

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2012 年 10 月 26 日 (26.10.2012)



(10) 国际公布号
WO 2012/142938 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2012/074191
- (22) 国际申请日: 2012 年 4 月 17 日 (17.04.2012)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201110097169X 2011 年 4 月 18 日 (18.04.2011) CN
- (71) 申请人 (对除美国外的所有指定国): 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室 (德胜园区), Beijing 100088 (CN)。
- (72) 发明人; 及
- (75) 发明人/申请人 (仅对美国): 陈宁一 (CHEN, Ningyi) [CN/CN]; 中国北京市朝阳区建国路 71 号惠通时代广场 D 座, Beijing 100025 (CN)。 郑文彬 (ZHENG, Wenbin) [CN/CN]; 中国北京市朝阳区建国路 71 号惠通时代广场 D 座, Beijing 100025 (CN)。 肖鹏 (XIAO, Peng) [CN/CN]; 中国北京市朝阳区建国路 71

号惠通时代广场 D 座, Beijing 100025 (CN)。 朱翼鹏 (ZHU, Yipeng) [CN/CN]; 中国北京市朝阳区建国路 71 号惠通时代广场 D 座, Beijing 100025 (CN)。

- (74) 代理人: 北京市德权律师事务所 (BEIJING DEQUAN LAW FIRM); 中国北京市朝阳区朝外大街乙 12 号昆泰国际大厦 1008 室, Beijing 100020 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,

[见续页]

(54) Title: METHOD AND CLIENT FOR ENSURING USER NETWORK SECURITY

(54) 发明名称: 一种保证用户网络安全性的方法及客户端

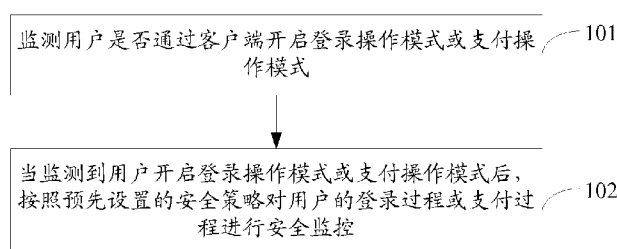


图 1 / Fig.1

101 MONITORING WHETHER A USER ENABLES A LOGIN OPERATION MODE OR PAYMENT OPERATION MODE VIA A CLIENT
102 WHEN MONITORING THAT THE LOGIN OPERATION MODE OR PAYMENT OPERATION MODE IS ENABLED BY THE USER, PERFORMING SECURITY MONITORING FOR THE LOGIN PROCESS OR PAYMENT PROCESS OF THE USER ACCORDING TO A PRESET SECURITY POLICY

(57) Abstract: A method and client for ensuring user network security, the method comprising: monitoring whether a user enables a login operation mode or payment operation mode via a client; when monitoring that the login operation mode or payment operation mode is enabled by the user, performing security monitoring for the login process or payment process of the user according to a preset security policy. By applying the embodiment of the present invention, when a client user is in a login process or online payment process, security protection can be implemented for the login process or payment process via multiple security policies specially used for ensuring the login process or payment process, and network security is ensured for the user during the login process or payment process via risky process interception, executable file prompt and browser invoke monitoring.

(57) 摘要: 一种保证用户网络安全性的方法及客户端, 该方法包括: 监测用户是否通过客户端开启登录操作模式或支付操作模式; 当监测到用户开启登录操作模式或支付操作模式后, 按照预先设置的安全策略对用户的登录过程或支付过程进行安全监控。应用本申请实施例, 当客户端用户处

于登录过程中或在线支付过程中时, 可以通过多种专门用于保障登录过程或支付过程的安全策略对登录过程或支付过程进行安全保护, 通过危险进程拦截、可执行文件提示及浏览器调用监控等, 保证用户在登录过程或支付过程中的网络安全性。

WO 2012/142938 A1



IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG,
CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD,
TG)。

— 发明人资格(细则 4.17(iv))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

根据细则 4.17 的声明:

— 关于申请人有权申请并被授予专利(细则 4.17(ii))

一种保证用户网络安全性的方法及客户端

技术领域

本申请涉及计算机网络技术领域，特别是涉及一种保证用户网络安全性的方法及客户端。

背景技术

随着网络应用的扩展，网络用户可以在线支付各种费用，最常见的应用就是用户登录网上商城购买物品时，通过预先开通的网络银行进行网上转账支付。在通过网络银行支付的过程中，用户需要输入银行卡账号和预先设置的密码，因此保护网络支付的安全性至关重要。现有技术中，恶意第三方往往会通过木马盗取用户的网络银行账号和密码，例如，当用户在网页上点击支付按钮时，可能进入的支付页面是恶意第三方预先设置好的、与正常支付网页相似的恶意网页，一旦用户在恶意网页上输入了用户名和密码，则导致用户信息会被盗取。由此可知，在现有网络支付过程中，用户网银容易被盗用，导致网络安全性不高，容易给用户造成损失。

发明内容

为了解决上述技术问题，本申请实施例提供了一种保证用户网络安全性的方法及客户端，以解决现有网络支付过程中用户信息容易被盗取，导致网络安全性不高的问题。

本申请实施例公开了如下技术方案：

一种保证用户网络安全性的方法，包括：

监测用户是否通过客户端开启登录操作模式或支付操作模式；

当监测到用户开启登录操作模式或支付操作模式后，按照预先设置的安全策略对用户的登录过程或支付过程进行安全监控，以便当监控到不安全事件时，向用户进行提示或者阻止所述不安全事件的执行。

其中，

所述监测用户是否通过客户端开启登录操作模式或支付操作模式包括：监

测用户是否通过客户端浏览器开启登录操作模式或支付操作模式。

其中,所述按照预先设置的安全策略对用户的登录过程或支付过程进行安全监控包括至少一种下述方式:

通过预设的进程列表对登录过程或支付过程中的危险进程进行监控;

对登录过程或支付过程中传输的可执行文件进行监控;

对登录过程或支付过程中的浏览器调用行为进行监控;

对登录过程或支付过程中的键盘输入内容的调用进行监控;

对登录过程或支付过程中客户端传输的数据对象进行监控;

对登录过程或支付过程中所开启的网页进行监控。

其中,所述通过预设的进程列表对登录过程或支付过程中的危险进程进行监控包括:

获取所述登录过程或支付过程中开启的当前进程,当在预置的白名单列表中未查找到所述当前进程时,则将所述当前进程确定为危险进程进行拦截,其中,所述预置的白名单列表中用于保存已经确认的对系统没有威胁的安全进程;或者,

获取所述登录过程或支付过程中开启的当前进程,当在预置的黑名单列表中查找到所述当前进程时,则将所述当前进程确定为危险进程进行拦截,其中,所述预置的黑名单列表中用于保存已经确认的对系统存在威胁的危险进程。

其中,所述对登录过程或支付过程中传输的可执行文件进行监控包括:

当监测到客户端准备接收可执行文件时,或者处于接收可执行文件过程中时,或者接收了可执行文件时,通过查找预置的可执行文件列表,确定所述可执行文件是否为可疑文件。

其中,所述通过查找预置的可执行文件列表,确定所述可执行文件是否为可疑文件包括:

当在预置的白名单中未查找到所述可执行文件时,则将所述可执行文件确定为可疑文件,其中,所述预置的白名单中用于保存所有安全的可执行文件;或者,

当在预置的黑名单中查找到所述可执行文件时,则将所述可执行文件确定为可疑文件,其中,所述预置的黑名单中用于保存所有危险的可执行文件。

其中,所述对登录过程或支付过程中传输的可执行文件进行监控包括:

当监测到客户端接收了可执行文件时，提取所述可执行文件中的行为特征，判断从可执行文件中提取的行为特征是否为预先记录的安全行为特征，如果不是，则将所述可执行文件确定为可以文件。

其中，所述对登录过程或支付过程中的浏览器调用行为进行监控包括：

通过底层驱动监控进程之间通讯的相关函数；

当监控到通过远程过程调用接口对浏览器进程进行操作所触发的相关函数调用时，拦截相应的调用事件；

解析所述调用事件，过滤出发起所述调用事件的进程；

通过查找预先设置的进程名单确定所述发起调用事件的进程是否为非法进程。

一种客户端，包括：

监测单元，用于监测用户是否通过客户端开启登录操作模式或支付操作模式；

监控单元，用于当监测到用户开启登录操作模式或支付操作模式后，按照预先设置的安全策略对用户的登录过程或支付过程进行安全监控，以便当监控到不安全事件时，向用户进行提示或者阻止所述不安全事件的执行。

其中，

所述监测单元，具体用于监测用户是否通过客户端浏览器开启登录操作模式或支付操作模式。

其中，所述监控单元包括至少一个下述单元：

危险进程监控单元，用于通过预设的进程列表对登录过程或支付过程中的危险进程进行监控；

可执行文件监控单元，用于对登录过程或支付过程中传输的可执行文件进行监控；

浏览器调用监控单元，用于对登录过程或支付过程中的浏览器调用行为进行监控；

输入内容调用监控单元，用于对登录过程或支付过程中的键盘输入内容的调用进行监控；

数据对象监控单元，用于对登录过程或支付过程中客户端传输的数据对象进行监控；

网页监控单元, 用于对登录过程或支付过程中所开启的网页进行监控。

其中, 所述危险进程监控单元包括至少一个下述单元:

白名单拦截单元, 用于获取所述登录过程或支付过程中开启的当前进程, 当在预置的白名单列表中未查找到所述当前进程时, 则将所述当前进程确定为危险进程进行拦截, 其中, 所述预置的白名单列表中用于保存已经确认的对系统没有威胁的安全进程;

黑名单拦截单元, 用于获取所述登录过程或支付过程中开启的当前进程, 当在预置的黑名单列表中查找到所述当前进程时, 则将所述当前进程确定为危险进程进行拦截, 其中, 所述预置的黑名单列表中用于保存已经确认的对系统存在威胁的危险进程。

其中, 所述可执行文件监控单元包括:

第一可执行文件监控单元, 用于当监测到客户端准备接收可执行文件时, 或者处于接收可执行文件过程中时, 或者接收了可执行文件时, 通过查找预置的可执行文件列表, 确定所述可执行文件是否为可疑文件。

其中, 所述第一可执行文件监控单元包括:

白名单监控单元, 用于当在预置的白名单中未查找到所述可执行文件时, 则将所述可执行文件确定为可疑文件, 其中, 所述预置的白名单中用于保存所有安全的可执行文件; 或者,

黑名单监控单元, 用于当在预置的黑名单中查找到所述可执行文件时, 则将所述可执行文件确定为可疑文件, 其中, 所述预置的黑名单中用于保存所有危险的可执行文件。

其中, 所述可执行文件监控单元包括:

第二可执行文件监控单元, 用于当监测到客户端接收了可执行文件时, 提取所述可执行文件中的行为特征, 判断从可执行文件中提取的行为特征是否为预先记录的安全行为特征, 如果不是, 则将所述可执行文件确定为可以文件。

其中, 所述浏览器调用监控单元包括:

函数监控单元, 用于通过底层驱动监控进程之间通讯的相关函数;

调用事件拦截单元, 用于当监控到通过远程过程调用接口对浏览器进程进行操作所触发的相关函数调用时, 拦截相应的调用事件;

调用事件解析单元, 用于解析所述调用事件, 过滤出发起所述调用事件的

进程;

非法进程确定单元,用于通过查找预先设置的进程名单确定所述发起调用事件的进程是否为非法进程。

由上述实施例可以看出,本申请实施例中在监测到用户开启登录操作模式或支付操作模式后,按照预先设置的安全策略对用户的登录过程或支付过程进行安全监控。应用本申请实施例,当客户端用户处于登录过程中或在线支付过程中时,可以通过多种专门用于保障登录过程或支付过程的安全策略对登录过程或支付过程进行安全保护,通过危险进程拦截、可执行文件提示及浏览器调用监控等,保证用户在登录过程或支付过程中的网络安全性。

附图说明

为了更清楚地说明本申请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,对于本领域普通技术人员而言,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。

图1为本申请保证用户网络安全性的方法的第一实施例流程图;

图2为本申请保证用户网络安全性的方法的第二实施例流程图;

图3为本申请保证用户网络安全性的方法的第三实施例流程图;

图4为本申请保证用户网络安全性的方法的第四实施例流程图;

图5为本申请客户端的实施例框图。

具体实施方式

本发明如下实施例提供了一种保证用户网络安全性的方法及客户端。

为了使本技术领域的人员更好地理解本发明实施例中的技术方案,并使本发明实施例的上述目的、特征和优点能够更加明显易懂,下面结合附图对本发明实施例中技术方案作进一步详细的说明。

参见图1,为申请保证用户网络安全性的方法的第一实施例流程图:

步骤101:监测用户是否通过客户端开启登录操作模式或支付操作模式。

本申请实施例可以特别应用在用户通过客户端进行网络支付的过程中,即检测用户是否通过客户端开启了支付页面。以保证支付过程中用户信息不会泄

露,提高网络支付的安全性。具体的,监测用户是否通过客户端浏览器开启登录操作模式或支付操作模式。

步骤 102: 当监测到用户开启登录操作模式或支付操作模式后,按照预先设置的安全策略对用户的登录过程或支付过程进行安全监控。

其中,安全策略为预先针对登录操作模式或支付操作模式所设置的安全策略。

客户端可以通过预设的进程列表对登录过程或支付过程中的危险进程进行监控;或者通过预设的安全的可执行文件列表对登录过程或支付过程中传输的可执行文件进行监控;或者对登录过程或支付过程中的浏览器调用行为进行监控;或者对登录过程或支付过程中的键盘输入内容的调用进行监控;或者对登录过程或支付过程中客户端传输的数据对象进行监控,例如,当监控到客户端向与登录过程或支付过程无关的对象传输与登录或支付相关的数据时,则应当拦截所传输的数据对象;或者对登录过程或支付过程中所开启的网页进行监控,例如,在登录过程或支付过程中,用户可能开启的支付网页为恶意第三方伪造的与真实支付网页类似的网页,因此需要对所开启的网页进行监控。

需要说明的是,上述所列六种安全策略执行方式可以在整个监控过程中并行执行,或者根据需要选择其中至少一个进行执行,对此本申请实施例不进行限制。

参见图 2,为本申请保证用户网络安全性的方法的第二实施例流程图,该实施例以在线支付为例,示出了对危险进程进行监控的过程:

步骤 201: 监测用户在客户端上的操作。

步骤 202: 根据监测结果判断用户是否开始在线支付,若是,则执行步骤 203; 否则,返回步骤 201。

在用户的客户端可以预先保存一个支付网站列表,当监测到用户打开浏览器后,获取浏览器访问页面的 URL (Uniform / Universal Resource Locator, 网页地址), 将获取的 URL 与支付网站列表中的支付网站 URL 进行对比, 如果找到一致的 URL, 则可确认用户进入了支付页面, 并开始在线支付。

步骤 203: 根据已开启的当前进程查找预设的白名单列表。

白名单列表中保存的是已经确认的对系统没有威胁的安全进程, 因此对于

这些进程可以不进行拦截。

白名单列表通常保存在本地，因此查找白名单列表的操作也相应在本地执行。进一步，也可以结合云查杀的方式，在当前进程运行的过程中，连接云服务器，通过网络中已经存在的多个白名单列表对当前进程是否为安全进程进行查找。

在整个在线支付过程中，可能会开启多个进程，当每个进程开启后，该进程都作为当前进程对其执行查找白名单列表的操作。

步骤 204：判断是否在白名单列表中查找到当前进程，若未查找到，则执行步骤 205；否查找到，则执行步骤 206。

步骤 205：将当前进程作为危险进程进行拦截。

对于未在白名单列表中的进程，可以将其直接作为危险进程进行拦截，也可以对用户进行提示，由用户选择是否允许该进程的执行，或者阻止该进程的执行。对于未在白名单列表中的进程，可以向用户提供限制这些进程执行的功能，包括但不限于冻结进程、隔离进程、终止进程。

本实施例以白名单查找为例，示出了对危险进程的拦截过程，实际应用过程中，也可以预设黑名单列表，当在所述黑名单列表中查找到当前进程时，则将所述当前进程作为危险进程进行拦截；对于既不在白名单也不在黑名单中的进程，可以对用户进行提示，由用户选择是否阻止这些进程的运行，防止未知进程中可能存在的危险进程。

步骤 206：判断用户是否已经结束在线支付，若是，则结束流程；否则，返回步骤 203。

参见图 3，为本申请保证用户网络安全性的方法的第三实施例流程图，该实施例以在线支付为例，示出了通过预设的安全的可执行文件列表对安全支付过程中接收到的可执行文件进行监控的过程：

步骤 301：监测用户在客户端上的操作。

步骤 302：根据监测结果判断用户是否开始在线支付，若是，则执行步骤 303；否则，返回步骤 301。

在用户的客户端可以预先保存一个支付网站列表，当监测到用户打开浏览器后，获取浏览器访问页面的 URL，将获取的 URL 与支付网站列表中的支付网

站 URL 进行对比, 如果找到一致的 URL, 则可确认用户进入了支付页面, 并开始在线支付。

步骤 303: 判断客户端是否接收到可执行文件, 若是, 则执行步骤 304; 否则, 返回步骤 303。

用户在线支付的过程中, 可能接收到第三方传输给用户的可执行文件(例如后缀为.exe 的文件), 这些可执行文件有些是支付过程中需要使用的文件, 有些则是恶意第三方发送给用户的危险文件。上述这些文件可能通过即时通信工具传输给用户所在的终端设备、通过下载或分享的方式诱导用户下载到其所在的终端设备、通过挂木马或病毒传播等非法方式传播到用户所在的终端设备、或者在拷贝移动存储设备中的文件时传输到用户所在的终端设备。

在检测可执行文件时, 可以通过用户的即时通信工具、浏览器等进行监控, 也可以在文件被下载到本地时实时检测到; 另外, 可执行文件在启动运行时, 以及启动运行后, 也都能够被系统检测到。

步骤 304: 查找预先设置的安全的可执行文件列表。

安全的可执行文件列表中可以记录文件的大小、文件的时间、文件的 MD5 信息、文件的签名等。

安全的可执行文件列表可以采用白名单的方式, 通过白名单保存所有安全的可执行文件; 或者采用黑名单的方式, 通过黑名单保存所有危险的可执行文件; 或者, 采用行为特征的方式, 记录所有安全行为特征, 在接收到可执行文件后, 提取可执行文件中的行为特征, 判断从可执行文件中提取的行为特征是否满足所记录的安全行为特征, 对于满足安全行为特征的文件则可确认为安全的可执行文件。

步骤 305: 判断是否在可执行文件列表中查找到接收的可执行文件, 若是, 则执行步骤 306; 否则, 执行步骤 307。

步骤 306: 输出请求用户选择是否运行所述可执行文件的选择提示信息。

步骤 307: 判断用户是否已经结束在线支付, 若是, 则结束流程; 否则, 返回步骤 303。

除了上述实施例所示出的对安全支付过程中接收到的可执行文件进行监控外, 也可以对客户端准备接收的可执行文件, 或者正在接收的可执行文件进行监控。具体的, 当监测到客户端准备接收可执行文件时, 查找预先设置的安

全的可执行文件列表，如果未在可执行文件列表中查找到该可执行文件，则确定该可执行文件为可疑文件，输出请求用户选择是否接收该可执行文件的选择提示信息；当监测到客户端处于接收可执行文件过程中时，查找预先设置的安全的可执行文件列表，如果未在可执行文件列表中查找到该可执行文件，则确定该可执行文件为可疑文件，输出请求用户选择是否接续接收该可执行文件的选择提示信息。

参见图 4，为本申请保证用户网络安全性的方法的第四实施例流程图，该实施例以在线支付为例，示出了对安全支付过程中的浏览器调用行为进行监控的过程：

步骤 401：监测用户在客户端上的操作。

步骤 402：根据监测结果判断用户是否开始在线支付，若是，则执行步骤 403；否则，返回步骤 401。

在用户的客户端可以预先保存一个支付网站列表，当监测到用户打开浏览器后，获取浏览器访问页面的 URL，将获取的 URL 与支付网站列表中的支付网站 URL 进行对比，如果找到一致的 URL，则可确认用户进入了支付页面，并开始在线支付。

步骤 403：通过底层驱动监控进程之间通讯的相关函数。

对于在线支付过程，底层驱动监控的进程之间的通讯函数可以包括如下示例的 API（Application Programming Interface，应用程序编程接口）函数：

NtAlpcSendWaitReceivePort

NtRequestWaitReplyPort

NtRequestPort

步骤 404：判断是否监控到通过远程过程调用接口对浏览器进程进行操作所触发的相关函数调用，若是，则执行步骤 405；否则，返回步骤 403。

当有程序试图调用进程之间通讯的相关函数时，会通过远程过程调用接口（例如，COM 接口）对浏览器进程的接口进行操作，当该操作试图控制浏览器进程的网址或页面内容时，会监控到相应的函数调用事件，此时就会触发对函数调用进行拦截。

步骤 405：拦截相应的调用事件，并解析调用事件，过滤出发起该调用事

件的进程。

拦截到的调用事件即为对函数调用的事件，通常函数调用是 RPC (Remote Procedure Call, 远程过程调用) 过程中调用的函数，此时对调用函数进行解析，例如，如果解析的调用函数为 NtRequestWaitReplyPort，则解析出的相关函数可以包括 RequestMessage、PortHandle 等。

在过滤通过远程过程调用接口对浏览器进程进行操作所触发的函数调用时，例如，A 进程试图操作浏览器进程 B，以跳转到恶意网址 C，达到劫持在线支付的网购过程，则 A 进程会连接浏览器进程 B 的远程过程调用接口，并产生一个端口句柄 (PortHandle)，然后将要调用的调用序号和跳转网址等信息封装到函数 NtRequestWaitReplyPort 的参数 RequestMessage 中，RequestMessage 为一个缓存地址，最后调用 NtRequestWaitReplyPortAPI 函数，将跳转请求发送给浏览器进程 B 的远程过程调用端口，实现跳转操控过程。本实施例中通过拦截、监视这个函数 NtRequestWaitReplyPort，从参数 RequestMessage 的缓存中解析并还原出所调用函数的调用序号和跳转网址等信息，将这些信息识别为一个操作浏览器调用事件，并获取触发该浏览器调用事件的 A 进程。

步骤 406：查找预先设置的进程名单。

在获取到触发浏览器调用事件的 A 进程后，可以获得该进程的进程 ID、执行路径、对应文件的文件信息等。根据执行路径获取对应文件，并对文件的摘要进行计算，获取代表该文件唯一性的哈希信息。

其中，进程名单可以采用白名单方式或者黑名单方式。在采用白名单方式时，在白名单中包含了所有安全进程对应文件的哈希信息，将获取到的进程的哈希信息与该白名单中的哈希信息进行比较，如果存在一致的哈希信息，则表示获取到的进程为安全进程，不用进行拦截；如果还存在黑名单，则对与黑名单中哈希信息匹配一致的进程进行拦截并发出警报；对于既不在白名单也不在黑名单中的哈希信息对应的进程，则可以进行拦截并向用户发出提示。

步骤 407：根据查找结果判断该进程是否为非法进程，若是，则执行步骤 408；否则，执行步骤 409。

步骤 408：拒绝该调用事件。

步骤 409：判断用户是否已经结束在线支付，若是，则结束流程；否则，

返回步骤 403。

由上述实施例可见,当客户端用户进行登录操作,特别是在线支付过程中,可以通过多种安全策略对支付过程进行安全保护,通过对危险进程进行拦截、对可执行文件进行提示及对浏览器调用进行监控等,保证用户在登录过程中的网络安全性。

与本申请保证用户网络安全性的方法的实施例相对应,本申请还提供了客户端的实施例。

参见图 5,为本申请客户端的实施例框图。

该客户端包括:监测单元 510 和监控单元 520。

其中,监测单元 510,用于监测用户是否通过客户端开启登录操作模式或支付操作模式;

监控单元 520,用于当监测到用户开启登录操作模式或支付操作模式后,按照预先设置的安全策略对用户的登录过程或支付过程进行安全监控,以便当监控到不安全事件时,向用户进行提示或者阻止所述不安全事件的执行。

其中,所述安全策略为预先设置的专用于保障所述登录过程或支付过程的安全策略;所述监测单元 510,具体用于监测用户是否通过客户端浏览器开启登录操作模式或支付操作模式。

其中,监控单元 520 可以包括至少一个下述单元(图 5 中未示出):

危险进程监控单元,用于通过预设的进程列表对登录过程或支付过程中的危险进程进行监控;

可执行文件监控单元,用于对登录过程或支付过程中传输的可执行文件进行监控;

浏览器调用监控单元,用于对登录过程或支付过程中的浏览器调用行为进行监控;

输入内容调用监控单元,用于对登录过程或支付过程中的键盘输入内容的调用进行监控;

数据对象监控单元,用于对登录过程或支付过程中客户端传输的数据对象进行监控;

网页监控单元,用于对登录过程或支付过程中所开启的网页进行监控。

具体的，危险进程监控单元可以包括至少一个下述单元：

白名单拦截单元，用于预设白名单列表，获取所述登录过程或支付过程中的当前进程，当在所述白名单列表中未查找到所述当前进程时，则将所述当前进程作为危险进程进行拦截；

黑名单拦截单元，用于预设黑名单列表，获取所述登录过程或支付过程中的当前进程，当在所述黑名单列表中查找到所述当前进程时，则将所述当前进程作为危险进程进行拦截。

具体的，可执行文件监控单元可以包括至少一个下述单元：

第一可执行文件监控单元，用于当监测到客户端准备接收可执行文件时，查找预先设置的可执行文件列表，如果未在所述可执行文件列表中查找到所述可执行文件，则确定所述可执行文件为可疑文件，还可以输出请求用户选择是否接收所述可执行文件的选择提示信息；或者，当监测到客户端处于接收可执行文件过程中时，查找预先设置的可执行文件列表，如果未在所述可执行文件列表中查找到所述可执行文件，则确定所述可执行文件为可疑文件，输出请求用户选择是否接续接收所述可执行文件的选择提示信息；或者，当监测到客户端接收了可执行文件时，查找预先设置的可执行文件列表，如果未在所述可执行文件列表中查找到所述可执行文件，则确定所述可执行文件为可疑文件，输出请求用户选择是否运行所述可执行文件的选择提示信息。

其中，第一可执行文件监控单元可以包括：

白名单监控单元，用于当在预置的白名单中未查找到所述可执行文件时，则将所述可执行文件确定为可疑文件，其中，所述预置的白名单中用于保存所有安全的可执行文件；或者，

黑名单监控单元，用于当在预置的黑名单中查找到所述可执行文件时，则将所述可执行文件确定为可疑文件，其中，所述预置的黑名单中用于保存所有危险的可执行文件。

在另一种实现方式下，可执行文件监控单元可以包括：

第二可执行文件监控单元，用于当监测到客户端接收了可执行文件时，提取所述可执行文件中的行为特征，判断从可执行文件中提取的行为特征是否为预先记录的安全行为特征，如果不是，则将所述可执行文件确定为可以文件。

具体的，浏览器调用监控单元可以包括：

函数监控单元, 用于通过底层驱动监控进程之间通讯的相关函数;

调用事件拦截单元, 用于当监控到通过远程过程调用接口对浏览器进程进行操作所触发的相关函数调用时, 拦截相应的调用事件;

调用事件解析单元, 用于解析所述调用事件, 过滤出发起所述调用事件的进程;

非法进程确定单元, 用于通过查找预先设置的进程名单确定所述发起调用事件的进程是否为非法进程, 所述进程名单包括白名单或者黑名单;

在需要阻止这种不安全事件的执行时, 还可以包括调用事件拒绝单元, 用于当确定所述进程为非法进程时, 拒绝所述调用事件。

通过对以上实施方式的描述可知, 本申请实施例中在监测到用户开启登录操作模式或支付操作模式后, 按照预先设置的安全策略对用户的登录过程或支付过程进行安全监控。应用本申请实施例, 当客户端用户处于登录过程中或在线支付过程中时, 可以通过多种专门用于保障登录过程或支付过程的安全策略对登录过程或支付过程进行安全保护, 通过危险进程拦截、可执行文件提示及浏览器调用监控等, 保证用户在登录过程或支付过程中的网络安全性。

本领域的技术人员可以清楚地了解到本发明实施例中的技术可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解, 本发明实施例中的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来, 该计算机软件产品可以存储在存储介质中, 如 ROM/RAM、磁碟、光盘等, 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) 执行本发明各个实施例或者实施例的某些部分所述的方法。

本说明书中的各个实施例均采用递进的方式描述, 各个实施例之间相同相似的部分互相参见即可, 每个实施例重点说明的都是与其他实施例的不同之处。尤其, 对于系统实施例而言, 由于其基本相似于方法实施例, 所以描述的比较简单, 相关之处参见方法实施例的部分说明即可。

以上所述的本发明实施方式, 并不构成对本发明保护范围的限定。任何在本发明的精神和原则之内所作的修改、等同替换和改进等, 均应包含在本发明的保护范围之内。

权 利 要 求 书

1、一种保证用户网络安全性的方法，其特征在于，包括：

监测用户是否通过客户端开启登录操作模式或支付操作模式；

当监测到用户开启登录操作模式或支付操作模式后，按照预先设置的安全策略对用户的登录过程或支付过程进行安全监控，以便当监控到不安全事件时，向用户进行提示或者阻止所述不安全事件的执行。

2、根据权利要求1所述的方法，其特征在于，

所述监测用户是否通过客户端开启登录操作模式或支付操作模式包括：监测用户是否通过客户端浏览器开启登录操作模式或支付操作模式。

3、根据权利要求1所述的方法，其特征在于，所述按照预先设置的安全策略对用户的登录过程或支付过程进行安全监控包括至少一种下述方式：

通过预设的进程列表对登录过程或支付过程中的危险进程进行监控；

对登录过程或支付过程中传输的可执行文件进行监控；

对登录过程或支付过程中的浏览器调用行为进行监控；

对登录过程或支付过程中的键盘输入内容的调用进行监控；

对登录过程或支付过程中客户端传输的数据对象进行监控；

对登录过程或支付过程中所开启的网页进行监控。

4、根据权利要求3所述的方法，其特征在于，所述通过预设的进程列表对登录过程或支付过程中的危险进程进行监控包括：

获取所述登录过程或支付过程中开启的当前进程，当在预置的白名单列表中未查找到所述当前进程时，则将所述当前进程确定为危险进程进行拦截，其中，所述预置的白名单列表中用于保存已经确认的对系统没有威胁的安全进程；或者，

获取所述登录过程或支付过程中开启的当前进程，当在预置的黑名单列表中查找到所述当前进程时，则将所述当前进程确定为危险进程进行拦截，其中，所述预置的黑名单列表中用于保存已经确认的对系统存在威胁的危险进程。

5、根据权利要求3所述的方法，其特征在于，所述对登录过程或支付过程中传输的可执行文件进行监控包括：

当监测到客户端准备接收可执行文件时，或者处于接收可执行文件过程中时，或者接收了可执行文件时，通过查找预置的可执行文件列表，确定所述可

执行文件是否为可疑文件。

6、根据权利要求 5 所述的方法，其特征在于，所述通过查找预置的可执行文件列表，确定所述可执行文件是否为可疑文件包括：

当在预置的白名单中未查找到所述可执行文件时，则将所述可执行文件确定为可疑文件，其中，所述预置的白名单中用于保存所有安全的可执行文件；或者，

当在预置的黑名单中查找到所述可执行文件时，则将所述可执行文件确定为可疑文件，其中，所述预置的黑名单中用于保存所有危险的可执行文件。

7、根据权利要求 3 所述的方法，其特征在于，所述对登录过程或支付过程中传输的可执行文件进行监控包括：

当监测到客户端接收了可执行文件时，提取所述可执行文件中的行为特征，判断从可执行文件中提取的行为特征是否为预先记录的安全行为特征，如果不是，则将所述可执行文件确定为可以文件。

8、根据权利要求 3 所述的方法，其特征在于，所述对登录过程或支付过程中的浏览器调用行为进行监控包括：

通过底层驱动监控进程之间通讯的相关函数；

当监控到通过远程过程调用接口对浏览器进程进行操作所触发的相关函数调用时，拦截相应的调用事件；

解析所述调用事件，过滤出发起所述调用事件的进程；

通过查找预先设置的进程名单确定所述发起调用事件的进程是否为非法进程。

9、一种客户端，其特征在于，包括：

监测单元，用于监测用户是否通过客户端开启登录操作模式或支付操作模式；

监控单元，用于当监测到用户开启登录操作模式或支付操作模式后，按照预先设置的安全策略对用户的登录过程或支付过程进行安全监控，以便当监控到不安全事件时，向用户进行提示或者阻止所述不安全事件的执行。

10、根据权利要求 9 所述的客户端，其特征在于，

所述监测单元，具体用于监测用户是否通过客户端浏览器开启登录操作模

式或支付操作模式。

11、根据权利要求 9 所述的客户端，其特征在于，所述监控单元包括至少一个下述单元：

危险进程监控单元，用于通过预设的进程列表对登录过程或支付过程中的危险进程进行监控；

可执行文件监控单元，用于对登录过程或支付过程中传输的可执行文件进行监控；

浏览器调用监控单元，用于对登录过程或支付过程中的浏览器调用行为进行监控；

输入内容调用监控单元，用于对登录过程或支付过程中的键盘输入内容的调用进行监控；

数据对象监控单元，用于对登录过程或支付过程中客户端传输的数据对象进行监控；

网页监控单元，用于对登录过程或支付过程中所开启的网页进行监控。

12、根据权利要求 11 所述的客户端，其特征在于，所述危险进程监控单元包括至少一个下述单元：

白名单拦截单元，用于获取所述登录过程或支付过程中开启的当前进程，当在预置的白名单列表中未查找到所述当前进程时，则将所述当前进程确定为危险进程进行拦截，其中，所述预置的白名单列表中用于保存已经确认的对系统没有威胁的安全进程；

黑名单拦截单元，用于获取所述登录过程或支付过程中开启的当前进程，当在预置的黑名单列表中查找到所述当前进程时，则将所述当前进程确定为危险进程进行拦截，其中，所述预置的黑名单列表中用于保存已经确认的对系统存在威胁的危险进程。

13、根据权利要求 11 所述的客户端，其特征在于，所述可执行文件监控单元包括：

第一可执行文件监控单元，用于当监测到客户端准备接收可执行文件时，或者处于接收可执行文件过程中时，或者接收了可执行文件时，通过查找预置的可执行文件列表，确定所述可执行文件是否为可疑文件。

14、根据权利要求 13 所述的客户端，其特征在于，所述第一可执行文件

监控单元包括:

白名单监控单元, 用于当在预置的白名单中未查找到所述可执行文件时, 则将所述可执行文件确定为可疑文件, 其中, 所述预置的白名单中用于保存所有安全的可执行文件; 或者,

黑名单监控单元, 用于当在预置的黑名单中查找到所述可执行文件时, 则将所述可执行文件确定为可疑文件, 其中, 所述预置的黑名单中用于保存所有危险的可执行文件。

15、根据权利要求 11 所述的客户端, 其特征在于, 所述可执行文件监控单元包括:

第二可执行文件监控单元, 用于当监测到客户端接收了可执行文件时, 提取所述可执行文件中的行为特征, 判断从可执行文件中提取的行为特征是否为预先记录的安全行为特征, 如果不是, 则将所述可执行文件确定为可以文件。

16、根据权利要求 11 所述的客户端, 其特征在于, 所述浏览器调用监控单元包括:

函数监控单元, 用于通过底层驱动监控进程之间通讯的相关函数;

调用事件拦截单元, 用于当监控到通过远程过程调用接口对浏览器进程进行操作所触发的相关函数调用时, 拦截相应的调用事件;

调用事件解析单元, 用于解析所述调用事件, 过滤出发起所述调用事件的进程;

非法进程确定单元, 用于通过查找预先设置的进程名单确定所述发起调用事件的进程是否为非法进程。

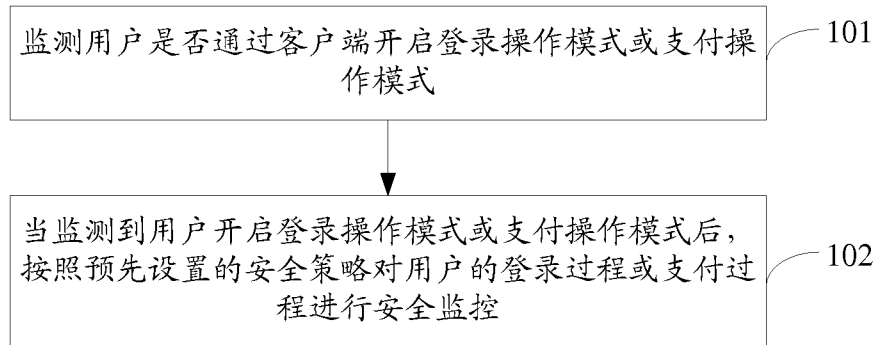


图 1

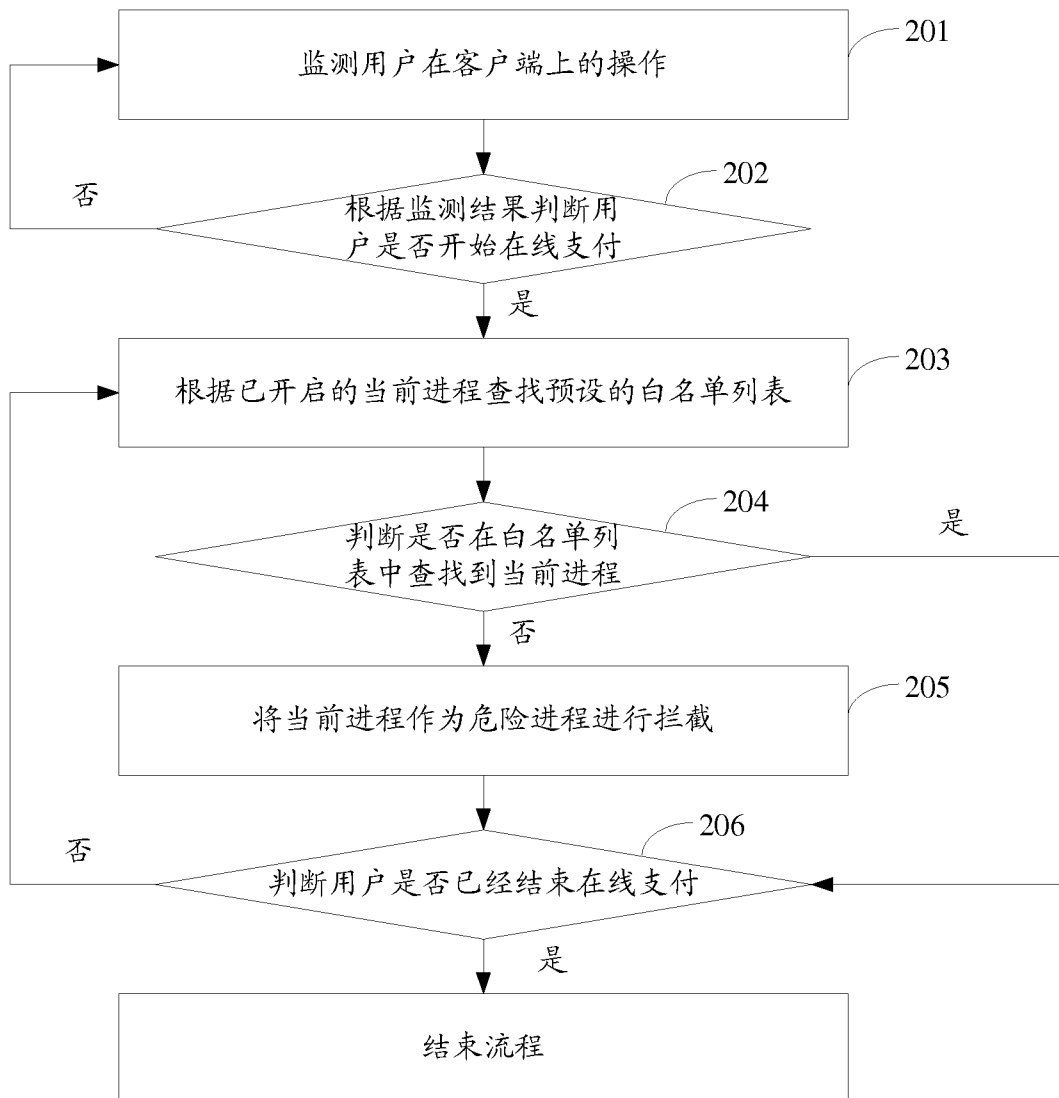


图 2

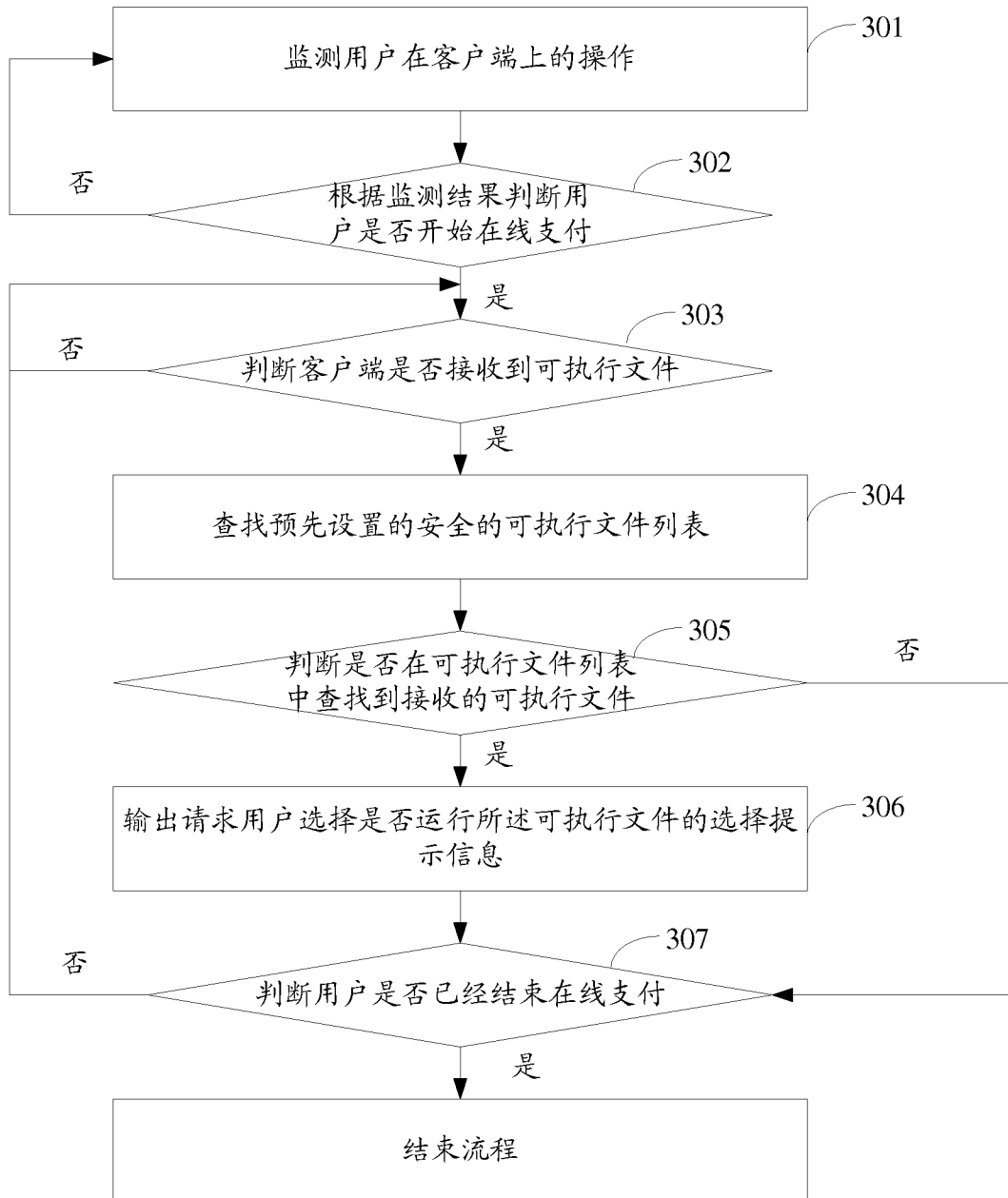


图 3

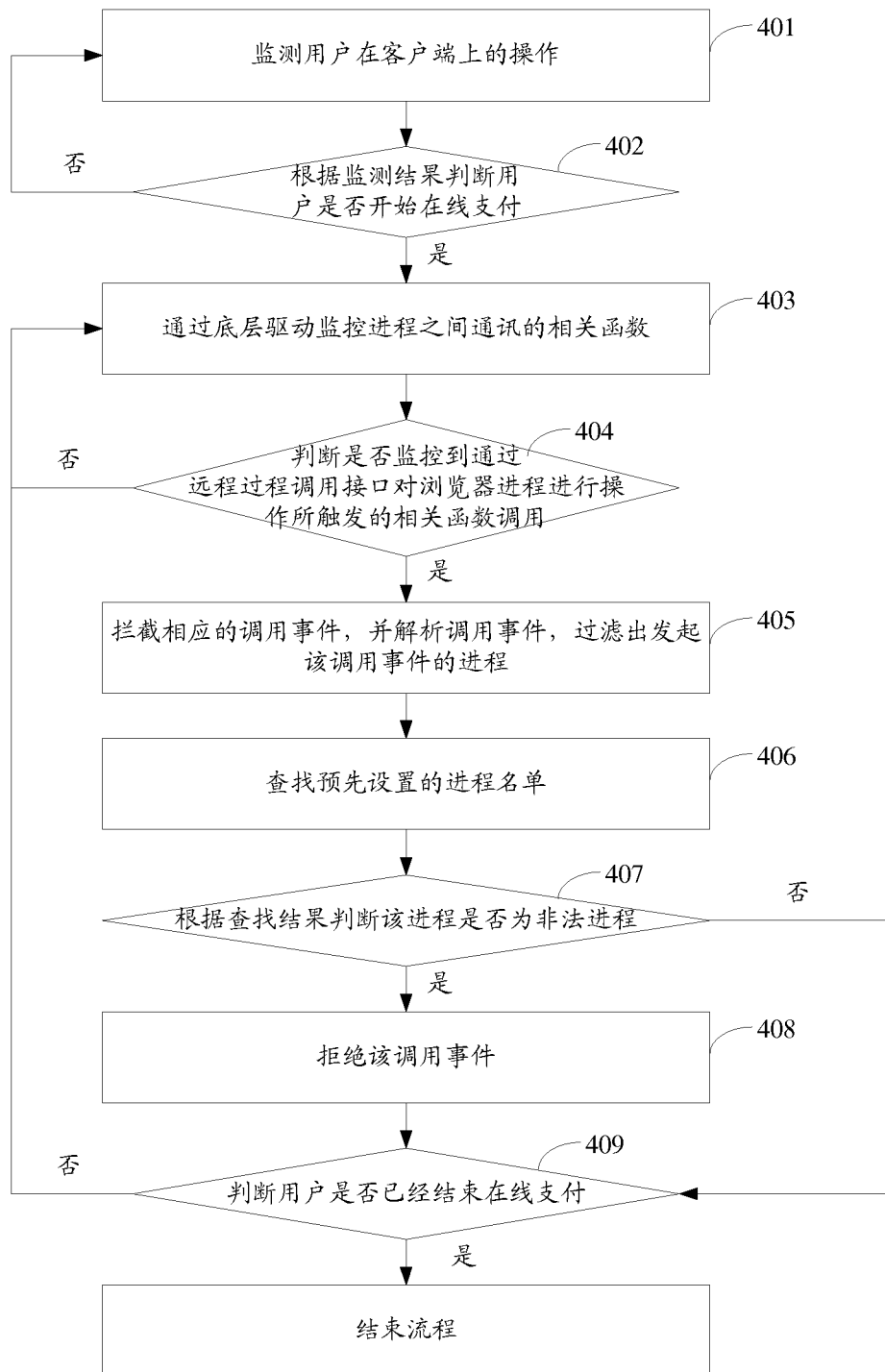


图 4

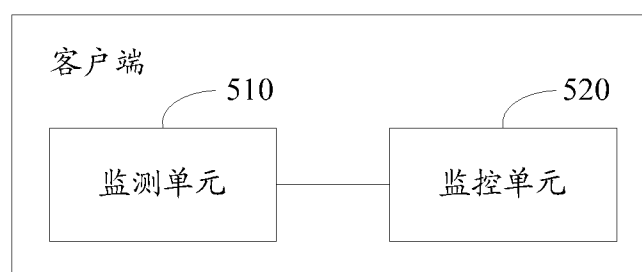


图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2012/074191

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC:H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS;CNTXT;VEN: network, security, safe, protect+, monitor+, listen+, log+, payment, trade, business, strategy, policy, rule, preset+, on w line, on w site, prevent+, avoid+, intercept+, alarm, danger+, black w list, attack, suspicious, threat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN102164138A(QIHOO SOFTWARE BEIJING CO LTD) 24 Aug. 2011(24.08.2011) claims 1-12	1-16
X	CN101409719A(LENOVO BEIJING CO LTD) 15 Apr. 2009(15.04.2009) description, page 7 line 5 to page 8 line 4, page 11 line 3 to page 14 line 9	1-16
A	CN101478407A(LENOVO BEIJING CO LTD) 08 Jul. 2009(08.07.2009) the whole document	1-16
A	US7483972B2(CISCO TECHNOLOGY INC) 27 Jan. 2009(27.01.2009) the whole document	1-16

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 02 Jul. 2012(02.07.2012)	Date of mailing of the international search report 02 Aug. 2012(02.08.2012)
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10)62019451	Authorized officer LU, Qiuyan Telephone No. (86-10)62411228

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2012/074191

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN102164138A	24.08.2011	NONE	
CN101409719A	15.04.2009	US2009094150A1	09.04.2009
		JP2009093660A	30.04.2009
		GB2453652B	14.07.2010
		JP4949348B2	06.06.2012
		GB2453652A	15.04.2009
CN101478407A	08.07.2009	US2009177883A1	09.07.2009
		CN101478407B	25.05.2011
US7483972B2	27.01.2009	US2004133672A1	08.07.2004

国际检索报告

国际申请号
PCT/CN2012/074191

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC:H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNABS;CNTXT;VEN:网络, 安全, 防护, 保护, 监控, 监测, 监听, 登录, 支付, 交易, 策略, 预置, 预设, 预先, 网上, 线上, 在线, 提示, 阻止, 避免, 拦截, 危险, 恶意, 黑名单, 威胁, 可疑, network, security, safe, protect+, monitor+, listen+, log+, payment, trade, business, strategy, policy, rule, preset+, on w line, on w site, prevent+, avoid+, intercept+, alarm, danger+, black w list, attack, suspicious, threat+

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN102164138A (奇智软件(北京)有限公司) 24.8 月 2011(24.08.2011) 权利要求 1-12	1-16
X	CN101409719A (联想(北京)有限公司) 15.4 月 2009(15.04.2009) 说明书 第 7 页第 5 行至第 8 页第 4 行, 第 11 页第 3 行至第 14 页第 9 行	1-16
A	CN101478407A (联想(北京)有限公司) 08.7 月 2009(08.07.2009) 全文	1-16
A	US7483972B2 (CISCO TECHNOLOGY INC) 27.1 月 2009(27.01.2009) 全文	1-16

☐ 其余文件在 C 栏的续页中列出。

☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期
02.7 月 2012(02.07.2012)

国际检索报告邮寄日期
02.8 月 2012 (02.08.2012)

ISA/CN 的名称和邮寄地址:
中华人民共和国国家知识产权局
中国北京市海淀区蓟门桥西土城路 6 号 100088
传真号: (86-10)62019451

受权官员

鲁秋艳

电话号码: (86-10) **62411228**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2012/074191

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN102164138A	24.08.2011	无	
CN101409719A	15.04.2009	US2009094150A1	09.04.2009
		JP2009093660A	30.04.2009
		GB2453652B	14.07.2010
		JP4949348B2	06.06.2012
		GB2453652A	15.04.2009
CN101478407A	08.07.2009	US2009177883A1	09.07.2009
		CN101478407B	25.05.2011
US7483972B2	27.01.2009	US2004133672A1	08.07.2004