(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103605924 B
(45)授权公告日 2016.08.24

(21)申请号 201310625876.0

(22)申请日 2013.11.28

(73)专利权人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
专利权人 奇智软件(北京)有限公司

(72)发明人 张聪 肖鹏 孙晓骏

(74)专利代理机构 北京市浩天知识产权代理事务所(普通合伙) 11276
代理人 宋菲 刘兰兰

(51)Int.Cl.
G06F 21/56(2013.01)

(56)对比文件

CN 102999718 A,2013.03.27,说明书第2页第6段-第4页第8段,图1-7.
CN 102663289 A,2012.09.12,全文.
CN 103034807 A,2013.04.10,全文.
WO 2012022225 A1,2012.02.23,全文.
US 2013205396 A1,2013.08.08,全文.

审查员 赵洋

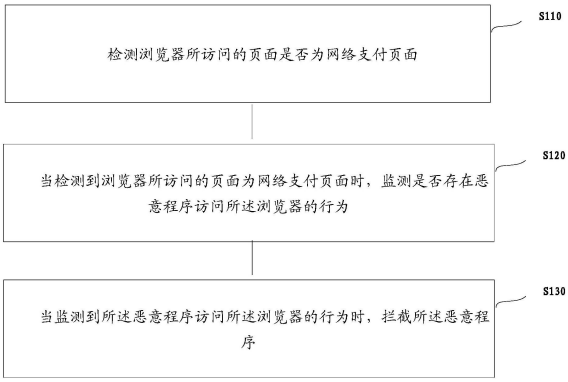
权利要求书2页 说明书12页 附图1页

(54)发明名称

一种防止恶意程序攻击网络支付页面的方法及装置

(57)摘要

本发明涉及网络通信技术领域,其公开了一种防止恶意程序攻击网络支付页面的方法及装置,该方法包括:检测浏览器所访问的页面是否为网络支付页面;当检测到浏览器所访问的页面为网络支付页面时,监测是否存在恶意程序访问所述浏览器的行为;当监测到所述恶意程序访问所述浏览器的行为时,拦截所述恶意程序。由此,一旦检测到浏览器所访问的页面为网络支付页面,则加强对浏览器的监测,以便确定在浏览器访问网络支付页面的过程中是否存在恶意程序访问浏览器的行为,当存在这种行为时,则对该恶意程序进行拦截,以达到保护支付信息不被泄露,提高支付安全性的效果。



CN 103605924 B

1.一种防止恶意程序攻击网络支付页面的方法,包括:

预先设置特征数据库,所述特征数据库中存储的网络支付页面的特征包括:特征信息以及模板信息;

根据所述特征信息以及模板信息检测浏览器所访问的页面是否为网络支付页面;其中,判断浏览器所访问的页面的页面特征与所述特征信息是否匹配,当判断结果为否时,确定所述浏览器所访问的页面不是网络支付页面;当判断结果为是时,进一步根据浏览器所访问的页面的内容特征与所述模板信息是否匹配来确定所述浏览器所访问的页面是否为网络支付页面;

当检测到浏览器所访问的页面为网络支付页面时,通过挂钩技术监测是否存在恶意程序访问所述浏览器的行为;

当监测到所述恶意程序访问所述浏览器的行为时,拦截所述恶意程序。

2.如权利要求1所述的方法,其中,所述浏览器所访问的页面的页面特征包括浏览器所访问的页面的URL,且所述特征数据库中存储的网络支付页面的特征信息包括网络支付页面的URL,其中,当所述网络支付页面为动态页面中的顶级页或内嵌页时,所述特征数据库中存储的网络支付页面的特征信息进一步包括:所述网络支付页面对应的refer链,其中,所述refer链用于存储所述网络支付页面所属的动态页面中的顶级页与各个内嵌页之间的嵌套关系,以及所述顶级页与各个内嵌页对应的URL。

3.如权利要求1或2所述的方法,其中,所述特征数据库为存储在客户端本地的本地特征数据库,或者,所述特征数据库为存储在网络服务器端的网络特征数据库。

4.如权利要求1所述的方法,其中,所述恶意程序访问所述浏览器的行为包括以下行为中的一个或多个:

所述恶意程序获取所述浏览器的窗口句柄的行为;

所述恶意程序获取所述浏览器的接口指针的行为;

所述恶意程序获取所述浏览器的浏览器句柄的行为。

5.如权利要求4所述的方法,其中,所述恶意程序访问所述浏览器的行为是所述恶意程序获取所述浏览器的浏览器句柄的行为。

6.一种防止恶意程序攻击网络支付页面的装置,包括:

存储单元,适于预先设置特征数据库,所述特征数据库中存储的网络支

付页面的特征包括:特征信息以及模板信息;

检测单元,适于根据所述特征信息以及模板信息检测浏览器所访问的页面是否为网络支付页面;其中,判断浏览器所访问的页面的页面特征与所述特征信息是否匹配,当判断结果为否时,确定所述浏览器所访问的页面不是网络支付页面;当判断结果为是时,进一步根据浏览器所访问的页面的内容特征与所述模板信息是否匹配来确定所述浏览器所访问的页面是否为网络支付页面;

监测单元,适于当检测到浏览器所访问的页面为网络支付页面时,通过挂钩技术监测是否存在恶意程序访问所述浏览器的行为;

拦截单元,适于当监测到所述恶意程序访问所述浏览器的行为时,拦截所述恶意程序。

7.如权利要求6所述的装置,其中,所述浏览器所访问的页面的页面特征包括浏览器所访问的页面的URL,且所述特征数据库中存储的网络支付页面的特征信息包括网络支付页

面的URL，其中，当所述网络支付页面为动态页面中的顶级页或内嵌页时，所述特征数据库中存储的页面的特征信息进一步包括：所述网络支付页面对应的refer链，其中，所述refer链用于存储所述网络支付页面所属的动态页面中的顶级页与各个内嵌页之间的嵌套关系，以及所述顶级页与各个内嵌页对应的URL。

8.如权利要求6所述的装置，其中，所述监测单元监测的恶意程序访问所述浏览器的行为包括以下行为中的一个或多个：

所述恶意程序获取所述浏览器的窗口句柄的行为；

所述恶意程序获取所述浏览器的接口指针的行为；

所述恶意程序获取所述浏览器的浏览器句柄的行为。

9.如权利要求8所述的装置，其中，所述监测单元监测的恶意程序访问所述浏览器的行为是所述恶意程序获取所述浏览器的浏览器句柄的行为。

一种防止恶意程序攻击网络支付页面的方法及装置

技术领域

[0001] 本发明涉及网络通信技术领域，具体涉及一种防止恶意程序攻击网络支付页面的方法及装置。

背景技术

[0002] 随着互联网的发展，网络支付功能得到了越来越广泛的应用。用户通过网络支付功能可以在线支付各种费用。例如，当用户登录网上商城购买物品时，可以通过预先开通的网络银行进行网上转帐支付，在具体支付过程中，用户需要输入有关支付的重要信息(包括银行卡账号和预先设置的密码等)，这些重要信息一旦被恶意第三方盗取则会严重威胁支付的安全性。

[0003] 在现有技术中，恶意第三方为了通过木马盗取用户的重要信息，可以在用户通过网页点击支付按钮时，诱导用户的浏览器跳转到恶意第三方预先设置好的恶意网页上，由于该恶意网页与正常的支付网页非常相似，因此，用户很可能会毫无防备地在该恶意网页上输入与支付有关的重要信息，此时，就会造成用户信息的泄漏，进而威胁到支付的安全性。

发明内容

[0004] 鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的防止恶意程序攻击网络支付页面的方法及装置。

[0005] 根据本发明的一个方面，提供了一种防止恶意程序攻击网络支付页面的方法，包括：检测浏览器所访问的页面是否为网络支付页面；当检测到浏览器所访问的页面为网络支付页面时，监测是否存在恶意程序访问所述浏览器的行为；当监测到所述恶意程序访问所述浏览器的行为时，拦截所述恶意程序。

[0006] 可选地，进一步包括步骤：预先设置特征数据库，所述特征数据库用于存储网络支付页面的特征，所述检测浏览器所访问的页面是否为网络支付页面的步骤具体包括：获取浏览器所访问的页面的特征，并判断所述浏览器所访问的页面的特征是否与所述特征数据库中存储的特征匹配，当判断结果为是时，确定所述浏览器所访问的页面是网络支付页面；当判断结果为否时，确定所述浏览器所访问的页面不是网络支付页面。

[0007] 可选地，所述浏览器所访问的页面的特征包括浏览器所访问的页面的URL，且所述特征数据库中存储的网络支付页面的特征包括网络支付页面的URL，其中，当所述网络支付页面为动态页面中的顶级页或内嵌页时，所述特征数据库中存储的网络支付页面的特征进一步包括：所述网络支付页面对应的refer链，其中，所述refer链用于存储所述网络支付页面所属的动态页面中的顶级页与各个内嵌页之间的嵌套关系，以及所述顶级页与各个内嵌页对应的URL。

[0008] 可选地，所述特征数据库为存储在客户端本地的本地特征数据库，或者，所述特征数据库为存储在网络服务器端的网络特征数据库。

[0009] 可选地，所述恶意程序访问所述浏览器的行为包括以下行为中的一个或多个：所述恶意程序获取所述浏览器的窗口句柄的行为；所述恶意程序获取所述浏览器的接口指针的行为；所述恶意程序获取所述浏览器的浏览器句柄的行为。

[0010] 可选地，监测所述恶意程序访问所述浏览器的行为通过挂钩技术实现。

[0011] 可选地，所述恶意程序访问所述浏览器的行为是所述恶意程序获取所述浏览器的浏览器句柄的行为。

[0012] 根据本发明的另一方面，提供了一种防止恶意程序攻击网络支付页面的装置，包括：检测单元，适于检测浏览器所访问的页面是否为网络支付页面；监测单元，适于当检测到浏览器所访问的页面为网络支付页面时，监测是否存在恶意程序访问所述浏览器的行为；拦截单元，适于当监测到所述恶意程序访问所述浏览器的行为时，拦截所述恶意程序。

[0013] 可选地，进一步包括存储单元，适于预先设置特征数据库，所述特征数据库用于存储网络支付页面的特征；所述检测单元适于获取浏览器所访问的页面的特征，并判断所述浏览器所访问的页面的特征是否与所述特征数据库中存储的特征匹配，当判断结果为是时，确定所述浏览器所访问的页面是网络支付页面；当判断结果为否时，确定所述浏览器所访问的页面不是网络支付页面。

[0014] 可选地，所述浏览器所访问的页面的特征包括浏览器所访问的页面的URL，且所述特征数据库中存储的网络支付页面的特征包括网络支付页面的URL，其中，当所述网络支付页面为动态页面中的顶级页或内嵌页时，所述特征数据库中存储的网络支付页面的特征进一步包括：所述网络支付页面对应的refer链，其中，所述refer链用于存储所述网络支付页面所属的动态页面中的顶级页与各个内嵌页之间的嵌套关系，以及所述顶级页与各个内嵌页对应的URL。

[0015] 可选地，所述监测单元监测的恶意程序访问所述浏览器的行为包括以下行为中的一个或多个：所述恶意程序获取所述浏览器的窗口句柄的行为；所述恶意程序获取所述浏览器的接口指针的行为；所述恶意程序获取所述浏览器的浏览器句柄的行为。

[0016] 可选地，所述监测单元通过挂钩技术监测所述恶意程序访问所述浏览器的行为。

[0017] 可选地，所述监测单元监测的恶意程序访问所述浏览器的行为是所述恶意程序获取所述浏览器的浏览器句柄的行为。

[0018] 根据本发明的方法及装置，一旦检测到浏览器所访问的页面为网络支付页面，则加强对浏览器的监测，以便确定在浏览器访问网络支付页面的过程中是否存在恶意程序访问浏览器的行为，当存在这种行为时，则对该恶意程序进行拦截，以达到保护支付信息不被泄露，提高支付安全性的效果。

[0019] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0020] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0021] 图1示出了本发明实施例提供的防止恶意程序攻击网络支付页面的方法流程图；以及

[0022] 图2示出了本发明实施例提供的防止恶意程序攻击网络支付页面的装置结构图。

具体实施方式

[0023] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0024] 本发明提供了一种防止恶意程序攻击网络支付页面的方法及装置，用以解决目前在网络支付过程中由于用户信息泄漏所导致的威胁支付安全性的问题。

[0025] 图1示出了本发明实施例提供的防止恶意程序攻击网络支付页面的方法流程图。该方法的执行主体例如可以是安装在客户端上的独立于浏览器的软件程序(例如安全卫士等)，或者，也可以是直接安装在客户端浏览器上的浏览器插件，另外，上述客户端既可以是固定终端(例如电脑终端)，也可以是移动终端(例如手机终端)。如图1所示，该方法起始于步骤S110，在步骤S110中，检测浏览器所访问的页面是否为网络支付页面。

[0026] 其中，在步骤S110中，需要对浏览器当前所访问的页面进行持续监测，在此过程中，主要是对浏览器切换新页面的行为进行监测，并且，每当监测到浏览器打开了一个新页面时，判断该新页面是否为网络支付页面。其中，浏览器打开新页面的行为具体包括下述几种情形：

[0027] 在第一种情形中，浏览器打开的新页面为静态页面，所谓静态页面，是指页面内容是不能随时改动的，而是一次性写好页面内容后放在服务器上供客户端浏览器浏览的，如果想改动页面内容，必须先在页面上修改完毕后再上传到服务器以覆盖原有页面。由于静态页面上所显示的内容有可能是钓鱼网站预先写好的内容，因此，当浏览器打开一个新的静态页面时需要进行监测。

[0028] 在第二种情形中，浏览器打开的新页面为动态页面，所谓动态页面，是指页面内容是能够随时改动的。例如，在服务器端与客户端的页面内容不相同，最原始的页面存在服务器端，根据用户反馈的内容或者要求，在服务器端计算得出结果以后，直接把结果传递到客户端电脑上显示出来。由于动态页面上每次所显示的内容都有可能是钓鱼网站预先写好的内容，因此，当浏览器打开一个新的动态页面时更需要进行监测。

[0029] 在上述两种情形中所打开的新页面，既有可能是用户通过地址栏输入URL后主动请求加载的页面，也有可能是通过其他页面上的超链接等元素引导进入的页面，或者还可能是一些脚本运行完毕后自动加载的页面，总之，无论上述新页面是如何加载的，都需要进行监测。

[0030] 介绍完浏览器打开新页面的行为方式之后，下面结合上述行为方式给出判断上述新页面是否为网络支付页面的方法。其中，由于动态页面的内容繁多，而且还可以通过脚本来修改当前显示的页面内容，所以即使是在页面掩码貌似正常的情况下，也有可能在脚本加载完成后显示出一个伪造的支付宝或中奖内容，从而诱使用户受骗。因此，下面主要针对第二种情形中的动态网页的特点来介绍判断新页面是否为网络支付页面的方式。

[0031] 其中，动态页面通常采用嵌套页的形式实现，例如，在顶级页的内容中进一步嵌套了多个层次的内嵌页。这时，为了防止仅仅关注顶级页面，漏掉钓鱼欺诈网页信息的情况发生，需要对动态页面的每个层次都进行识别和监测。为此，需要先通过浏览器辅助对象(Browser Helper Object，BHO)获取事件标记的方式来识别出当前页面是内嵌页还是顶级页，然后再根据内嵌页或顶级页的特点进行有针对性的监测。

[0032] 为了清楚地表示出动态页面的顶级页与各个内嵌页之间的层次关系，在本发明中引入refer链的概念。下面详细介绍一下refer链的含义和确定方式：

[0033] 首先，将浏览器所打开的当前页面称为第i级页面，$i \geq 2$，该第i级页面是由初始页面(即顶级页)的第i级链接所打开的页面。通常，在用户打开浏览器后，浏览器访问默认的初始页面或者通过用户在地址栏的输入触发初始页面的访问请求，通过用户在初始页面上点击链接或者其它链接方式由初始页面链接到第2级页面，通过用户在第2级页面上点击链接或者其它链接方式由第2级页面链接到第3级页面，依此类推，最后由第i-1级页面链接到第i级页面。举例来说，用户打开浏览器后在地址栏输入www.so.com，该页面就是初始页面(下面用A来表示其URL)；然后，用户在搜索栏输入“话费充值”，点击搜索按钮，浏览器会跳到http://www.so.com/s?ie=utf-8&src=360sou_home&q=%E8%AF%9D%E8%B4%B9%E5%85%85%E5%80%BC，该页面为第2级页面(下面用B来表示其URL)；第2级页面提供了很多链接，用户点击其中一个链接，浏览器会跳到此链接对应的页面http://chongzhi.360.cn/mobile/，该页面为第3级页面(下面用C来表示其URL)；用户在第3级页面上点击“网游点卡”链接，浏览器会跳到http://chongzhi.360.cn/Game Card/index，该页面为第4级页面(下面用D来表示其URL)。用户在第3级页面上点击“网游点卡”链接，浏览器就会监控到第4级页面：http://cho ngzhi.360.cn/GameCard/index的访问请求。

[0034] 然后，在监控到第i级页面的访问请求后，浏览器将加载第i级页面，在加载第i级页面的过程中，获取包含第i级页面的页面ID的refer链。该refer链包含初始页面至第i级页面的页面ID和URL，其中各级页面的页面ID是浏览器在加载页面的过程中为页面所生成的唯一的ID，在refer链中它作为页面的URL的索引值。浏览器通过第i级页面的页面ID查询包含第i级页面的URL且第i级页面是最后一级页面的refer链。例如，refer链为A(ID1)->B(ID2)->C(ID3)->D(ID4)，其中A、B、C和D分别为各级页面的URL，ID1、ID2、ID3和ID4分别为各级页面的页面ID。在浏览器加载页面D时，根据页面D的页面ID4查询到上述refer链。因此，在上述示例中，在加载第4级页面的过程中，将获取如下refer链：A(ID1)->B(ID2)->C(ID3)->D(ID4)。获取到该refer链之后，客户端可以将该refer链所包含的所有URL发送给服务器。客户端可以仅将refer链所包含的各级页面的URL上报给服务器，无需上报各级页面的页面ID。对于refer链：A(ID1)->B(ID2)->C(ID3)->D(ID4)，客户端将A->B->C->D发送给服务器。可选地，根据与服务器之间的云查询协议，本方法可以将refer链所包含的所有URL加密成密文发送给服务器。

[0035] 综上，每当通过初始页面的各级链接打开新页面时，负责维护refer链的进程获取新页面的页面ID和URL以及新页面的上一级页面的页面ID或URL，根据该上一级页面的页面ID或URL查询对应的refer链，创建refer链的对应节点。由此可见，通过refer链能够清楚地表示出动态页面中的顶级页与各个内嵌页之间的嵌套关系，如果某一顶级页或当前打开的内嵌页的上一级内嵌页存在钓鱼信息，则可以确定当前打开的内嵌页也是不安全的，因此，

通过refer链能够识别出当前打开的内嵌页的来源，因而能够更加准确地判断该内嵌页是否安全。另外，具体到本实施例中，即使浏览器当前打开的内嵌页不是网络支付页面，但如果该内嵌页的上一级页面或上几级页面是网络支付页面，那么，也应该对该内嵌页加强监测。总之，通过refer链能够使步骤S110中的监测角度更加全面。

[0036] 基于动态页面的上述特点以及refer链的含义，具体地，在判断该新页面是否为网络支付页面时可以根据网络支付页面的特点灵活选择多种判断方式：

[0037] 在第一种判断方式中，预先设置特征数据库，该特征数据库用来存储网络支付页面的特征。这里所说的网络支付页面主要是指包含“确认付款”等类按钮的页面，一旦用户在支付页面上点击了“确认付款”的按钮，就会将款项打入对方帐号，因此，对这类支付页面进行监控是非常有必要的。其中，网络支付页面的特征可以通过多种形式表现，例如，可以是网络支付页面的URL地址，因为根据URL地址就可以唯一地标识一个网页。当采用URL地址作为网络支付页面的特征时，需要预先获取各类支付页面的URL地址，例如，可以将常见的各类付款方式(如各个银行的信用卡、储蓄卡以及支付宝等)所对应的支付页面的URL地址存储到该特征数据库中。这里所说的URL地址既可以是完整的URL地址，也可以仅仅是URL地址中所要包含的部分特征。例如，假设用户通过建设银行的网上银行功能进行付款，在其对应的支付页面的URL地址中一定会包含有关建设银行的标识信息，那么，只要在特征数据库中存储该标识信息就可以监测到所有包含该标识信息的支付页面，从而能够监测到所有通过建设银行进行付款的页面。同理，在特征数据库中还应该存储其他的各个银行以及其他各类支付方式所对应的URL地址(或URL地址中有关于付款的标识信息)。另外，当网络支付页面为动态页面中的顶级页或内嵌页时，在特征数据库中还可以进一步存储该网络支付页面对应的refer链，该refer链存储了该网络支付页面所属的动态页面中的顶级页与各个内嵌页之间的嵌套关系，以及顶级页与各个内嵌页对应的URL的集合。这样，即使浏览器当前打开的新页面不是网络支付页面，但只要在该页面所属的动态页面的某一级页面中包含网络支付页面，也会将该页面识别出来，由此使得监测更加全面。

[0038] 在第二种判断方式中，也需要预先设置特征数据库，该特征数据库中不仅包括用来存储网络支付页面的特征信息(如第一种判断方式中的URL等)，另外，在特征数据库中还需要存储网络支付页面的模板信息。

[0039] 首先，特征数据库中的特征信息用于精准识别，所谓精准识别，就是抓取的页面特征会生成一个签名，该签名中的全部特征必须都与特征数据库中的特征信息匹配。例如，根据浏览器当前访问页面的页面特征生成的签名中包含20个特征，必须是20个特征全部与特征数据库中的特征信息匹配才可以。只有在浏览器打开的新页面与特征信息匹配的情况下，才会进一步根据模板信息来确认该新页面是否为网络支付页面，否则则直接中止对该新页面的检测，因此，通过特征信息精准识别的方式能够快速过滤掉大量的无关网页，从而集中精力识别潜在的网络支付页面。

[0040] 然后，特征数据库中的模板信息用于模糊识别：在模板信息中存储了网络支付页面的一些内容特征(例如与支付有关的敏感词汇：“支付”、“付款”等)，通常，模板信息中存储的内容特征为多个；然后，对浏览器打开的新页面的内容进行识别，以判断其内容是否与模板信息符合。具体地，在对浏览器打开的新页面的内容进行识别时，如果是动态页面，要等脚本(如js脚本)运行完毕，且网页的文档对象模型(DOM)组建完毕后进行识别，才能保证

识别的内容是网页的完整内容，如果该动态页面包含多级页面，还需要对其中的每一层内嵌页都进行识别，从而防止漏掉钓鱼信息。识别出浏览器打开的页面内容之后，判断页面内容与模板信息中的各项内容特征之间的相似度，根据相似度分别进行打分，并且，还可以根据每项内容特征的重要性为其赋予不同的权重，根据页面内容对应于每项内容特征的分值以及该项内容特征的权重来得出页面内容的综合得分，根据综合得分的高低来判断该页面是否为网络支付页面。因此，在模糊识别的过程中，是通过打分，或者综合评价的方式来识别的，例如可以采用统计模型和神经网络等算法实现。对于常见的文字混淆，图片混淆，或者改变语言顺序的混淆方式都可以通过模糊识别检测出来。

[0041] 由此可见，第二种判断方式在第一种判断方式的基础上又增加了基于页面内容的模糊识别技术，因而判断结果更为准确。实际上，第二种判断方式中的基于页面内容的模糊识别技术也可以单独作为一种判断方式来实现。另外，本领域技术人员还可以根据需要灵活采用其它的判断方式，例如，也可以根据正则表达式的匹配方式进行判断等。

[0042] 另外，上述两种方式中的特征数据库既可以是存储在客户端本地的本地特征数据库，也可以是存储在网络服务器端的网络特征数据库。优选地，可以将特征数据库同时存储在网络服务器端和客户端本地，这样，当发现新的支付页面的特征时，首先对网络服务器端的特征数据库进行更新，更新后，可以由网络服务器主动将更新后的特征数据库中的内容发送给各个客户端，由各个客户端对本地存储的特征数据库进行相应的更新；或者，也可以由各个客户端每隔预设时间间隔自动地向服务器端请求最新的特征数据库。通过在网络服务器端和客户端本地同时存储特征数据库的方式，既能够确保特征数据库的及时更新，又能够在客户端暂时断网的情况下为客户端提供保护。

[0043] 设置好上述的特征数据库之后，在判断浏览器所访问的页面是否为网络支付页面时，首先需要获取浏览器所访问的页面的特征，即该页面的URL地址；然后，判断该URL地址是否与特征数据库中存储的某一特征匹配，当判断结果为是时，确定该浏览器所访问的页面是网络支付页面；当判断结果为否时，则确定该浏览器所访问的页面不是网络支付页面。

[0044] 另外，在步骤S110中，也可以由浏览器本身对访问的页面进行判断，当判断出访问页面为网络支付页面时，由浏览器通知本方法的执行主体。

[0045] 当在上述步骤S110中检测到该浏览器所访问的页面为网络支付页面时，则转入步骤S120，在步骤S120中，监测是否存在恶意程序访问该浏览器的行为。也就是说，当检测到该浏览器所访问的页面为网络支付页面时，则使浏览器转入强力保护模式，在该模式下，对浏览器加强检测，从而提高浏览器的主动防御功能，避免受到恶意程序的攻击。其中，恶意程序可以通过恶意网址类别和可信度值来判断，其中，恶意网址类别又可以进一步包括：钓鱼网站，假冒主站、虚假信息以及医疗广告等类别。

[0046] 其中，恶意程序访问浏览器的行为包括以下行为中的一个或多个：恶意程序获取浏览器的窗口句柄的行为；恶意程序获取浏览器的接口指针的行为；以及，恶意程序获取浏览器的浏览器句柄(handle)的行为。具体地，获取浏览器的窗口句柄的目的在于查找到浏览器本身；在获取到窗口句柄之后，如果进一步获取到浏览器的接口指针，则可以对查找到的该浏览器进行访问；再进一步地，如果该浏览器当前打开了多个页面，那么，只有进一步获取到具体的某一页面所对应的浏览器句柄，才可以对该页面进行访问。通过上述描述可以看出，上述的三个行为是依次发生的，因此，上述三个行为的危险性也是逐步加深的：如

果监测到获取窗口句柄的行为，只能说明有恶意程序希望访问该浏览器；如果监测到获取接口指针的行为，也只能说明有恶意程序能够访问该浏览器；而只有监测到了获取浏览器句柄的行为，才能够确定有恶意程序能够访问该浏览器所访问的当前页面，即：该恶意程序对当前页面已经构成了威胁。由此可以看出，如果监测前两种行为，则能够较早地发现潜在的恶意程序，但是也有可能导致误报率较高，而且监测成本也较高；相比之下，如果监测第三种行为，既可以有效地预防恶意程序发起的攻击，还可以显著降低误报率，且监测成本也较低。因此，优选地，本实施例中以监测第三种行为为例进行介绍。

[0047] 在介绍关于第三种行为的具体监测方式之前，首先介绍一下恶意程序通过第三种行为攻击网络支付页面的具体实现方式：首先，恶意程序通过windows的远程程序调用(Remote Procedure Call，RPC)机制，获取到浏览器句柄。其中，浏览器句柄可以通过一个接口表示，该接口例如可以是表达上下文字段PresentationContext接口，或者，该接口也可以是浏览器事件响应注册接口、浏览器对象接口、HTML修改接口等各类能够操作浏览器的接口。恶意程序获取到浏览器句柄之后，就可以利用该浏览器句柄实现操作浏览器的目的。通常情况下，恶意程序获取到浏览器句柄之后，可以篡改浏览器所显示的网络支付页面。例如，恶意程序可以采用如下两种篡改方式：在第一种篡改方式中，恶意程序提前注册为一个商家，然后将浏览器所显示的正确的网络支付页面修改为恶意程序对应的商家的虚假支付页面，该虚假支付页面与浏览器所显示的正确的网络支付页面通常非常相似，因此，用户一般不易察觉，从而会因疏忽而将钱款打入虚假支付页面对应的收款方，从而使用户的钱财造成损失。在第二种篡改方式中，恶意程序不仅会将正确的网络支付页面修改为恶意程序对应的商家的虚假支付页面，而且，还会对支付金额等重要信息进行篡改，例如，将支付金额为10元篡改为支付金额为1000元，从而导致用户出现重要的财产损失。除了篡改浏览器所显示的网络支付页面的方式之外，恶意程序还可能获取到用户支付时的帐号信息和密码，从而直接利用用户的帐号信息和密码来完成一些非法的支付操作，从而为用户带来更大的损失。由此可见，虽然恶意程序攻击网络支付页面时的攻击行为多种多样，但实现这些攻击行为的共同前提是：必须获取到浏览器句柄。因此，通过监测恶意程序获取浏览器句柄的行为能够有效杜绝恶意程序的攻击行为。

[0048] 下面介绍一下监测恶意程序获取浏览器句柄的行为的具体监测方式。具体地，可以通过挂钩(HOOK)技术来实现对恶意程序的监测，即：在浏览器程序中的指定位置设置挂钩(HOOK)，以实现对指定位置的运行状态的监测。为了实现对浏览器句柄进行监测的目的，上面提到的指定位置可以是浏览器句柄所对应的接口(如PresentationContext接口)。通过对浏览器句柄所对应的接口设置挂钩，可以在任何程序(包括恶意程序在内)试图获取浏览器句柄时，先触发预设的挂钩函数中的逻辑功能。其中，挂钩函数中的逻辑功能例如可以是：通知本发明中的方法的执行主体(例如安全卫士软件等)，只有得到许可后才可以获取浏览器句柄，从而使本发明在步骤S120中监测到恶意程序访问浏览器的行为。

[0049] 可选地，在步骤S120中，还可以进一步在浏览器程序的多个位置设置挂钩函数，例如，可以在每个能够访问浏览器的接口处(包括上述的恶意程序获取浏览器的窗口句柄的行为所对应的接口，以及恶意程序获取浏览器的接口指针的行为所对应的接口等)都设置挂钩函数，这样，只要有程序试图访问浏览器，就会通过这些预设的挂钩函数通知本发明中的方法的执行主体，因此，只要没有得到本发明中的方法的执行主体的许可，任何程序都无

法访问浏览器。换句话说，在本发明中，当浏览器访问网页支付页面时，使浏览器进行强力保护模式，在该模式下，任何访问浏览器的行为都会受到监控，相当于为浏览器提供了一道坚实的壁垒。

[0050] 当监测到上述恶意程序访问浏览器的行为时，执行步骤S130。在步骤S130中，拦截该恶意程序。具体拦截时，可以直接杀死该恶意程序，使其无法运行；或者，也可以将该恶意程序提示给用户，由用户来决定是否清除该恶意程序。总之，只要能够阻止恶意程序的攻击行为即可。

[0051] 另外，在本发明提供的防止恶意程序攻击网络支付页面的方法中，还可以进一步包括步骤：当检测到浏览器退出对网络支付页面的访问时，使浏览器退出强力保护模式，转入正常模式，在正常模式下，不对上述访问浏览器的行为进行监测。

[0052] 综上所述，在本发明提供的防止恶意程序攻击网络支付页面的方法中，首先检测浏览器所访问的页面是否为网络支付页面，并在浏览器访问网络支付页面时，进入浏览器的强力保护模式，以加强对浏览器的安全监测。在强力保护模式下，持续监测是否存在恶意程序访问浏览器的行为，并在监测到这种行为时拦截恶意程序，由此避免了恶意程序对支付页面的攻击。

[0053] 由此可见，在本发明提供的方法中，不需要提前查找各类恶意程序，由于恶意程序种类繁多且千变万化，因此，如果通过提前查找所有的恶意程序来实现拦截的目的，不仅会耗费大量的程序资源，而且还容易造成漏查。在本发明中，是根据浏览器对应的用户场景来决定是否监测的（即：针对浏览器所访问的页面类型来提供保护）：在浏览器访问安全页面（例如与支付无关，因而不会受骗的页面）时，无需对浏览器提供强力保护，由此能够节约程序资源，避免了不必要的资源消耗；在浏览器访问敏感页面（例如与支付有关，可能会导致受骗的页面）时，对浏览器提供强力保护，并且，在保护过程中，不是漫无目的地寻找潜在的攻击源，而是有针对性地监测与攻击有关的行为，一旦监测到了这样的行为，就对该行为的执行者（即恶意程序）进行拦截。通过上述方式，使本发明中的防止恶意程序攻击网络支付页面的方法更有针对性、更节约资源、且不会造成漏查，因而安全性也更高。

[0054] 图2示出了本发明实施例提供的防止恶意程序攻击网络支付页面的装置的结构示意图。该装置例如可以是安装在客户端上的软件程序模块（例如安全卫士模块等）。如图2所示，该装置包括：检测单元21、监测单元22以及拦截单元23。

[0055] 其中，检测单元21检测浏览器所访问的页面是否为网络支付页面。

[0056] 其中，检测单元21需要对浏览器当前所访问的页面进行持续监测，在此过程中，主要是对浏览器切换新页面的行为进行监测，并且，每当监测到浏览器打开了一个新页面时，判断该新页面是否为网络支付页面。

[0057] 具体地，在判断该新页面是否为网络支付页面时可以根据网络支付页面的特点灵活选择多种判断方式，下面给出一种可能的判断方式：

[0058] 首先，预先设置特征数据库，为此，该装置还需要包括一个存储单元，由该存储单元来存储特征数据库。该特征数据库用来存储网络支付页面的特征。这里所说的网络支付页面主要是指包含“确认付款”等类按钮的页面，一旦用户在支付页面上点击了“确认付款”的按钮，就会将款项打入对方帐号，因此，对这类支付页面进行监控是非常有必要的。其中，网络支付页面的特征可以通过多种形式表现，例如，可以是网络支付页面的URL地址，因为

根据URL地址就可以唯一地标识一个网页。当采用URL地址作为网络支付页面的特征时，需要预先获取各类支付页面的URL地址，例如，可以将常见的各类付款方式（如各个银行的信用卡、储蓄卡以及支付宝等）所对应的支付页面的URL地址存储到该特征数据库中。这里所说的URL地址既可以是完整的URL地址，也可以仅仅是URL地址中所要包含的部分特征。例如，假设用户通过建设银行的网上银行功能进行付款，在其对应的支付页面的URL地址中一定会包含有关建设银行的标识信息，那么，只要在特征数据库中存储该标识信息就可以监测到所有包含该标识信息的支付页面，从而能够监测到所有通过建设银行进行付款的页面。同理，在特征数据库中还应该存储其他的各个银行以及其他各类支付方式所对应的URL地址（或URL地址中有关于付款的标识信息）。

[0059] 另外，上述的特征数据库既可以是存储在客户端本地的本地特征数据库，也可以是存储在网络服务器端的网络特征数据库。优选地，可以将特征数据库同时存储在网络服务器端和客户端本地，这样，当发现新的支付页面的特征时，首先对网络服务器端的特征数据库进行更新，更新后，可以由网络服务器主动将更新后的特征数据库中的内容发送给各个客户端，由各个客户端对本地存储的特征数据库进行相应的更新；或者，也可以由各个客户端每隔预设时间间隔自动地向服务器端请求最新的特征数据库。通过在网络服务器端和客户端本地同时存储特征数据库的方式，既能够确保特征数据库的及时更新，又能够在客户端暂时断网的情况下为客户端提供保护。

[0060] 设置好上述的特征数据库之后，检测单元21在判断浏览器所访问的页面是否为网络支付页面时，首先需要获取浏览器所访问的页面的特征，即该页面的URL地址；然后，判断该URL地址是否与特征数据库中存储的某一特征匹配，当判断结果为是时，确定该浏览器所访问的页面是网络支付页面；当判断结果为否时，则确定该浏览器所访问的页面不是网络支付页面。

[0061] 除了采用URL地址来判断浏览器所访问的页面是否为网络支付页面外，本领域技术人员也可以灵活采用其他的判断方式，例如，可以在特征数据库中存储一些与支付有关的敏感词汇（例如“支付”、“付款”等），然后检测单元21持续监测浏览器所访问的页面内容，当监测到页面内容中包含上述敏感词汇时则确定浏览器所访问的页面为网络支付页面。

[0062] 当检测单元21检测到该浏览器所访问的页面为网络支付页面时，由监测单元22监测是否存在恶意程序访问该浏览器的行为。也就是说，当检测到该浏览器所访问的页面为网络支付页面时，则使浏览器转入强力保护模式，在该模式下，对浏览器加强监测，从而提高浏览器的主动防御功能，避免受到恶意程序的攻击。

[0063] 其中，恶意程序访问浏览器的行为包括以下行为中的一个或多个：恶意程序获取浏览器的窗口句柄的行为；恶意程序获取浏览器的接口指针的行为；以及，恶意程序获取浏览器的浏览器句柄（handle）的行为。具体地，获取浏览器的窗口句柄的目的在于查找到浏览器本身；在获取到窗口句柄之后，如果进一步获取到浏览器的接口指针，则可以对查找到的该浏览器进行访问；再进一步地，如果该浏览器当前打开了多个页面，那么，只有进一步获取到具体的某一页面所对应的浏览器句柄，才可以对该页面进行访问。通过上述描述可以看出，上述的三个行为是依次发生的，因此，上述三个行为的危险性也是逐步加深的：如果监测到获取窗口句柄的行为，只能说明有恶意程序希望访问该浏览器；如果监测到获取接口指针的行为，也只能说明有恶意程序能够访问该浏览器；而只有监测到了获取浏览器

句柄的行为，才能够确定有恶意程序能够访问该浏览器所访问的当前页面，即：该恶意程序对当前页面已经构成了威胁。由此可以看出，如果监测前两种行为，则能够较早地发现潜在的恶意程序，但是也有可能导致误报率较高，而且监测成本也较高；相比之下，如果监测第三种行为，既可以有效地预防恶意程序发起的攻击，还可以显著降低误报率，且监测成本也较低。因此，优选地，本实施例中以监测第三种行为为例进行介绍。

[0064] 下面介绍一下监测单元22监测恶意程序获取浏览器句柄的行为的具体监测方式。具体地，可以通过挂钩(HOOK)技术来实现对恶意程序的监测，即：在浏览器程序中的指定位置设置挂钩(HOOK)，以实现对指定位置的运行状态的监测。为了实现对浏览器句柄进行监测的目的，上面提到的指定位置可以是浏览器句柄所对应的接口(如PresentationContext接口)。通过对浏览器句柄所对应的接口设置挂钩，可以在任何程序(包括恶意程序在内)试图获取浏览器句柄时，先触发预设的挂钩函数中的逻辑功能。其中，挂钩函数中的逻辑功能例如可以是：通知本发明中的装置中的监测单元，只有得到监测单元的许可后才可以获取浏览器句柄。

[0065] 可选地，监测单元22还可以进一步在浏览器程序的多个位置设置挂钩函数，例如，可以在每个能够访问浏览器的接口处(包括上述的恶意程序获取浏览器的窗口句柄的行为所对应的接口，以及恶意程序获取浏览器的接口指针的行为所对应的接口等)都设置挂钩函数，这样，只要有程序试图访问浏览器，就会通过这些预设的挂钩函数通知监测单元，因此，只要没有得到监测单元的许可，任何程序都无法访问浏览器。换句话说，在本发明中，当浏览器访问网页支付页面时，使浏览器进行强力保护模式，在该模式下，任何访问浏览器的行为都会受到监控，相当于为浏览器提供了一道坚实的壁垒。

[0066] 当监测到上述恶意程序访问浏览器的行为时，由拦截单元23拦截该恶意程序。具体拦截时，可以直接杀死该恶意程序，使其无法运行；或者，也可以将该恶意程序提示给用户，由用户来决定是否清除该恶意程序。总之，只要能够阻止恶意程序的攻击行为即可。

[0067] 综上所述，在本发明提供的防止恶意程序攻击网络支付页面的装置中，首先检测浏览器所访问的页面是否为网络支付页面，并在浏览器访问网络支付页面时，进入浏览器的强力保护模式，以加强对浏览器的安全监测。在强力保护模式下，持续监测是否存在恶意程序访问浏览器的行为，并在监测到这种行为时拦截恶意程序，由此避免了恶意程序对支付页面的攻击。

[0068] 由此可见，在本发明提供的装置中，不需要提前查找各类恶意程序，由于恶意程序种类繁多且千变万化，因此，如果通过提前查找所有的恶意程序来实现拦截的目的，不仅会耗费大量的程序资源，而且还容易造成漏查。在本发明中，是根据浏览器对应的用户场景来决定是否监测的(即：针对浏览器所访问的页面类型来提供保护)：在浏览器访问安全页面(例如与支付无关，因而不会受骗的页面)时，无需对浏览器提供强力保护，由此能够节约程序资源，避免了不必要的资源消耗；在浏览器访问敏感页面(例如与支付有关，可能会导致受骗的页面)时，对浏览器提供强力保护，并且，在保护过程中，不是漫无目的地寻找潜在的攻击源，而是有针对性地监测与攻击有关的行为，一旦监测到了这样的行为，就对该行为的执行者(即恶意程序)进行拦截。通过上述方式，使本发明中的防止恶意程序攻击网络支付页面的装置更有针对性、更节约资源、且不会造成漏查，因而安全性也更高。

[0069] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。

各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0070] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0071] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0072] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0073] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0074] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的浏览器客户端中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0075] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项

来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

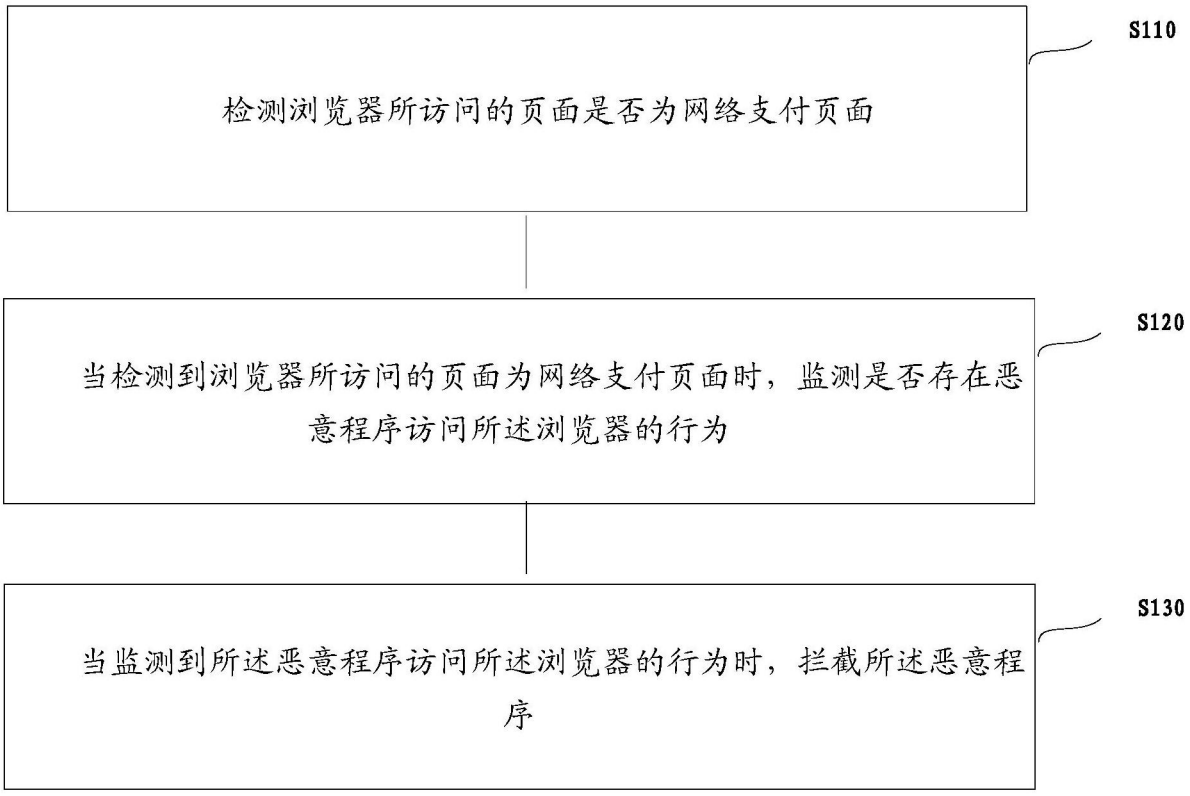

S110
检测浏览器所访问的页面是否为网络支付页面
S120
当检测到浏览器所访问的页面为网络支付页面时，监测是否存在恶意程序访问所述浏览器的行为
S130
当监测到所述恶意程序访问所述浏览器的行为时，拦截所述恶意程序

图1

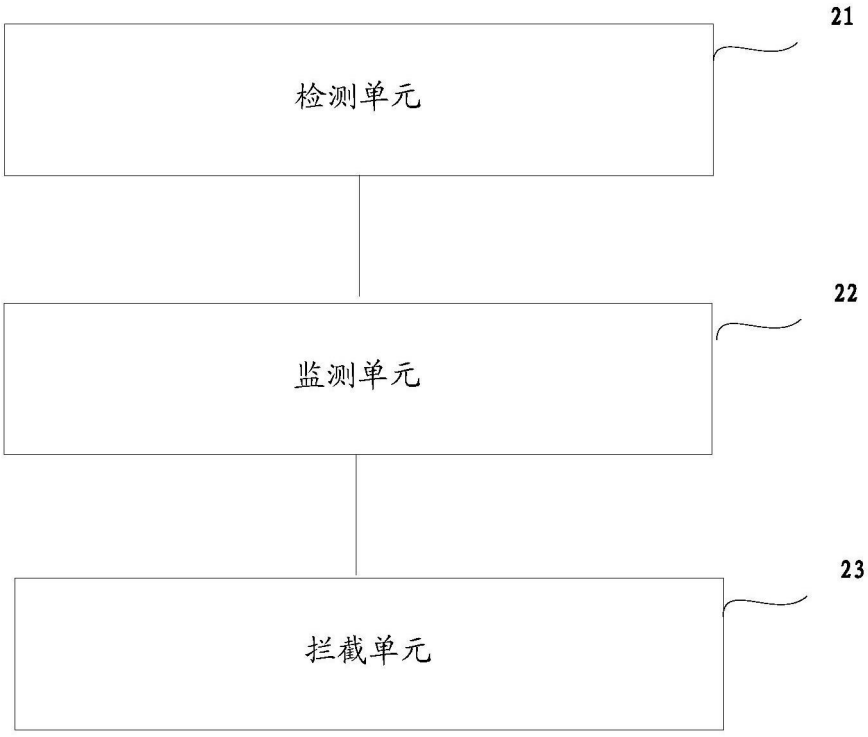

21
检测单元
22
监测单元
23
拦截单元

图2