

(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
2016年2月4日 (04.02.2016)



(10) 国际公布号
WO 2016/015680 A1

- (51) 国际专利分类号:
G06F 21/56 (2013.01)
- (21) 国际申请号: PCT/CN2015/085802
- (22) 国际申请日: 2015年7月31日 (31.07.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410377593.3 2014年8月1日 (01.08.2014) CN
- (71) 申请人: 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)。奇智软件(北京)有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED) [CN/CN]; 中国北京市朝阳区酒仙桥路6号院2号楼B座2层、3层301-306室, Beijing 100015 (CN)。
- (72) 发明人: 孟齐源 (MENG, Qiyuan); 中国北京市朝阳区酒仙桥路6号院2号楼, Beijing 100015 (CN)。高伟玮 (GAO, Yiwei); 中国北京市朝阳区酒仙桥路6号院2号楼, Beijing 100015 (CN)。

- (74) 代理人: 北京智汇东方知识产权代理事务所(普通合伙) (WISEAST INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区花园路13号5幢320房间, Beijing 100088 (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, BN, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, 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, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: SECURITY DETECTION METHOD AND SECURITY DETECTION APPARATUS FOR MOBILE TERMINAL INPUT WINDOW

(54) 发明名称: 移动终端输入窗口的安全检测方法和安全检测装置

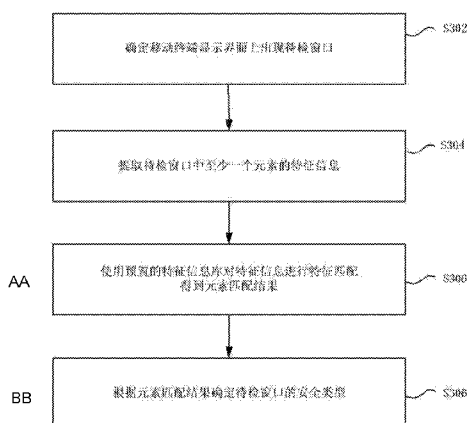


图3 / Fig. 3

S302 Determining that a window to be detected appears on a mobile terminal display interface
S304 Extracting feature information about at least one element in the window to be detected
AA Using a pre-set feature information base to perform feature matching on the feature information, so as to obtain an element matching result
BB Determining the security type of the window to be detected according to the element matching result

(57) Abstract: A security detection method and security detection apparatus for a mobile terminal input window. The security detection method based on a mobile terminal interface window comprises: determining that a window to be detected appears on a mobile terminal display interface (S302); extracting feature information about at least one element in the window to be detected (S304); using a pre-set feature information base to perform feature matching on the feature information, so as to obtain an element matching result (S306); and determining the security type of the window to be detected according to the element matching result, wherein the feature information base pre-stores element feature information about a window of a payment-type software type and/or element feature information about a window of a malicious sample. The method and apparatus can perform matching of window element features using a window to be detected on a display interface, so as to prevent the case where a malicious program intercepts user information by means of window camouflage, which improves the security of user information.

(57) 摘要:

[见续页]

WO 2016/015680 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种移动终端输入窗口的安全检测方法和安全检测装置。其中基于移动终端界面窗口的安全检测方法包括：确定移动终端显示界面上出现待检窗口（S302）；提取待检窗口中至少一个元素的特征信息（S304）；使用预置的特征信息库对特征信息进行特征匹配，得到元素匹配结果（S306）；根据元素匹配结果确定待检窗口的安全类型，其中特征信息库预先保存有支付类软件类窗口的元素特征信息和/或恶意样本的窗口的元素特征信息。该方法和装置能够利用显示界面上出现的待检窗口进行窗口元素特征的匹配，防止出现恶意程序通过窗口伪装方法截取用户信息情况，提高了用户信息安全。

移动终端输入窗口的安全检测方法和安全检测装置

技术领域

本发明涉及互联网安全领域，特别是涉及一种移动终端输入窗口的安全检测方法5 和安全检测装置。

背景技术

随着网络技术和电子商务的发展，在移动终端上进行网购和电子支付越来越普及，然而移动终端的信息安全成为了影响移动终端网购和电子支付发展的重要阻碍。

10 移动终端的信息安全涉及用户信息的保密、用户资金和支付信息的安全等问题，目前存在一些恶意应用程序，通过盗取终端数据或伪装成正规网购客户端或支付客户端的页面骗取用户信息的方式，骗取用户的银行或支付账号信息进行金融诈骗，导致用户遭受损失。

针对以上问题，现有技术中出现了多种针对移动应用程序的扫描方法，常用的15 方法是使用移动应用程序的静态或者动态特征，与预置的特征库进行匹配，判别进行检测的移动应用程序属于黑名单或者白名单，其中白名单是指已经经过验证的正常应用程序列表，而黑名单是指已经确认为恶意应用程序的列表。然而由于当前移动应用程序的变化速度很快，现有预置特征库的更新速度不能满足新出现的应用程序的检测要求，从而导致出现一些无法判别类型的移动应用，从而不能达到实时有20 效保护移动终端的信息安全的目的。

发明内容

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移动终端输入窗口的安全检测装置和相应的移动终端输入窗口的安全检25 测方法。本发明一个进一步的目的是要使得通过显示窗口确定是否存在窃取用户信息的安全隐患，保证用户信息安全。

本发明另一个进一步的目的是要充分利用显示窗口的各种元素进行判断，确保检测的准确性。

依据本发明的一个方面，提供了一种基于移动终端界面窗口的安全检测方法。30 该基于移动终端界面窗口的安全检测方法包括：确定移动终端显示界面上出现待检窗口；提取待检窗口中至少一个元素的特征信息；使用预置的特征信息库对特征信息进行特征匹配，得到元素匹配结果；根据元素匹配结果确定待检窗口的安全类型，其中特征信息库预先保存有支付类软件类窗口的元素特征信息和/或恶意样本的窗口的元素特征信息。

35 根据本发明的另一方面，提供了移动终端输入窗口的安全检测装置。该安全检测装置包括界面监测模块，适于确定移动终端显示界面上生成出现待检窗口；特征信息提取模块，适于提取待检窗口中至少一个元素的特征信息；特征匹配模块，适

于使用预置的特征信息库中对特征信息进行特征匹配，得到元素的匹配结果，并根据元素匹配结果确定待检窗口的安全类型，其中特征信息库预先保存有支付类软件类窗口的元素的特征信息和/或恶意样本的窗口的元素特征信息。

- 根据本发明的又一个方面，提供了一种计算机程序，其包括计算机可读代码，
- 5 当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行上述基于移动终端界面窗口的安全检测方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了上述的计算机程序。

- 本发明的移动终端输入窗口的安全检测方法利用显示界面上出现的待检窗口进行窗口元素特征的匹配，以判别待检窗口是否伪装成安全应用程序的显示窗口，从而防止出现恶意程序通过窗口伪装方法截取用户信息情况，提高了用户信息安全。
- 10

进一步地，本发明的移动终端输入窗口的安全检测方法，可以采用白样本特征匹配和黑样本特征匹配的方式进行检测，既可以确定待检窗口为安全窗口，也可以确定待检窗口为恶意窗口，提高了安全检测的准确性。

- 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。
- 15

附图说明

- 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：
- 20

图 1 是根据本发明一个实施例的移动终端输入窗口的安全检测装置的示意框图；

25

图 2 是根据本发明一个实施例的移动终端输入窗口的安全检测装置的应用环境图；

图 3 是根据本发明一个实施例的基于移动终端界面窗口的安全检测方法的示意图；

- 图 4 是根据本发明一个实施例的基于移动终端界面窗口的安全检测方法的一种可选流程图；
- 30

图 5 是根据本发明一个实施例的基于移动终端界面窗口的安全检测方法的中一个待检窗口的示意图；

- 图 6 示意性地示出了用于执行根据本发明的基于移动终端界面窗口的安全检测方法的计算设备的框图；以及
- 35

图 7 示意性地示出了用于保持或者携带实现根据本发明的基于移动终端界面窗口的安全检测方法的程序代码的存储单元。

具体实施方式

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，
5 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。

图 1 是根据本发明一个实施例的移动终端输入窗口的安全检测装置 100 的示意框图。该移动终端输入窗口的安全检测装置 100 一般性地可包括：界面监测模块 110、特征信息提取模块 120、特征匹配模块 130，这些部件可以根据移动终端输入窗口的
10 安全检测装置 100 的功能和使用环境进行灵活配置，在一些优选的实施例中可以通过增加部件，实现更多的功能已达到不同的技术效果，例如，还可以增加设置进程扫描模块 140 和安全提示模块 150，另外，特征匹配模块 130 的一种可选结构为包括白样本匹配子模块 132、黑样本匹配子模块 134、信息上传子模块 136。

在本实施例的移动终端输入窗口的安全检测装置 100 中，界面监测模块 110 可
15 以适于确定移动终端显示界面上生成出现待检窗口，其一种可选的流程为检测移动终端中的进程变化；确定进程在移动终端显示界面上生成新窗口。检测移动终端中的进程可以利用主防技术，注入系统进程内部，获取进程生成窗口的情况。优选地，界面监测模块 110 可以将带有输入框的窗口作为待检窗口。

特征信息提取模块 120 提取待检窗口中至少一个元素的特征信息，一般显示窗
20 口的元素待检窗口的元素包括以下至少一项：输入框、标题栏、标签、菜单、操作按钮，对应地，特征信息提取模块 120 提取的特征信息可以包括以上元素的文本内容、位置信息、链接地址、元素类型中的一项或多项。

特征匹配模块 130 可以使用预置的特征信息库中对特征信息进行特征匹配，得到元素的匹配结果，并根据元素匹配结果确定待检窗口的安全类型。以上特征信息
25 库预先保存有支付类软件类窗口的元素的特征信息和/或恶意样本的窗口的元素特征信息，例如特征信息库预先保存的支付类软件窗口的元素特征信息包括：支付类软件的登录窗口的元素特征信息、支付类软件的账号绑定窗口的元素特征信息、支付类软件的支付窗口的元素特征信息，以将支付类软件类窗口的元素的特征信息作为白样本的匹配依据。恶意样本的窗口的元素特征信息可以提取上报的恶意样本的
30 窗口的元素的特征作为黑样本的匹配依据。

具体地，白样本匹配子模块 132 可以提取待检窗口中元素的文本内容包含的支付关键词，根据支付关键词确定出对应的支付类软件；将待检窗口的元素的特征信息
35 与特征信息库中对应的支付类软件的窗口元素特征信息进行比对，若比对结果为一一致，确定待检窗口为安全窗口。对于安全窗口，本实施例的移动终端输入窗口的安全检测装置 100 可以不做任何干预，以由用户进行正常操作。

黑样本匹配子模块 134 可以将待检窗口的特征信息与特征信息库中恶意样本的窗口的元素特征信息进行匹配，若出现匹配，确定待检窗口为恶意窗口。对于恶意窗口，如果用户在其中输入账号信息等内容有可能被截取，导致信息泄露，因此需

要向用户报告，并采取必要的措施。例如通过安全提示模块 150 在移动终端显示界面上输出与安全类型对应的提示信息。进一步地，还可以采取其他方式进行安全防范，例如将恶意窗口的输入框设置为不可输入，以避免用户在不知情的情况下进行输入，仅在用户忽略提示信息的情况下，回复输入框的输入功能。

5 以上信息匹配过程可以在终端侧进行，也可以利用云端技术在云端进行匹配，例如利用信息上传子模块 136 将特征信息上传至安全分析服务器，利用预置于安全分析服务器中的预置的特征信息库进行以上信息匹配的过程。一种具体的配置方式为，在终端侧和网络侧分别预置数据库以用于窗口元素的特征匹配，以适用于不同的使用环境。

10 进程扫描模块 140 可以对生成窗口的进程进行安全扫描，以确定进程的样本类型；特征信息提取模块 130 在进程扫描模块的扫描结果为在进程不属于已知安全进程或已知危险进程中的任一种时，才执行提取窗口中至少一个元素的特征信息的步骤。也就是说，首先使用进程检测的方式进行筛选，仅在进程检测不能确定安全性时，执行在进行窗口元素的特征匹配的步骤。

15 图 2 是根据本发明一个实施例的移动终端输入窗口的安全检测装置 100 的应用环境图，本实施例的移动终端输入窗口的安全检测装置 100 可以设置于各类移动终端 10 中，例如智能手机、平板电脑、掌上电脑等中。这些移动终端 10 可以运行于安卓等操作系统中，本实施例的移动终端输入窗口的安全检测装置 100 利用对以上操作系统的进程主防确定移动终端显示界面上出现待检窗口，并使用预置于移动终端中保存有窗口元素特征的特征信息库进行特征匹配。以上特征信息库由安全分析服务器 30 通过移动网络 20 进行下发，另外，移动终端输入窗口的安全检测装置 100 还可以将提取出的待检窗口的元素的特征信息通过移动网络 20 上传，由安全分析服务器 30 预置于移动终端中保存有窗口元素特征的特征信息库进行特征匹配，并将匹配结果下发给移动终端 10，并对恶意窗口进行提示。

25 本发明实施例还提供了一种基于移动终端界面窗口的安全检测方法，该基于移动终端界面窗口的安全检测方法可以由以上实施例介绍的任意一种基于移动终端界面窗口的安全检测装置来执行，以提高移动终端的信息安全性。图 3 是根据本发明一个实施例的基于移动终端界面窗口的安全检测方法的示意图，如图所示，该基于移动终端界面窗口的安全检测方法包括以下步骤：

30 步骤 S302，确定移动终端显示界面上出现待检窗口；
步骤 S304，提取待检窗口中至少一个元素的特征信息；
步骤 S306，使用预置的特征信息库对特征信息进行特征匹配，得到元素匹配结果；
步骤 S308，根据元素匹配结果确定待检窗口的安全类型。

35 在以上步骤中，步骤 S302 可以通过检测移动终端中进程变化确定出现待检窗口，具体可以检测移动终端中进程变化以确定进程在移动终端显示界面上生成新窗口。检测移动终端中进程可以利用主防技术，注入系统进程内部，获取进程生成窗口的情况。由于本实施例所要解决的一个技术问题为防止用户输入的账户信息或支

付信息被截取，因此以上待检窗口可以具体是带有输入框的窗口，特别是该输入框的类型为密码框的情况下。又例如新出现的窗口的标题栏中的文字包括有以下关键词：“快捷支付”、“支付宝支付”、“微信支付”、“移动支付”、“手机银行”等，则需要将该窗口作为待检窗口。

- 5 一般显示窗口的元素待检窗口的元素包括以下至少一项：输入框、标题栏、标签、菜单、操作按钮，步骤 S304 提取的特征信息可以包括以上元素的文本内容、位置信息、链接地址、元素类型中的一项或多项。

步骤 S306 使用的特征信息库预先保存有支付类软件类窗口的元素特征信息和/或恶意样本的窗口的元素特征信息，也就是既可以识别安全窗口也可以识别危险窗口，对待检窗口采取非黑即白的检测测量。

相应地，步骤 S306 可以包括对特征信息进行白样本特征匹配和黑样本特征匹配两种匹配方式中的任一种或全部两种。

例如，特征信息库预先保存的支付类软件窗口的元素特征信息包括以下内容：支付类软件的登录窗口的元素特征信息、支付类软件的账号绑定窗口的元素特征信息、支付类软件的支付窗口的元素特征信息。步骤 S306 进行白样本特征匹配的流程可以为：提取待检窗口中元素的文本内容包含的支付关键词，根据支付关键词确定出对应的支付类软件；将待检窗口的元素的特征信息与特征信息库中对应的支付类软件的窗口元素特征信息进行比对，若比对结果为一一致，确定待检窗口为安全窗口。一个具体的实例为窗口的标题栏中文字为“微信支付”，将该窗口的元素特征与微信客户端中支付界面的元素特征进行匹配，若匹配成功，就可以确认该待检窗口为微信支付窗口，否则就可以认为该待检窗口为恶意窗口或者需要进行进一步检测。

步骤 S306 对特征信息进行黑样本特征匹配的一种流程为包括：将待检窗口的特征信息与特征信息库中恶意样本的窗口的元素特征信息进行匹配，若出现匹配，确定待检窗口为恶意窗口。对于恶意窗口，在步骤 S308 之后还可以在移动终端显示界面上输出与安全类型对应的提示信息，以提醒用户。另外，在出现恶意窗口的情况下，还可以对恶意窗口进行处理，例如屏蔽窗口，将输入框置灰处于不可输入状态等，防止用户进行操作，如果用户的提醒信息进行忽略操作，则恢复窗口。

除了利用移动终端上预置的特征信息库进行黑白样本特征匹配之外，本实施例的移动终端输入窗口的安全检测方法还可以将特征信息上传至安全分析服务器，并接收安全分析服务器下发的特征匹配结果，从而利用网络侧的大数据进行匹配，得到的结果更加准确。

在步骤 304 之前，还可以利用移动端的病毒查杀系统对进程的样本进行检测，例如对生成窗口的进程进行安全扫描，以确定进程的样本类型；在进程不属于已知安全进程或已知危险进程中的任一种时，然后执行步骤 S304。也就是说，首先使用进程检测的方式进行筛选，仅在进程检测不能确定安全性时，执行在进行窗口元素的特征匹配的步骤。

图 4 是根据本发明一个实施例的基于移动终端界面窗口的安全检测方法的一种可选流程图，该流程包括：

步骤 S402, 确定移动终端显示界面上生成新的待检窗口

步骤 S404, 使用移动终端的病毒主防软件判断生成窗口的进程是否为已知的安全进程, 若是允许窗口正常运行, 若否执行步骤 S406;

5 步骤 S406, 使用移动终端的病毒主防软件判断生成窗口的进程是否为已知的恶意进程, 若是向用户进行安全提示, 并执行相应安全操作 (例如结束进程、删除文件、放入隔离区等), 若否, 说明无法确定进程安全性, 需要进行后续窗口元素特征匹配;

步骤 S408, 判断新生成的窗口是否存在输入框, 若否说明该窗口仅为内容显示窗口, 可不进行检测;

10 步骤 S410, 确定窗口为待检窗口;

步骤 S412, 提取窗口元素的特征, 具体可以包括以下内容: 输入框、标题栏、标签、菜单、操作按钮等元素各自的文本内容、位置信息、链接地址、元素等。

步骤 S414, 使用白样本窗口元素的特征进行匹配, 若匹配成功, 若是允许窗口正常运行;

15 步骤 S416, 使用黑样本窗口元素的特征进行匹配, 若匹配不成功, 可以将元素特征上传至安全分析服务器进行进一步分析;

步骤 S418, 提示窗口安全风险, 并对窗口进行安全防范操作, 例如将屏蔽窗口, 将输入框置灰以处于不可输入状态等, 防止用户进行操作, 泄露个人信息。以上提示窗口中可以提示出窗口的安全隐患, 还可以向用户提供操作选项, 例如卸载相关应用、上传安全检测结果、忽略提示等, 以使用户自行判断并进行相应操作。

20 执行本发明以上实施例的基于移动终端界面窗口的安全检测方法, 判断客户端的界面的类似程度, 例如对话框弹出时, 可以对对话框里的元素 (提示框的类别、标题栏) 进行特征判别, 比如标题栏是否提示淘宝支付宝登陆, 界面栏有没有某种形式的提示框, 是不是密码框。又例如在提取出元素的特征串后, 可以根据界面里的输入框和文字进行识别, 建立类似于判定模型, 判定是否是支付或其他金融界面 (例如类似于淘宝、微信的登录框, 是否是微信支付宝绑定银行卡的界面)。

25 对于安卓系统终端, 例如安卓智能手机, 提取窗口的元素可以利用类似脚本的语言进行, 结合其判定规则进行判定, 形成安卓系统显示界面的弹框的判定模型, 相对于现有对判断包名签名的识别, 本实施例的基于移动终端界面窗口的安全检测方法可以弥补其更新速度不能满足要求的不足。

30 图 5 是根据本发明一个实施例的基于移动终端界面窗口的安全检测方法的中一个待检窗口的示意图, 在确定界面上出现图 5 所示的窗口后, 首先由主防引擎判断生成该窗口的客户端的安全类型 (例如对包名、权限信息特征匹配), 如果该窗口属于白样本, 则可以使该窗口正常运行, 如果该窗口属于黑样本, 则需要提醒用户安全风险, 并提供相应安全措施选项 (例如提示卸载, 对该应用的弹窗进行拦截等), 如果无法确定客户端的安全类型, 提取标题栏、标签和输入框的类型, 在图 5 中的标题栏出现 “请输入支付密码”, 而且标签中也出现金额和银行卡信息, 此时需要将以上这些元素的特征 (位置、链接地址、文本) 与特征库中的黑白窗口元素

的特征进行匹配，如果确定这些特征是已知的安全支付窗口，则允许窗口正常运行，如果确定这些特征与伪装成支付窗口的黑样本的特征匹配，则在窗口展示界面上提示风险，并在用户进行进一步操作前，将输入框设置为不可输入。从而防止用户输入的账户信息被截取导致损失。

- 5 使用本实施例的基于移动终端界面窗口的安全检测方法利用显示界面上出现的待检窗口进行窗口元素特征的匹配，防止出现恶意程序通过窗口伪装方法截取用户信息情况，提高了用户信息安全。

10 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。

15 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，本发明的各个特征信息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信息更多的特征信息。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信息。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。

20 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，以及此外可以把它分成多个子模块或子单元或子组件。除了这样的特征信息和/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）中公开的所有特征信息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。25 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）中公开的每个特征信息可以由提供相同、等同或相似目的的替代特征信息来代替。

30 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信息而不是其它特征信息，但是不同实施例的特征信息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。

35 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基于移动终端界面窗口的安全检测装置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。

例如，图 6 示出了可以实现根据本发明的基于移动终端界面窗口的安全检测方法的计算设备。该计算设备传统上包括处理器 610 和以存储器 620 形式的计算机程序产品或者计算机可读介质。存储器 620 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 620 具有用于执行上述方法
5 中的任何方法步骤的程序代码 631 的存储空间 630。例如，用于程序代码的存储空间 630 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 631。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图 7 所述的便携式或者固定存储单元。该存储
10 单元可以具有与图 6 的计算设备中的存储器 620 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 631’，即可以由例如诸如 610 之类的处理器读取的代码，这些代码当由计算设备运行时，导致该计算设备执行上面所描述的方法中的各个步骤。

本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，
15 结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

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。

至此，本领域技术人员应认识到，虽然本文已详尽示出和描述了本发明的多个示例性实施例，但是，在不脱离本发明精神和范围的情况下，仍可根据本发明公开的内容直接确定或推导出符合本发明原理的许多其他变型或修改。因此，本发明的范围应被理解和认定为覆盖了所有这些其他变型或修改。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权 利 要 求

1. 一种基于移动终端界面窗口的安全检测方法，包括：

确定移动终端显示界面上出现待检窗口；

5 提取所述待检窗口中至少一个元素的特征信息；

使用预置的特征信息库对所述特征信息进行特征匹配，得到元素匹配结果；

根据元素匹配结果确定所述待检窗口的安全类型，其中所述特征信息库预先保存有支付类软件类窗口的元素特征信息和/或恶意样本的窗口的元素特征信息。

10 2. 根据权利要求 1 所述的方法，其中，确定移动终端显示界面上出现待检窗口包括：

检测所述移动终端中的进程变化；

确定所述进程在移动终端显示界面上生成新窗口。

3. 根据权利要求 1 所述的方法，其中，使用预置的特征信息库中对所述特征信息进行特征匹配包括：

15 对所述特征信息进行白样本特征匹配和/或黑样本特征匹配。

4. 根据权利要求 3 所述的方法，其中，对所述特征信息进行白样本特征匹配包括：

提取所述待检窗口中元素的文本内容包含的支付关键词，

根据所述支付关键词确定出对应的支付类软件；

20 将所述待检窗口的元素的特征信息与所述特征信息库中所述对应的支付类软件的窗口元素特征信息进行比对，若比对结果为一致，确定所述待检窗口为安全窗口。

5. 根据权利要求 4 所述的方法，其中，所述特征信息库预先保存的所述支付类软件窗口的元素特征信息包括：所述支付类软件的登录窗口的元素特征信息、所述支付类软件的账号绑定窗口的元素特征信息、所述支付类软件的支付窗口的元素特征信息。

25 6. 根据权利要求 3 所述的方法，其中，对所述特征信息进行黑样本特征匹配包括：

将所述待检窗口的特征信息与所述特征信息库中恶意样本的窗口的元素特征信息进行匹配，若出现匹配，确定所述待检窗口为恶意窗口。

30 7. 根据权利要求 1 至 6 中任一项所述的方法，其中，

所述待检窗口的元素包括以下至少一项：输入框、标题栏、标签、菜单、操作按钮；

提取所述待检窗口中至少一个元素的特征信息包括：提取所述元素的文本内容、位置信息、链接地址、元素类型中的一项或多项。

35 8. 根据权利要求 1 至 7 中任一项所述的方法，其中，

所述预置的特征信息库预置于安全分析服务器中，

在对所述特征信息进行特征匹配之前还包括：将所述特征信息上传至所述安全分析服务器。

9. 根据权利要求 1 至 8 任一项中所述的方法，其中，在提取所述窗口中至少一个元素的特征信息之前还包括：

对生成所述窗口的进程进行安全扫描，以确定所述进程的样本类型；

5 在所述进程不属于已知安全进程或已知危险进程中的任一种时，执行提取所述窗口中至少一个元素的特征信息的步骤。

10. 根据权利要求 1 至 9 任一项中所述的方法，其中，在确定所述待检窗口的安全类型之后还包括：

在所述移动终端显示界面上输出与所述安全类型对应的提示信息。

11. 一种移动终端输入窗口的安全检测装置，包括：

10 界面监测模块，适于确定移动终端显示界面上生成出现待检窗口；

特征信息提取模块，适于提取所述待检窗口中至少一个元素的特征信息；

特征匹配模块，适于使用预置的特征信息库中对所述特征信息进行特征匹配，得到元素的匹配结果，并根据元素匹配结果确定所述待检窗口的安全类型，其中所述特征信息库预先保存有支付类软件类窗口的元素的特征信息和/或恶意样本的窗口
15 的元素特征信息。

12. 根据权利要求 11 所述的装置，其中，所述界面监测模块还适于：

检测所述移动终端中的进程变化；

确定所述进程在移动终端显示界面上生成新窗口。

13. 根据权利要求 11 所述的装置，其中，所述特征匹配模块包括：

20 白样本匹配子模块，适于：提取所述待检窗口中元素的文本内容包含的支付关键词，根据所述支付关键词确定出对应的支付类软件；将所述待检窗口的元素的特征信息与所述特征信息库中所述对应的支付类软件的窗口元素特征信息进行比较，若比对结果为一一致，确定所述待检窗口为安全窗口，和/或

黑样本匹配子模块，适于：将所述待检窗口的特征信息与所述特征信息库中恶意样本的窗口的元素特征信息进行匹配，若出现匹配，确定所述待检窗口为恶意窗口。
25

14. 根据权利要求 13 所述的装置，其中，所述特征信息库预先保存的所述支付类软件窗口的元素特征信息包括：所述支付类软件的登录窗口的元素特征信息、所述支付类软件的账号绑定窗口的元素特征信息、所述支付类软件的支付窗口的元素
30 特征信息。

15. 根据权利要求 11 至 14 中任一项所述的装置，其中，

所述待检窗口的元素包括以下至少一项：输入框、标题栏、标签、菜单、操作按钮；

35 提取所述待检窗口中至少一个元素的特征信息包括：提取所述元素的文本内容、位置信息、链接地址、元素类型中的一项或多项。

16. 根据权利要求 11 至 15 中任一项所述的装置，其中，所述特征匹配模块包括：

信息上传子模块，适于将所述特征信息上传至安全分析服务器，所述预置的特

征信息库预置于所述安全分析服务器中。

17. 根据权利要求 11 至 16 任一项中所述的装置，其中，还包括：

进程扫描模块，适于对生成所述窗口的进程进行安全扫描，以确定所述进程的样本类型；

5 所述特征信息提取模块还适于：在所述进程扫描模块的扫描结果为在所述进程不属于已知安全进程或已知危险进程中的任一种时，执行提取所述窗口中至少一个元素的特征信息的步骤。

18. 根据权利要求 11 至 17 任一项中所述的装置，其中，还包括：

10 安全提示模块，适于在所述移动终端显示界面上输出与所述安全类型对应的提示信息。

19、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据权利要求 1-10 中的任一个所述的基于移动终端界面窗口的安全检测方法。

20、一种计算机可读介质，其中存储了如权利要求 19 所述的计算机程序。

15

1/5

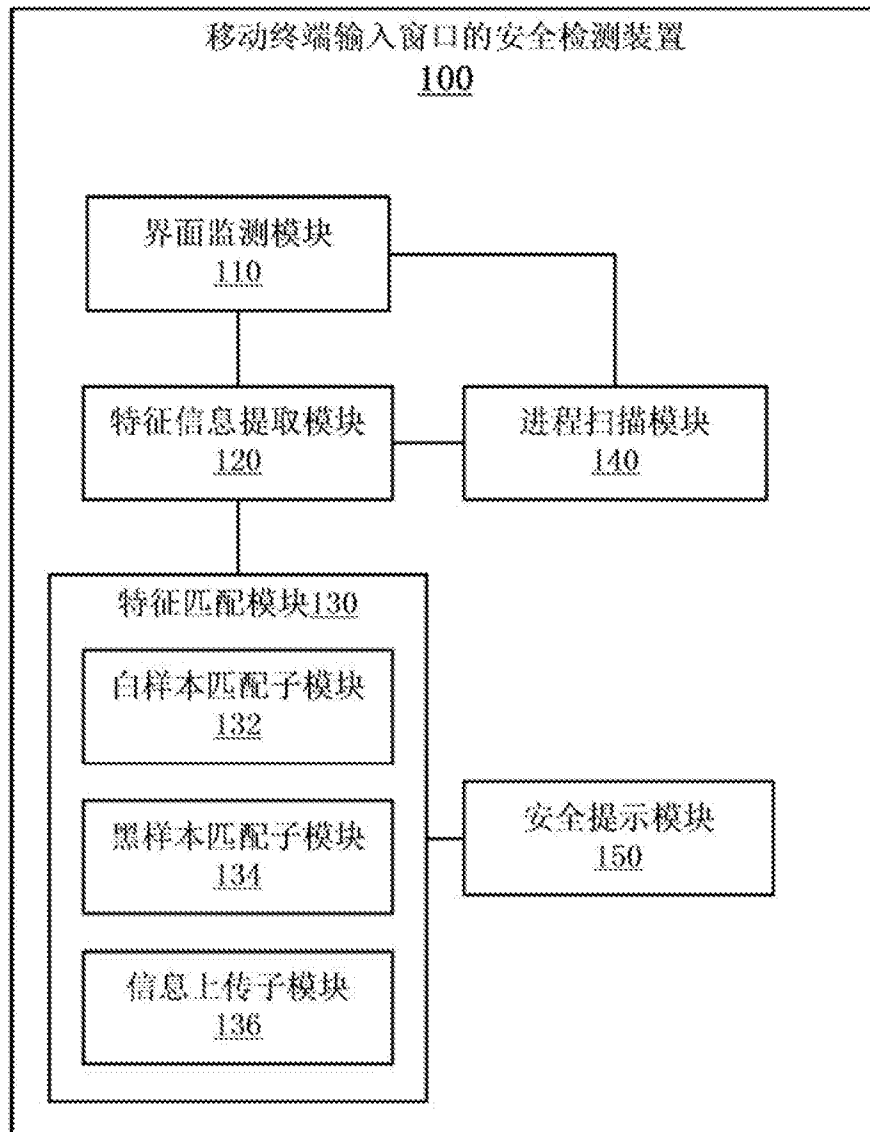


图 1

2/5

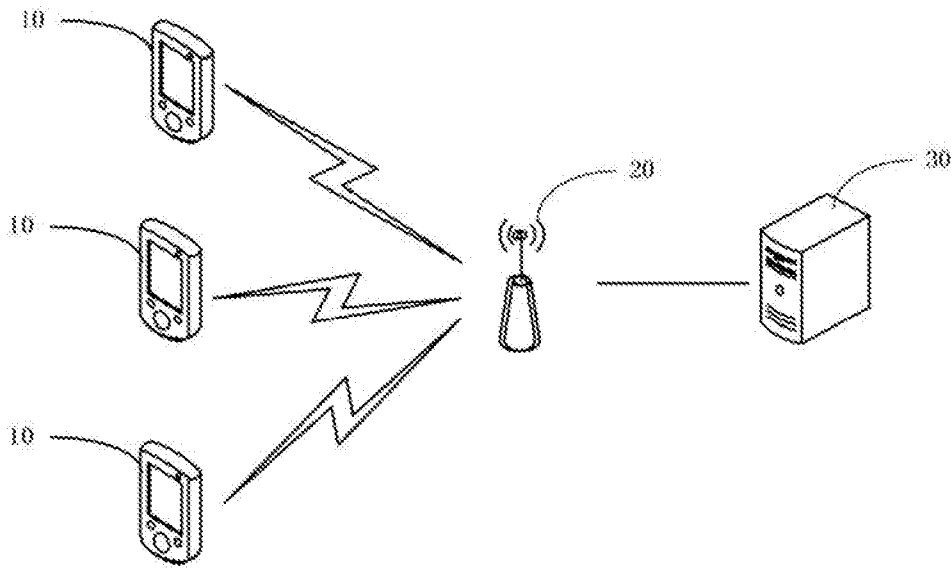


图 2

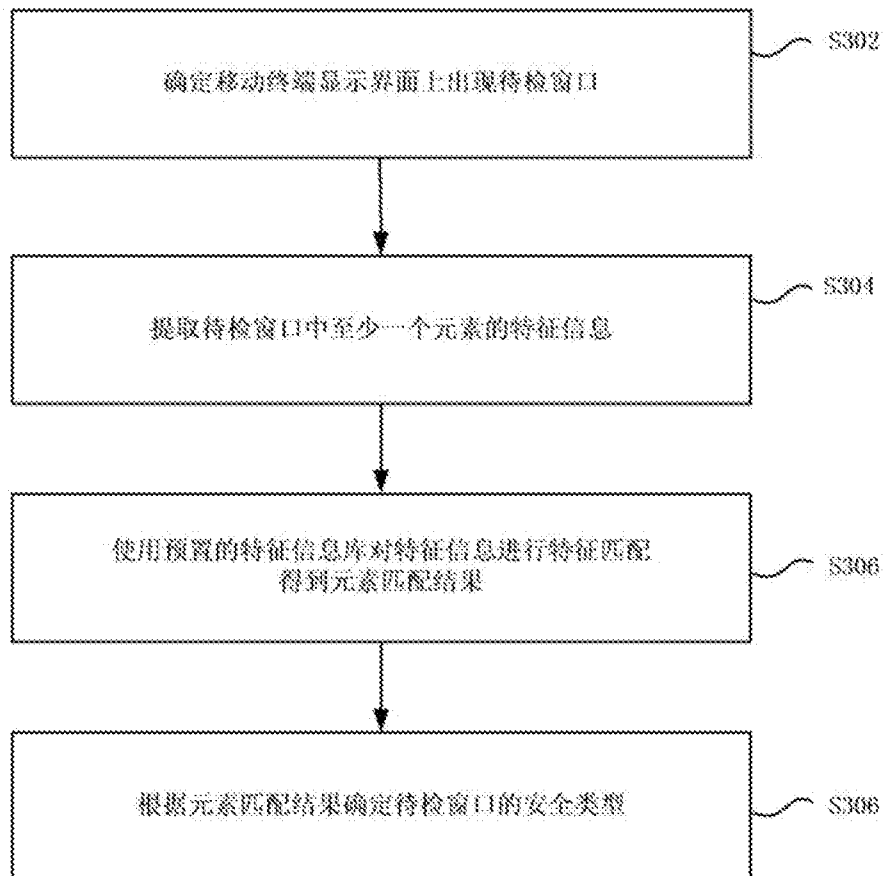


图 3

3/5

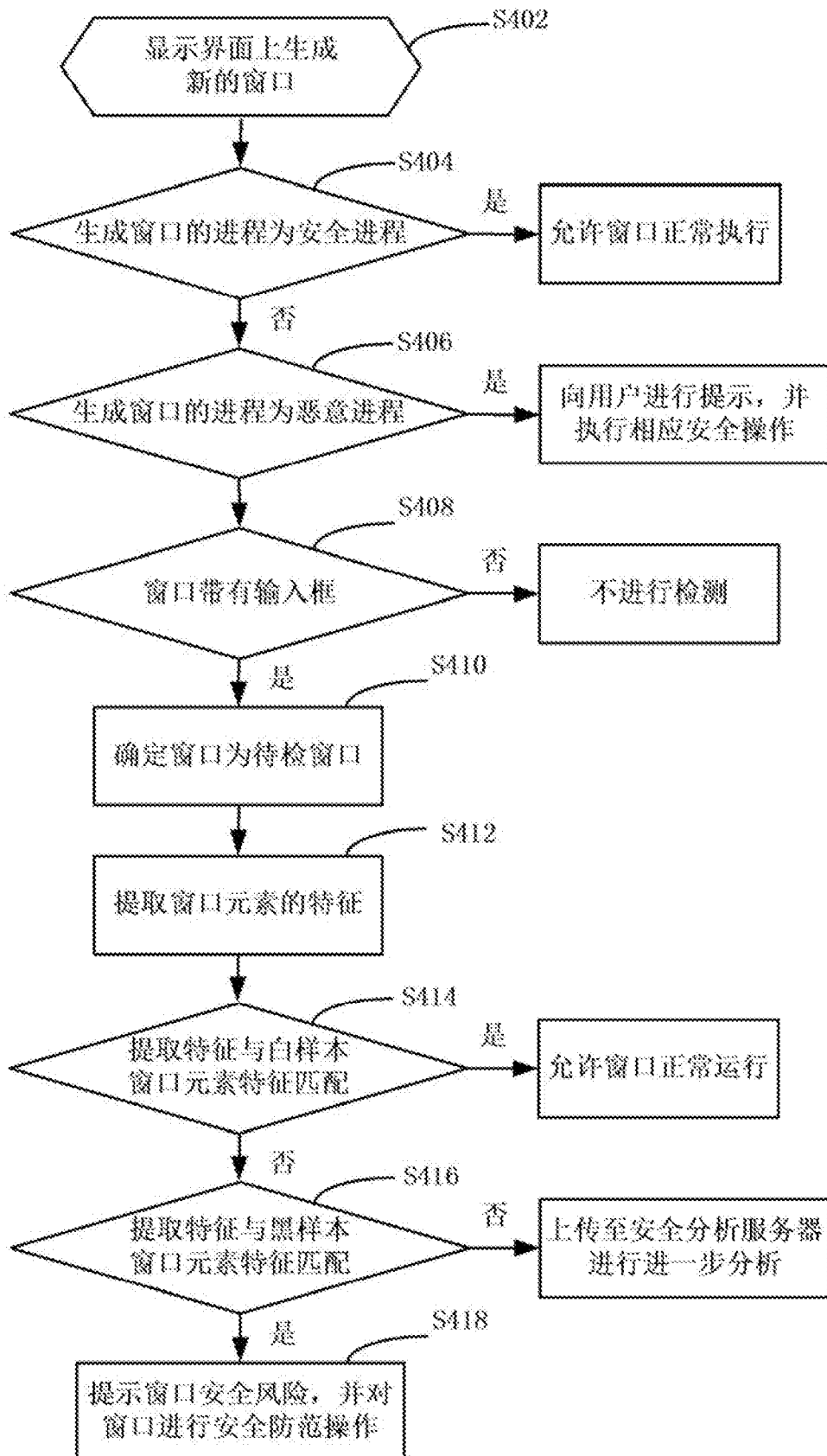


图 4



图 5

5/5

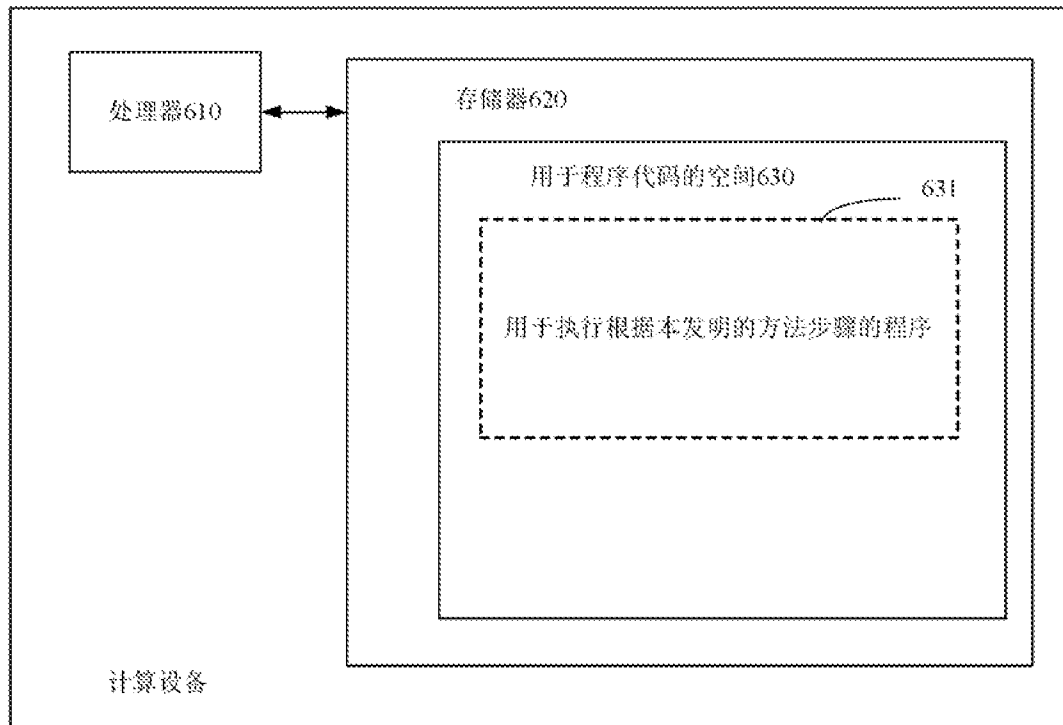


图 6

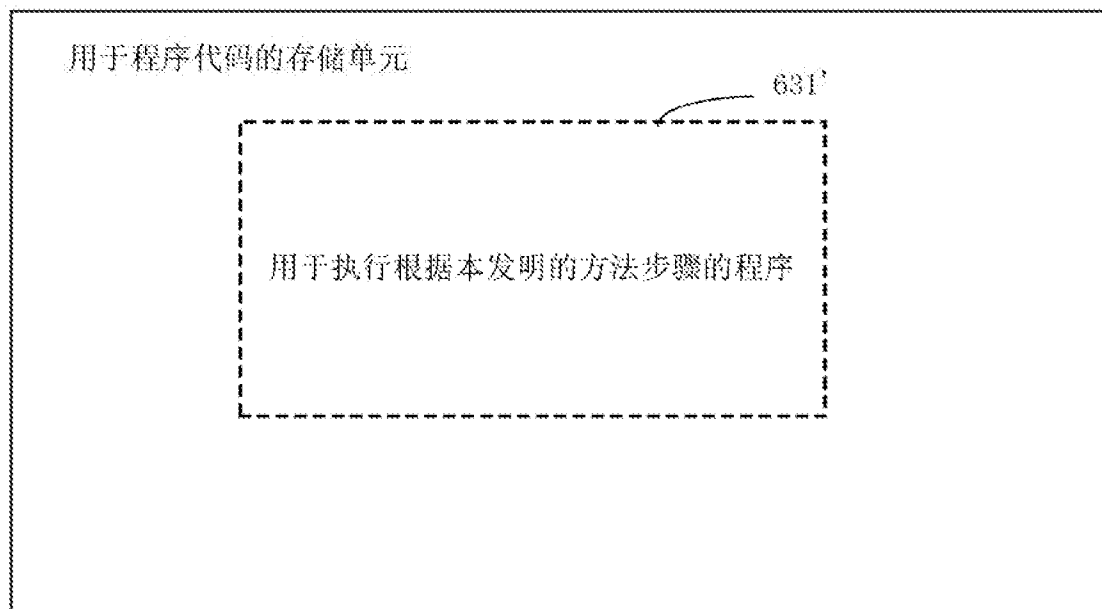


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/085802

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/56 (2013.01) 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)

G06F

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)

EPODOC, WPI, CNPAT, CNKI, IEEE, GOOGLE: phishing website, characteristic information, safe+, login, terminal, element, match+, page, window?, detect+, phishing, sites, characteristic, information

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 103795703 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 14 May 2014 (14.05.2014), description, paragraphs 66-83, and figures 1-3	1-20
Y	CN 102737183 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 17 October 2012 (17.10.2012), description, paragraph 09, and figure 1	1-20
PX	CN 104182687 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 03 December 2014 (03.12.2014), claims 1-10, description, paragraphs 75-78, and figures 1-3	1-20
PX	CN 104021339 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 03 September 2014 (03.09.2014), description, paragraphs 34-45, and claims 1-10	1-20
PX	CN 104021467 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 03 September 2014 (03.09.2014), description, paragraphs 47-66	1-20
PX	CN 104134143 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 05 November 2014 (05.11.2014), description, paragraphs 102-112	1-20
A	CN 102592067 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 18 July 2012 (18.07.2012), the whole document	1-20

☒ 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 28 September 2015 (28.09.2015)	Date of mailing of the international search report 16 October 2015 (16.10.2015)
Name and mailing address of the ISA/CN: 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 WU, Qing Telephone No.: (86-10) 61648111

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/085802**C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103825866 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 28 May 2014 (28.05.2014), the whole document	1-20
A	CN 102622553 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 01 August 2012 (01.08.2012), the whole document	1-20
A	CN 103390128 A (BEIKE INTERNET SECURITY TECHNOLOGY CO., LTD. et al.), 13 November 2013 (13.11.2013), the whole document	1-20
A	US 8468597 B1 (UAB RESEARCH FOUNDATION), 18 June 2013 (18.06.2013), the whole document	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/CN2015/085802

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103795703 A	14 May 2014	None	
CN 102737183 A	17 October 2012	None	
CN 104182687 A	03 December 2014	None	
CN 104021339 A	03 September 2014	None	
CN 104021467 A	03 September 2014	None	
CN 104134143 A	05 November 2014	None	
CN 102592067 A	18 July 2012	None	
CN 103825866 A	28 May 2014	None	
CN 102622553 A	01 August 2012	None	
CN 103390128 A	13 November 2013	None	
US 8468597 B1	18 June 2013	US 8381292 B1	19 February 2013
		US 8495735 B1	23 July 2013

国际检索报告

国际申请号

PCT/CN2015/085802

A. 主题的分类

G06F 21/56(2013.01)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)

G06F

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))

EPDOC, WPI, CNPAT, CNKI, IEEE, GOOGLE: 安全, 登陆, 终端, 元素, 特征, 匹配, 页面, 窗口, 检测, 钓鱼网站, 特征信息, safe+, login, terminal, element, match+, page, window?, detect+, phishing, sites, characteristic, information

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
Y	CN 103795703 A (北京奇虎科技有限公司 等) 2014年 5月 14日 (2014 - 05 - 14) 说明书第66-83段, 附图1-3	1-20
Y	CN 102737183 A (腾讯科技深圳有限公司) 2012年 10月 17日 (2012 - 10 - 17) 说明书第09段, 附图1	1-20
PX	CN 104182687 A (北京奇虎科技有限公司 等) 2014年 12月 3日 (2014 - 12 - 03) 权利要求1-10、说明书75-78段、附图1-3	1-20
PX	CN 104021339 A (北京奇虎科技有限公司 等) 2014年 9月 3日 (2014 - 09 - 03) 说明书第34-45段、权利要求1-10	1-20
PX	CN 104021467 A (北京奇虎科技有限公司 等) 2014年 9月 3日 (2014 - 09 - 03) 说明书第47-66段	1-20
PX	CN 104134143 A (北京奇虎科技有限公司 等) 2014年 11月 5日 (2014 - 11 - 05) 说明书第102-112段	1-20
A	CN 102592067 A (腾讯科技深圳有限公司) 2012年 7月 18日 (2012 - 07 - 18) 全文	1-20

☒ 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

2015年 9月 28日

国际检索报告邮寄日期

2015年 10月 16日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
北京市海淀区蓟门桥西土城路6号
100088 中国

传真号 (86-10)62019451

受权官员

吴卿

电话号码 (86-10)61648111

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
A	CN 103825866 A (腾讯科技深圳有限公司) 2014年 5月 28日 (2014 - 05 - 28) 全文	1-20
A	CN 102622553 A (腾讯科技深圳有限公司) 2012年 8月 1日 (2012 - 08 - 01) 全文	1-20
A	CN 103390128 A (贝壳网际北京安全技术有限公司 等) 2013年 11月 13日 (2013 - 11 - 13) 全文	1-20
A	US 8468597 B1 (UAB RESEARCH FOUNDATION) 2013年 6月 18日 (2013 - 06 - 18) 全文	1-20

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/085802

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	103795703	A	2014年 5月 14日	无	
CN	102737183	A	2012年 10月 17日	无	
CN	104182687	A	2014年 12月 3日	无	
CN	104021339	A	2014年 9月 3日	无	
CN	104021467	A	2014年 9月 3日	无	
CN	104134143	A	2014年 11月 5日	无	
CN	102592067	A	2012年 7月 18日	无	
CN	103825866	A	2014年 5月 28日	无	
CN	102622553	A	2012年 8月 1日	无	
CN	103390128	A	2013年 11月 13日	无	
US	8468597	B1	2013年 6月 18日	US 8381292 B1	2013年 2月 19日
				US 8495735 B1	2013年 7月 23日

表 PCT/ISA/210 (同族专利附件) (2009年7月)