(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 102999718 B
(45)授权公告日 2015.07.29

(21)申请号 201110277604.7

(22)申请日 2011.09.16

(73)专利权人 腾讯科技(深圳)有限公司
地址 518057 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 林杰 班五三 孟齐源

(74)专利代理机构 广州三环专利代理有限公司 44202
代理人 郝传鑫 熊永强

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

审查员 崔哲

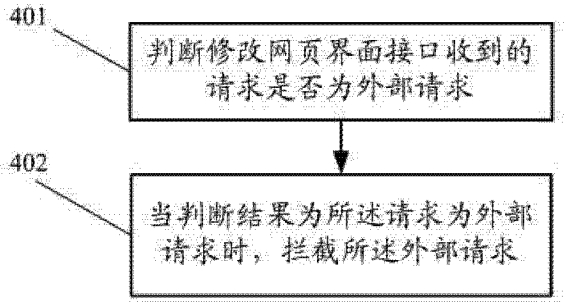
权利要求书2页 说明书4页 附图5页

(54)发明名称

一种支付网页防修改方法和装置

(57)摘要

本发明实施例公开了一种支付网页防修改方法和装置，该方法包括：判断修改网页界面接口收到的请求是否为外部请求，所述外部请求是指与运行所述网页进程不同的其他进程发出的跨进程请求；当判断结果为所述请求为外部请求时，拦截所述外部请求。采用本发明，可以避免木马程序对页面的篡改，起到提高电子商务安全性的目的。



CN 102999718 B

1.一种支付网页防修改方法,其特征在于,所述方法包括 :

判断修改网页界面接口收到的请求是否为外部请求,所述外部请求是指与运行所述网页进程不同的其他进程发出的跨进程请求 ;

当判断结果为所述请求为外部请求时,拦截所述外部请求 ;

其中,所述修改网页界面接口包括与修改支付网页内容有关的 HTML 修改接口,所述外部请求包括所述 HTML 修改接口的写入函数,所述拦截所述外部请求包括 :

拦截所述其他进程通过调用所述 HTML 修改接口的写入函数修改支付页面的内容 ;或者,

所述修改网页界面接口包括与修改支付网页内容有关的 HTML 修改接口和浏览器事件响应注册接口,所述外部请求包括所述 HTML 修改接口的写入函数和所述浏览器事件响应注册接口的 Advise 函数,所述拦截所述外部请求包括 :

拦截所述其他进程通过调用所述 HTML 修改接口的写入函数修改支付页面的内容 ;

拦截所述其他进程通过调用所述浏览器事件响应注册接口的 Advise 函数获取浏览器信息 ;或者,

所述修改网页界面接口包括与修改支付网页内容有关的 HTML 修改接口和浏览器对象接口,所述外部请求包括所述 HTML 修改接口的写入函数和浏览器对象接口的获取本地 URL 函数,所述拦截所述外部请求包括 :

拦截所述其他进程通过调用所述 HTML 修改接口的写入函数修改支付页面的内容 ;

拦截所述其他进程通过调用所述浏览器对象接口的获取本地 URL 函数判断当前页面是否为支付页面 ;或者,

所述修改网页界面接口包括与修改支付网页内容有关的 HTML 修改接口、浏览器事件响应注册接口和浏览器对象接口,所述外部请求包括所述 HTML 修改接口的写入函数、所述浏览器事件响应注册接口的 Advise 函数和浏览器对象接口的获取本地 URL 函数,所述拦截所述外部请求包括 :

拦截所述其他进程通过调用所述 HTML 修改接口的写入函数修改支付页面的内容 ;

拦截所述其他进程通过调用所述浏览器事件响应注册接口的 Advise 函数获取浏览器信息 ;

拦截所述其他进程通过调用所述浏览器对象接口的获取本地 URL 函数判断当前页面是否为支付页面。

2.如权利要求 1 所述的方法,其特征在于,所述判断修改网页界面接口收到的请求是否为外部请求包括 :

判断所述修改网页界面接口的调用栈中是否有 RPCRT4.dll 文件 ;

当判断结果为有 RPCRT4.dll 文件时,判断所述修改网页界面接口收到了外部请求。

3.一种支付网页防修改装置,其特征在于,所述装置包括 :

修改接口判断单元,用于判断修改网页界面接口收到的请求是否为外部请求,其中,所述外部请求是指与运行所述网页进程不同的其他进程发出的跨进程请求 ;

拦截单元,用于当判断结果为所述请求为外部请求时,拦截所述外部请求 ;

其中,所述修改网页界面接口包括与修改支付网页内容有关的 HTML 修改接口,所述外部请求包括所述 HTML 修改接口的写入函数,所述拦截单元包括 :

修改拦截子单元，用于拦截所述其他进程通过调用所述 HTML 修改接口的写入函数修改支付页面的内容；或者，

所述修改网页界面接口包括与修改支付网页内容有关的 HTML 修改接口和浏览器事件响应注册接口，所述外部请求包括所述 HTML 修改接口的写入函数和所述浏览器事件响应注册接口的 Advise 函数，所述拦截单元包括：

信息拦截子单元，用于拦截所述其他进程通过调用所述浏览器事件响应注册接口的 Advise 函数获取浏览器信息；

修改拦截子单元，用于拦截所述其他进程通过调用所述 HTML 修改接口的写入函数修改支付页面的内容；或者，

所述修改网页界面接口包括与修改支付网页内容有关的 HTML 修改接口和浏览器对象接口，所述外部请求包括所述 HTML 修改接口的写入函数和浏览器对象接口的获取本地 URL 函数，所述拦截单元包括：

判断拦截子单元，用于拦截所述其他进程通过调用所述浏览器对象接口的获取本地 URL 函数判断当前页面是否为支付页面；

修改拦截子单元，用于拦截所述其他进程通过调用所述 HTML 修改接口的写入函数修改支付页面的内容；或者，

所述修改网页界面接口包括与修改支付网页内容有关的 HTML 修改接口、浏览器事件响应注册接口和浏览器对象接口，所述外部请求包括所述 HTML 修改接口的写入函数、所述浏览器事件响应注册接口的 Advise 函数和浏览器对象接口的获取本地 URL 函数，所述拦截单元包括：

信息拦截子单元，用于拦截所述其他进程通过调用所述浏览器事件响应注册接口的 Advise 函数获取浏览器信息；

判断拦截子单元，用于拦截所述其他进程通过调用所述浏览器对象接口的获取本地 URL 函数判断当前页面是否为支付页面；

修改拦截子单元，用于拦截所述其他进程通过调用所述 HTML 修改接口的写入函数修改支付页面的内容。

4. 如权利要求 3 所述的装置，其特征在于，所述修改接口判断单元还用于，判断所述修改网页界面接口的调用栈中是否有 RPCRT4.dll 文件；当判断结果为有 RPCRT4.dll 文件时，判断所述修改网页界面接口收到了外部请求。

一种支付网页防修改方法和装置

技术领域

[0001] 本发明涉及互联网技术领域，尤其涉及一种支付网页防修改方法和装置。

背景技术

[0002] 随着互联网技术的不断普及和发展，电子商务已成为互联网业务中的重要业务。但是电子商务中的安全问题一直对电子商务的普及和发展起到极大的制约，比如，用户在进行网上支付时，特别是采用浏览器网页进行支付时，会被木马程序篡改页面，从而造成用户的经济损失。

[0003] 如图 1~图 2 所示，为用户支付时进行支付的几个环节的页面，在这几个环节中，木马程序通过篡改提交的支付页面，让用户把支付请求发送到其他的电子商务网站，从而造成对木马程序定义的商品进行了支付，而用户实际想要购买的商品并没有被支付。

发明内容

[0004] 本发明实施例所要解决的技术问题在于，提供一种支付网页防修改方法和装置。可以避免木马进程等恶意进程对页面的篡改，起到提高电子商务安全性的目的。

[0005] 为了解决上述技术问题，本发明实施例提供了一种支付网页防修改方法，包括：

[0006] 判断修改网页界面接口收到的请求是否为外部请求，所述外部请求是指与运行所述网页进程不同的其他进程发出的跨进程请求；

[0007] 当判断结果为所述请求为外部请求时，拦截所述外部请求。

[0008] 相应的，本发明实施例还提供了一种支付网页防修改装置，包括：

[0009] 修改接口判断单元，用于判断修改网页界面接口收到的请求是否为外部请求，其中，所述外部请求是指与运行所述网页进程不同的其他进程发出的跨进程请求；

[0010] 拦截单元，用于当判断结果为所述请求为外部请求时，拦截所述外部请求

[0011] 在本发明实施例中，通过阻止修改网页界面接口的外部请求来起到防止恶意篡改页面的目的，由于木马程序一般是与运行页面的进程不同的进程运行的，通过阻止这种跨进程的外部请求，就可以很好的起到拦截木马程序的页面修改动作，提高支付交易的安全性。

附图说明

[0012] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术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，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0013] 图 1 是现有的网银支付方式选择页面；

[0014] 图 2 是现有的网银确认支付方式页面；

[0015] 图 3 是木马篡改网页内容时的 url 处理逻辑的示意图；

[0016] 图 4 是本发明实施例中的支付网页防修改方法的一个具体流程示意图；

[0017] 图 5 是本发明实施例中的支付网页防修改方法的另一个具体流程示意图；

[0018] 图 6 是本发明实施例中的支付网页防修改装置的一个具体组成示意图；

[0019] 图 7 是图 6 中的拦截单元的一个具体组成示意图。

具体实施方式

[0020] 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，本领域普通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。

[0021] 为了能清楚的描述本发明实施例中提供的技术方案，此处先简要描述浏览器结构和进程通讯的基本技术。在浏览器技术中，客户进程(即运行浏览器的进程)通过 com 库创建一个 com 组件(组件可实现页面加载和显示)，然后通过客户进程中的代理对象透明的调用组件对象提供的服务，即组件是被浏览器进程加载的模块，而其它进程或浏览器内其它模块可以通过连接点机制和组件进行通信。

[0022] 这样，木马进程也就可以通过连接点机制也可能实现对网页内容的篡改。如图 3 所示，本发明人研究发现木马进程对网页内容的篡改过程如下：首先，通过 InternetExplorer 对象获得当前浏览器的统一资源定位符(Uniform / Universal Resource Locator，url)，然后和 BeforeNavigate2 通知的 url 相比较，查询支付类 url 列表，判断当前页面是否是支付类 url (如，浏览器在 BeforeNavigate2 事件里会传回一个 url，把这个 url 和网银支付类的 url 做比较，如果相匹配就认为是支付页面)，若判断结果为是，则向 InternetExplorer 对象查询 IHTMLDocument2 接口，然后通过 IHTMLDocument2 接口 write 函数修改页面。

[0023] 而发明实施例中，通过在特定的接口拦截特定的请求，来实现对上述恶意篡改的防止。

[0024] 如图 4 所示，为本发明实施例中的支付网页防修改方法的一个具体流程示意图，该方法包括如下步骤。

[0025] 401、判断修改网页界面接口收到的请求是否为外部请求，其中，所述外部请求是指与运行所述网页进程不同的其他进程发出的跨进程请求。

[0026] 如前所述，当木马进程在修改支付页面的内容时，首先需要先连接上连接点，其次需要获知哪些页面是其需要进行修改的页面，然后才能对特定的页面内容进行修改。可见，有三处拦截木马的关键接口，即浏览器事件响应注册接口、浏览器对象接口、HTML 修改接口。即，所述修改网页界面接口包括与修改支付网页内容有关的浏览器事件响应注册接口、浏览器对象接口、HTML 修改接口中的一个或多个。

[0027] 网页进程是指运行当前网页的浏览器进程，由于木马进程是与运行当前页面进程不同的进程，因此通过拦截这种跨进程请求，就可以实现对木马进程的请求的拦截，而不一定要判断这种跨进程请求是否来自木马进程。

[0028] 在本步骤中，判断请求是否为外部请求，可以通过如下方式进行：判断所述修改网页界面接口的调用栈中是否有 RPCRT4.dll 文件；当判断结果为有 RPCRT4.dll 文件时，判断

所述修改网页界面接口收到了外部请求。如，判断连接容器接口、浏览器对象接口、HTML 修改接口的调用栈中是否有 RPCRT4.dll 文件；当判断结果为有 RPCRT4.dll 文件时，则判断所述修改网页界面接口收到了外部请求。

[0029] 同时，一般跨进程的请求有多种，为了进一步提高效率，在本发明的一些具体实施例中可将需要拦截的外部请求确定为以下几种，即本发明实施例中的外部请求包括所述浏览器事件响应注册接口的 Advise 函数、浏览器对象接口的获取本地 URL 函数、HTML 修改接口的写入函数。

[0030] 402、当判断结果为所述请求为外部请求时，拦截所述外部请求。根据接口的不同，拦截的外部请求也有所区别，如，对于浏览器事件响应注册接口，则拦截所述其他进程通过调用所述浏览器事件响应注册接口的 Advise 函数获取浏览器信息；对于浏览器对象接口，则拦截所述其他进程通过调用所述浏览器对象接口的获取本地 URL 函数判断当前页面是否为支付页面；对于 HTML 修改接口，则拦截所述其他进程通过调用所述 HTML 修改接口的写入函数修改支付页面的内容。

[0031] 由于不是所有的网页都是与支付有关的支付网页，因此在实施本发明实施例中在对支付页面进行外部请求拦截时，在步骤 401 中还包括判断所述页面是否为网银支付页面的过程。

[0032] 在判断页面是否为支付页面时，可以通过页面 url 进行判断，如对于一个支付页面，其 url 为 https://netpay.cmbchina.com/netpayment/BaseHttp.dll，则有支付 url 的路径：

[0033] <rule host="https://netpay.cmbchina.com" path="/netpayment/BaseHttp.dll?PrePayC*" level="3"/>

[0034] 通过将该 url 与存储的网银支付类 url 的特征（该特征可以预先定义并存储）进行比较，则可以判断出当前的页面为一网银支付页面。

[0035] 如图 5 所示，为对上述方法的进一步描述，在本发明实施例中包括了在三种不同的拦截点拦截木马修改页面的方式，这三种方式可以都执行，也可以只执行其中一种拦截方式，当然，一般在执行步骤 503 的基础上还执行步骤 501 或 / 和步骤 502 会有较好的拦截效率，以下描述是基于进行页面修改的拦截顺序排列的顺序，并不必然是本发明实施例中进行木马拦截时具体执行顺序。

[0036] 501、防止木马注册浏览器事件回调，即防止木马等恶意程序链接到浏览器（如 IE 浏览器）的组件上。由于，木马要监听浏览器事件一定要调用浏览器事件响应注册接口（如，连接点容器接口 IConnectionPointContainer）的 Advise 函数，因此本步骤中通过拦截来自外部的 Advise 函数，使得木马无法获取浏览器的信息，从而无法篡改页面。

[0037] 502、防止木马获取地址栏 url，即防止木马读取浏览器地址栏的 url。这样可以使木马混淆，弄不清除当前的是不是支付页面。

[0038] 由于木马在浏览器的事件回调内拿到的 url 有许多个（比如一个页面含有 frame 元素，打开这个页面的话，木马就会收到许多条 url），木马必须通过浏览器对象接口（如，IWebBrowser2 接口）的获取本地 URL 函数（如，GetLocationURL 函数）进行判断当前的页面是否是支付页面，因此本步骤中通过拦截 IWebBrowser2 接口的 GetLocationURL 函数，使得木马无法正确的判断支付页面。

[0039] 503、防止木马修改页面内容。不论步骤 501 和 502 中判断结果如何，木马要起到诈骗的目的最终还是要修改用户页面，因此本步骤中通过拦截 HTML 修改接口（如，IHTMLDocument2 接口）的写入函数（如，write 函数）来阻止木马修改页面。

[0040] 同时，在步骤 501~503 中，通过对 IHTMLDocument2、IConnectionPointContainer 和 IWebBrowser2 的调用栈做检查判断当前的函数请求是否是跨进程调用请求，从而阻止木马调用。一般在调用栈中若包括 RPCRT4.dll，则表明当前的函数请求是跨进程调用请求。

[0041] 如图 6 所示，为本发明实施例中的支付网页防修改装置的一个具体组成示意图，图中虚线所示为可选的单元。在实现时，该装置可以是以浏览器插件的形式来实现。

[0042] 该装置 6 可包括：修改接口判断单元 60，用于判断修改网页界面接口收到的请求是否为外部请求，其中，所述外部请求是指与运行所述网页进程不同的其他进程发出的跨进程请求求；拦截单元 62，用于当判断结果为所述请求为外部请求时，拦截所述外部请求。

[0043] 其中，所述修改网页界面接口包括与修改支付网页内容有关的浏览器事件响应注册接口、浏览器对象接口、HTML 修改接口中的一个或多个；所述外部请求则对应的包括所述浏览器事件响应注册接口的 Advise 函数、浏览器对象接口的获取本地 URL 函数、HTML 修改接口的写入函数中的一个或多个。

[0044] 其中，所述修改接口判断单元 60 还用于，判断所述修改网页界面接口的调用栈中是否有 RPCRT4.dll 文件；当判断结果为有 RPCRT4.dll 文件时，判断所述修改网页界面接口收到了外部请求。

[0045] 如图 7 所示，拦截单元 62 可包括下述子单元中的一个或多个：信息拦截子单元 620，用于拦截所述其他进程通过调用所述浏览器事件响应注册接口的 Advise 函数获取浏览器信息； 判断拦截子单元 622，用于拦截所述其他进程通过调用所述浏览器对象接口的获取本地 URL 函数判断当前页面是否为支付页面； 修改拦截子单元 624，用于拦截所述其他进程通过调用所述 HTML 修改接口的写入函数修改支付页面的内容。图 7 所示，为都包括的情况。

[0046] 当然，所述修改接口判断单元 60 只对网银支付页面判断修改网页界面接口收到的请求是否为外部请求，则该单元还可以判断所述页面是否为网银支付页面。

[0047] 可以理解，本实施例中的装置在实现其相应功能时，可以参考前述方法实施例中提供的具体函数、接口等，此处不做一一赘述。

[0048] 在本发明实施例中，通过阻止修改网页界面接口的外部请求来起到防止恶意篡改页面的目的，由于木马程序一般是与运行页面的进程不同的进程运行的，通过阻止这种跨进程的外部请求，就可以很好的起到拦截木马程序的页面修改动作，提高支付交易的安全性。

[0049] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）或随机存储记忆体（Random Access Memory，RAM）等。

[0050] 以上所揭露的仅为本发明一种较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

1、确认购买信息 →2、付款到支付宝 →3、卖家发货，买家确认收货 →4、支付宝付款给卖家
订单名称
收款方
...详单
您的支付宝账户：
可支付余额：0.00 元 账户充值
您的账户没有可支付余额，请使用其他方式付款，或充值后付款。
您可以使用其他方式付款：
储蓄卡
信用卡
网点
消费卡
选择您的付款方式
网上银行：
中国工商银行
招商银行
中国农业银行
交通银行
SPD BANK
广东发展银行
深圳发展银行
中国民生银行

图 1

支付宝 | 收银台
您好，
1、确认购买信息 →2、付款到支付宝 →3、卖家发货，买家确认收货 →4、支付宝付款给卖家
订单名称
收款方
... 详单
付款方式：
中国工商银行
储蓄卡
支付 元
页面内容被篡改
请输入验证码：
刷新
登录到网上银行支付
支付宝卡通：
免费升级到支付宝卡通，永久享受便捷付款
开通后无需登录网上银行，输入支付密码，即可完成付款。
立即开通

图 2

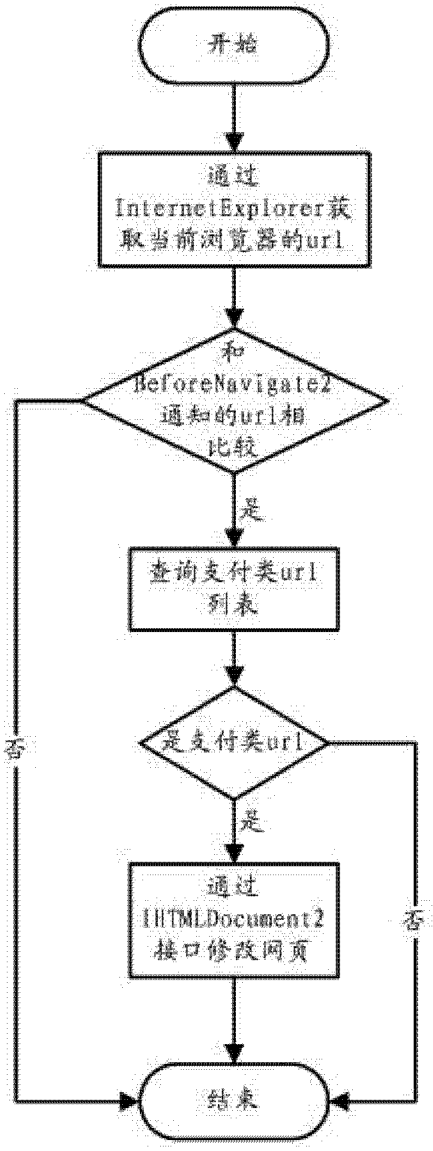

开始
通过InternetExplorer获取当前浏览器的url
和BeforeNavigate2通知的url相比较
是
查询支付类url列表
是支付类url
否
是
通过IHTMLDocument2接口修改网页
否
结束

图 3

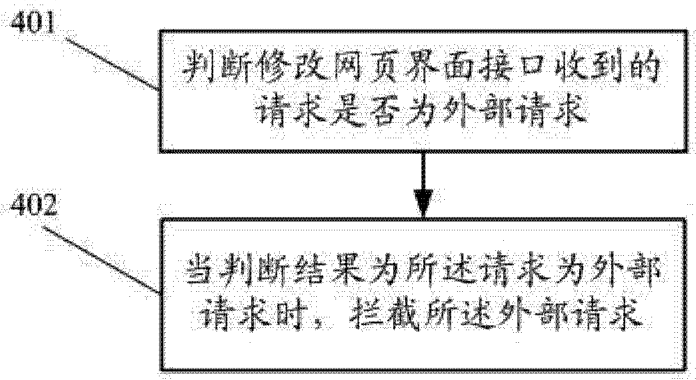

401
判断修改网页界面接口收到的请求是否为外部请求
402
当判断结果为所述请求为外部请求时，拦截所述外部请求

图 4

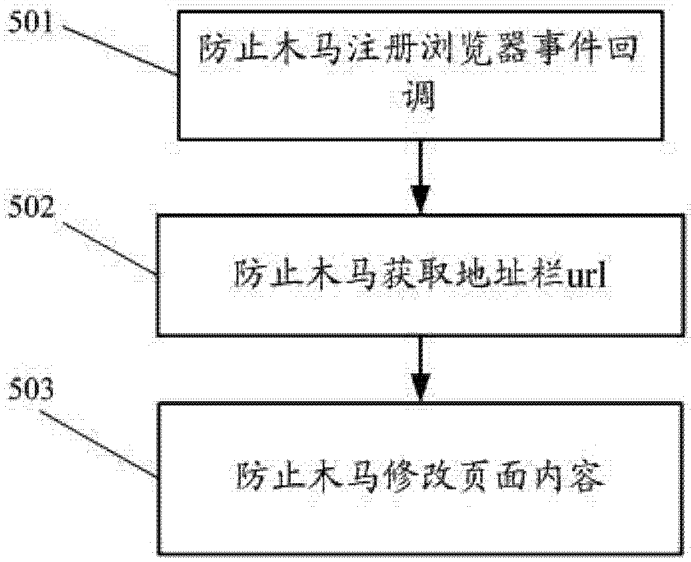

501
防止木马注册浏览器事件回调
502
防止木马获取地址栏url
503
防止木马修改页面内容

图 5

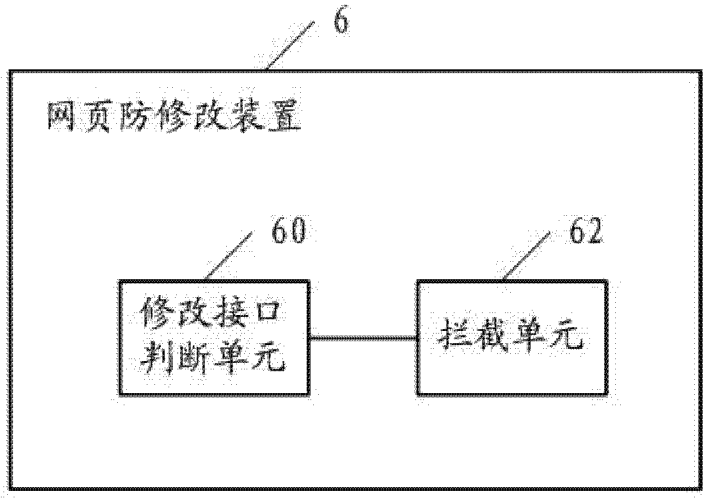

6
网页防修改装置
60
修改接口判断单元
62
拦截单元

图 6

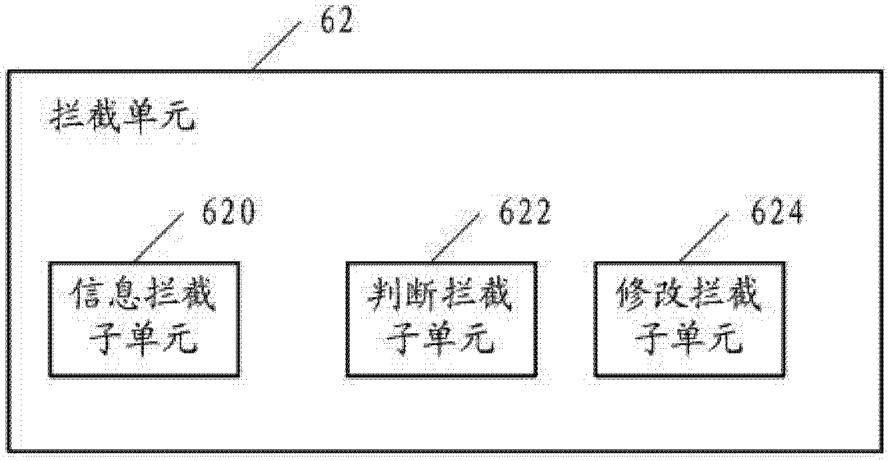


图 7