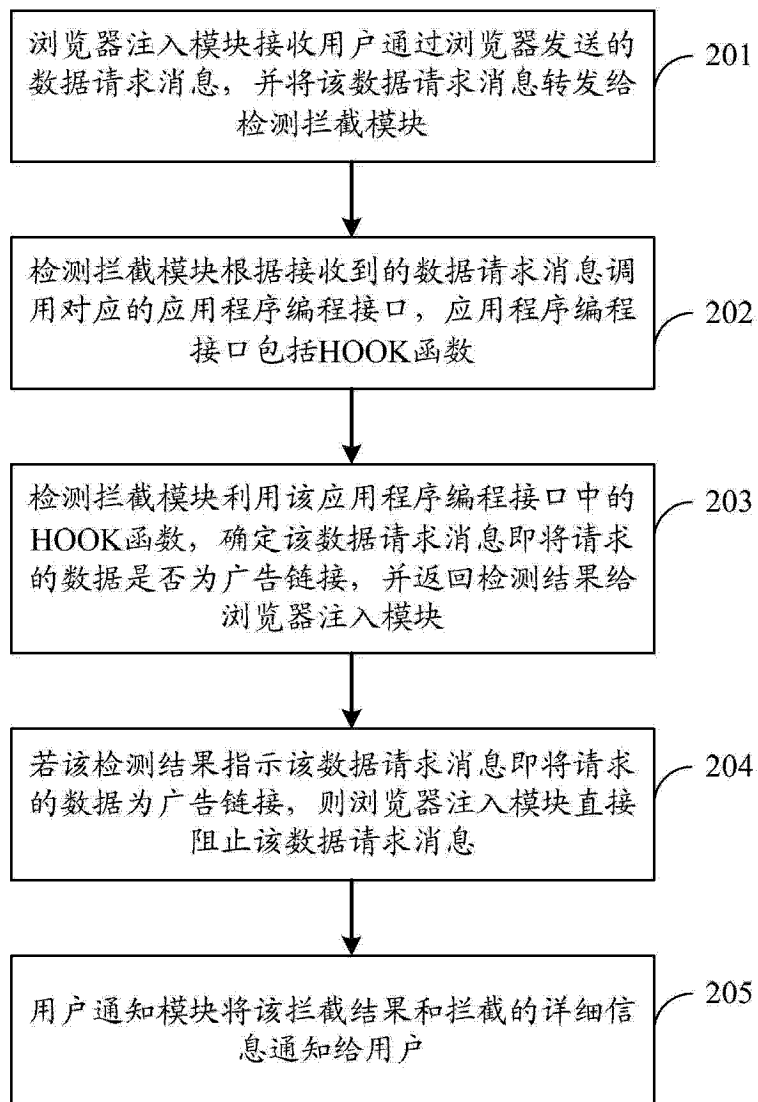


图 2b

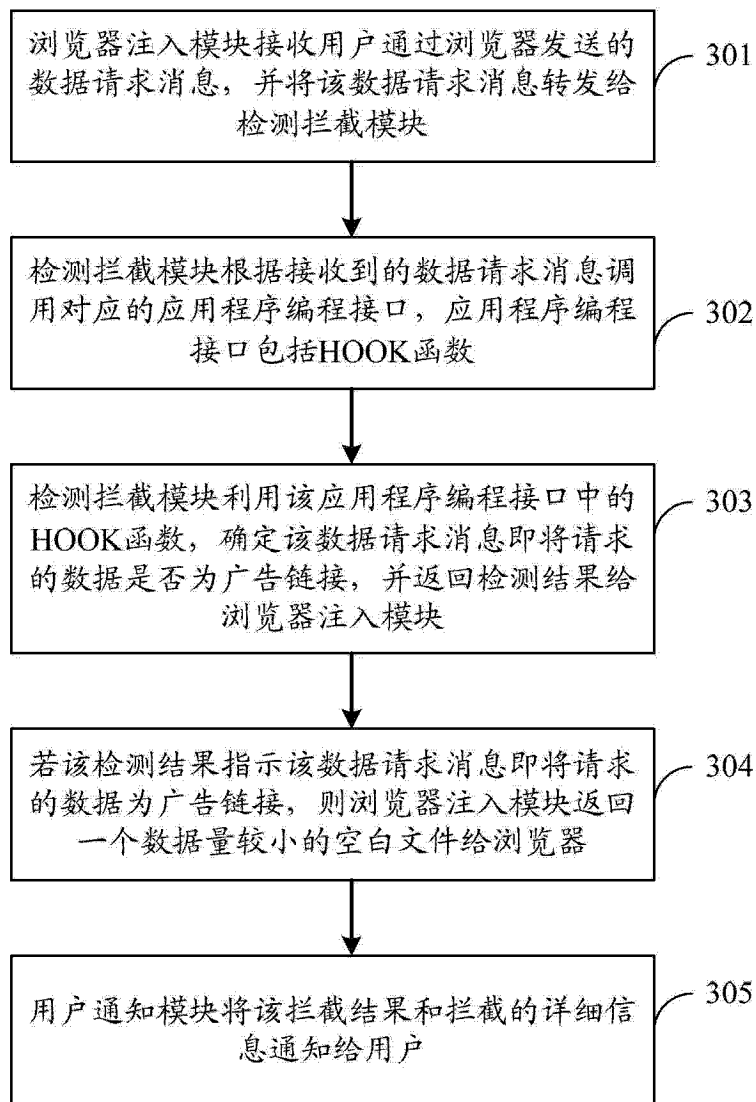


图 3

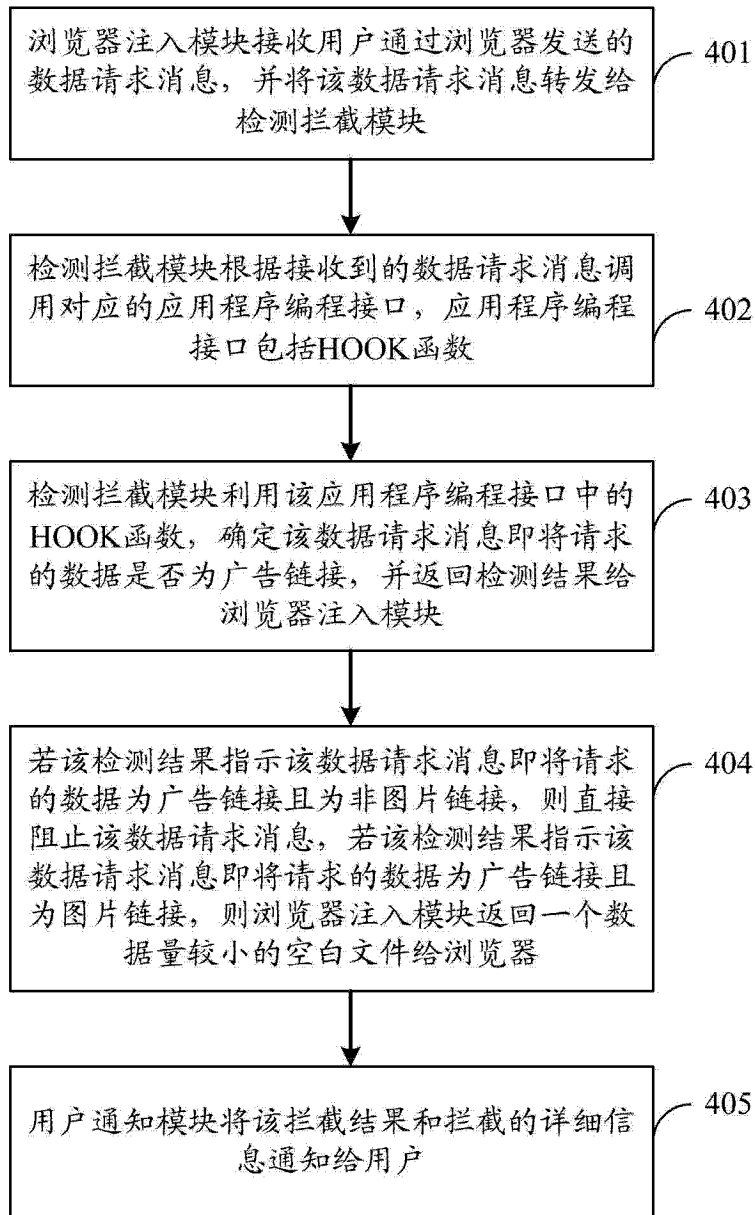


图 4



图 5

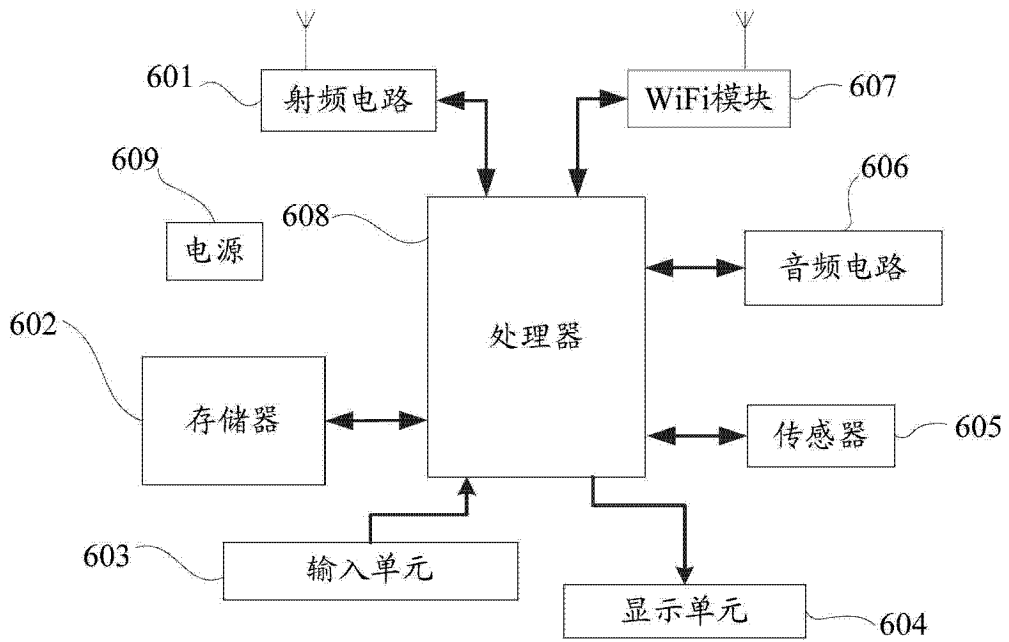


图 6