(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 106027520 B
(45)授权公告日 2019.02.26

(21)申请号 201610335249.7

(22)申请日 2016.05.19

(65)同一申请的已公布的文献号
申请公布号 CN 106027520 A

(43)申请公布日 2016.10.12

(73)专利权人 微梦创科网络科技(中国)有限公司
地址 100080 北京市海淀区彩和坊路6号7-10层

(72)发明人 崔培豪 罗诗尧

(74)专利代理机构 北京卓岚智财知识产权代理事务所(特殊普通合伙) 11624
代理人 任漱晨

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 104426885 A,2015.03.18,
CN 104519032 A,2015.04.15,
CN 105357169 A,2016.02.24,
CN 102664877 A,2012.09.12,
CN 101192926 A,2008.06.04,
CN 105656867 A,2016.06.08,
CN 104967594 A,2015.10.07,
US 2004199770 A1,2004.10.07,
US 2016080398 A1,2016.03.17,

审查员 张洁

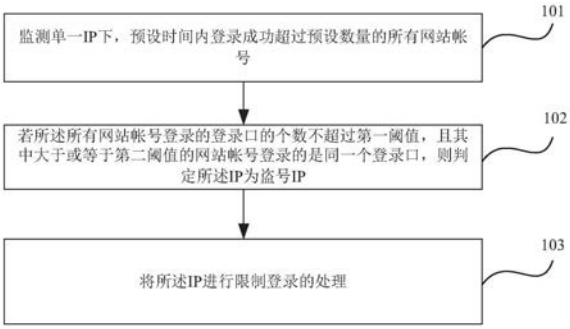
权利要求书2页 说明书6页 附图2页

(54)发明名称

一种检测处理盗取网站帐号的方法及装置

(57)摘要

本发明实施例提供一种检测处理盗取网站帐号的方法及装置,所述方法包括:监测单一IP下,预设时间内登录成功超过预设数量的所有网站帐号;若所述所有网站帐号登录的登录口的个数不超过第一阈值,且其中大于或等于第二阈值的网站帐号登录的是同一个登录口,则判定所述IP为盗号IP;将所述IP进行限制登录的处理。上述技术方案具有如下有益效果:提高了网站用户的网站帐号登录的安全性,本发明可以一定程度上检测盗号行为的发生,并在处理机制上,针对不同用户不同行为分别进行处理,在提高安全性的同时,也保证了用户体验。



1.一种检测处理盗取网站帐号的方法,其特征在于,所述方法包括:

监测单一IP下,预设时间内登录成功超过预设数量的所有网站帐号;

若所述所有网站帐号登录的登录口的个数不超过第一阈值,且其中登录同一个登录口的网站帐号与所述所有网站账号的数量比值大于或等于第二阈值,则判定所述IP为盗号IP;所述第二阈值小于1;

将所述IP进行限制登录的处理。

2.如权利要求1所述检测处理盗取网站帐号的方法,其特征在于,所述预设时间为1分钟,所述预设数量为10个。

3.如权利要求1所述检测处理盗取网站帐号的方法,其特征在于,所述第一阈值为3;所述第二阈值为90%。

4.如权利要求1所述检测处理盗取网站帐号的方法,其特征在于,所述将所述IP进行限制登录的处理,包括:

对所述IP进行封禁设定时间处理并私信通知用户修改密码,同时对所述IP下已登录成功的网站帐号,设置用于指示所述网站账号被盗的标记,并根据网站账号的用户属性和操作类型分别进行相应处理。

5.如权利要求4所述检测处理盗取网站帐号的方法,其特征在于,所述根据网站账号的用户属性和操作类型,分别进行相应处理,具体包括:如果所述网站账号的用户属性为浏览属性用户,当其操作类型为浏览操作时,相应处理为允许浏览操作,当其操作类型为敏感行为操作时,相应处理为密码之外额外验证身份后允许敏感行为操作;所述敏感行为操作包括如下行为操作:更改资料、支付、发布消息、发邮件,所述密码之外额外验证身份的方式包括:手机短信验证码验证。

6.一种检测处理盗取网站帐号的装置,其特征在于,所述装置包括:

监测单元,用于监测单一IP下,预设时间内登录成功超过预设数量的所有网站帐号;

判断单元,用于若所述所有网站帐号登录的登录口的个数不超过第一阈值,且其中登录同一个登录口的网站帐号与所述所有网站账号的数量比值大于或等于第二阈值,则判定所述IP为盗号IP;所述第二阈值小于1;处理单元,用于将所述IP进行限制登录的处理。

7.如权利要求6所述检测处理盗取网站帐号的装置,其特征在于,所述预设时间为1分钟,所述预设数量为10个。

8.如权利要求6所述检测处理盗取网站帐号的装置,其特征在于,所述第一阈值为3;所述第二阈值为90%。

9.如权利要求6所述检测处理盗取网站帐号的装置,其特征在于,

所述处理单元,具体用于对所述IP进行封禁设定时间处理并私信通知用户修改密码,同时对所述IP下已登录成功的网站帐号,设置用于指示所述网站账号被盗的标记,并根据网站账号的用户属性和操作类型分别进行相应处理。

10.如权利要求9所述检测处理盗取网站帐号的装置,其特征在于,所述处理单元进一步包括:

封禁处理模块,用于如果所述网站账号的用户属性为浏览属性用户,当其操作类型为浏览操作时,相应处理为允许浏览操作,当其操作类型为敏感行为操作时,相应处理为密码之外额外验证身份后允许敏感行为操作;所述敏感行为操作包括如下行为操作:更改资料、

支付、发布消息、发邮件，所述密码之外额外验证身份的方式包括：手机短信验证码验证。

一种检测处理盗取网站帐号的方法及装置

技术领域

[0001] 本发明涉及网络技术领域，尤其涉及一种检测处理盗取网站帐号的方法及装置。

背景技术

[0002] 网站帐号：俗称的网络身份证，是数字时代的代表，它是一种互联网身份认证协议，其具有唯一性和信息不可否认性，是在网络保存着一种用户身份记录。网站帐号是数字时代的代表，就是每个人在特定的项目中所代表自己的一些数字等。账号可以由中文或英文甚至符号组成。

[0003] 系统长期记录每个帐号的登录(在网站服务使用中，登录是用户进入网站服务开始进行身份认证的过程。几乎所有的登陆都需要用户有一个网站帐号和密码。当用键盘或其他输入设备输入正确的网站帐号和密码后完成。有些网站需要用户在使用之前注册，注册了的用户可以登陆以进入网站)信息，根据登录次数的多少，形成该帐号的常用地信息，例如一个帐号经常在北京登录。某一天，这个帐号突然在上海登录。那么系统可能认为用户存在被盗号(就是通过一定手段，盗取他人账号和密码。盗号是一种对用户和网站危害性极大的作恶行为)的问题。一般情况下，系统在一定时间会对该帐号进行强制下线且拒绝再次登录(即便帐号和密码匹配正确)。

[0004] 随着国家开发通信网络市场，很多第三方宽带或者移动服务商并非是严格按照城市去分配特定的IP，用户经常碰到明明是A城市接入网络，却被分配B城市的IP。这种情况下，基于用户常用登录地维度的检测机制，就非常容易造成误伤。

[0005] 或者用户本身出差等原因，造成无法形成一个稳定经常登录的城市。这种情况下，检测系统就因为没有常用登录地而无法工作。

[0006] 同时，对于被盗帐号，直接禁止对应帐号再次登录的处理，也比较简单粗暴，通常被盗情况下，系统会要求用户比较繁琐的验证身份后才可以解除，而有些用户使用网站只是简单的浏览操作，或者因为各种情况无法验证身份，例如验证工具为手机短信，用户可能手机忘记带或者因为短信延迟导致接收验证码存在问题。

[0007] 基于帐号和密码组合出现错误的次数进行检测。这种机制的理论基础是：常用的被盗方式包括暴力破解，即盗号者通常使用很多的计算机去尝试不同的密码，直到遍历出正确的密码。

[0008] 如果，一个帐号和不同密码的组合尝试登录后，几次错误后登录成功。那么系统会判断该帐号已经被盗。一般情况下，系统在一定时间会对该帐号进行强制下线且拒绝再次登录(即便帐号和密码匹配正确)。

[0009] 除了暴力破解外。当盗号者从一个其它已经获得特定帐号和密码，而通常两个网站的相同帐号对应的密码重合度，即对于单个帐号，通常一次登录就可以匹配正确登录成功。

[0010] 这种情况实际上非常普遍，因为普通用户的安全意识不强，加上记忆成本。一个用户在a网站注册帐号user a，密码password b，那么在b网站通常也是帐号user a和密码

password b的组合。盗号者从a网站获取一批帐号和密码，对于大型网站，用户的重合度很高，对应帐号和密码一样的比例非常高。

[0011] 所以，在这种场景下，基于帐号密码组合尝试登录错误的维度检测，效果会非常有限。

[0012] 目前网站安全非常重要的一个环节就是帐号安全，而帐号安全面临最大的威胁是帐号和密码被尝试或者泄露导致被盗。尤其已有帐号密码泄露，因为互联网早期，计算机性能限制和安全意识不强，很多网站保存用户密码是明文方式，一旦系统存在漏洞被盗号者获取，则盗号者会拿帐号和密码去不同网站登录。目前互联网上已经泄露的帐号有数十亿条。给网站和用户都带来极大的隐私和数据、财产安全的威胁。

发明内容

[0013] 本发明实施例提供一种检测处理盗取网站帐号的方法及装置，以提高网站用户的网站帐号登录的安全性。

[0014] 一方面，本发明实施例提供了一种检测处理盗取网站帐号的方法，所述方法包括：

[0015] 监测单一IP下，预设时间内登录成功超过预设数量的所有网站帐号；

[0016] 若所述所有网站帐号登录的登录口的个数不超过第一阈值，且其中大于或等于第二阈值的网站帐号登录的是同一个登录口，则判定所述IP为盗号IP；

[0017] 将所述IP进行限制登录的处理。

[0018] 另一方面，本发明实施例提供了一种检测处理盗取网站帐号的装置，所述装置包括：

[0019] 监测单元，用于监测单一IP下，预设时间内登录成功超过预设数量的所有网站帐号；

[0020] 判断单元，用于若所述所有网站帐号登录的登录口的个数不超过第一阈值，且其中大于或等于第二阈值的网站帐号登录的是同一个登录口，则判定所述IP为盗号IP；

[0021] 处理单元，用于将所述IP进行限制登录的处理。

[0022] 上述技术方案具有如下有益效果：提高了网站用户的网站帐号登录的安全性，本发明可以一定程度上检测盗号行为的发生，并在处理机制上，针对不同用户不同行为分别进行处理，在提高安全性的同时，也保证了用户体验。

附图说明

[0023] 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的前提下，还可以根据这些附图获得其他的附图。

[0024] 图1为本发明实施例一种检测处理盗取网站帐号的方法流程图；

[0025] 图2为本发明实施例一种检测处理盗取网站帐号的装置结构示意图；

[0026] 图3为本发明实施例处理单元结构示意图。

具体实施方式

[0027] 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做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。

[0028] 如图1所示，为本发明实施例一种检测处理盗取网站帐号的方法流程图，所述方法包括：

[0029] 101、监测单一IP下，预设时间内登录成功超过预设数量的所有网站帐号；

[0030] 102、若所述所有网站帐号登录的登录口的个数不超过第一阈值，且其中大于或等于第二阈值的网站帐号登录的是同一个登录口，则判定所述IP为盗号IP；

[0031] 103、将所述IP进行限制登录的处理。

[0032] 优选地，所述预设时间为1分钟，所述预设数量为10个。

[0033] 优选地，所述第一阈值为3；所述第二阈值为90％。

[0034] 优选地，所述将所述IP进行限制登录的处理，包括：对所述IP进行封禁设定时间处理并私信通知用户修改密码，同时对所述IP下已登录成功的网站帐号，设置用于指示所述网站账号被盗的标记，并根据网站账号的用户属性和操作类型分别进行相应处理。

[0035] 优选地，所述根据网站账号的用户属性和操作类型，分别进行相应处理，具体包括：如果所述网站账号的用户属性为浏览属性用户，当其操作类型为浏览操作时，相应处理为允许浏览操作，当其操作类型为敏感行为操作时，相应处理为密码之外额外验证身份后允许敏感行为操作；所述敏感行为操作包括如下行为操作：更改资料、支付、发布消息、发邮件等，所述密码之外额外验证身份的方式包括：手机短信验证码验证。

[0036] 对应于上述方法实施例，如图2所示，为本发明实施例一种检测处理盗取网站帐号的装置结构示意图，所述装置包括：

[0037] 监测单元21，用于监测单一IP下，预设时间内登录成功超过预设数量的所有网站帐号；

[0038] 判断单元22，用于若所述所有网站帐号登录的登录口的个数不超过第一阈值，且其中大于或等于第二阈值的网站帐号登录的是同一个登录口，则判定所述IP为盗号IP；

[0039] 处理单元23，用于将所述IP进行限制登录的处理。

[0040] 优选地，所述预设时间为1分钟，所述预设数量为10个。

[0041] 优选地，所述第一阈值为3；所述第二阈值为90％。

[0042] 优选地，所述处理单元，具体用于对所述IP进行封禁设定时间处理并私信通知用户修改密码，同时对所述IP下已登录成功的网站帐号，设置用于指示所述网站账号被盗的标记，并根据网站账号的用户属性和操作类型分别进行相应处理。

[0043] 优选地，如图3所示，为本发明实施例处理单元结构示意图，所述处理单元23，进一步包括：封禁处理模块231，用于如果所述网站账号的用户属性为浏览属性用户，当其操作类型为浏览操作时，相应处理为允许浏览操作，当其操作类型为敏感行为操作时，相应处理为密码之外额外验证身份后允许敏感行为操作；所述敏感行为操作包括如下行为操作：更改资料、支付、发布消息、发邮件等，所述密码之外额外验证身份的方式包括：手机短信验证码验证。

[0044] 上述技术方案具有如下有益效果:提高了网站用户的网站帐号登录的安全性,本发明可以一定程度上检测盗号行为的发生,并在处理机制上,针对不同用户不同行为分别进行处理,在提高安全性的同时,也保证了用户体验。

[0045] 以下举应用实例对本发明实施例上述技术方案进行详细说明:

[0046] 对于大型网站,通常有很多产品,对应不同的登录口,安全规则不统一。盗号者通常在安全防护薄弱的登录口,使用大量帐号和密码去尝试登录。帐号安全是互联网安全的一个重要环节,如果网站帐号大量被盗。盗号者一方面会利用这些帐号在网站上做恶,例如在社交平台发诈骗、色情等违规信息,会给网站的正常运营带来极大的干扰和危害。而对于用户,则可能损失绑定在网站帐号的各种敏感信息或者银行卡等财产信息。另外,如果对已经发送被盗的网站和密码进行处理一刀切禁止登录或者强制性验证密码之外的身份认证,会导致用户的强烈投诉,或者客服咨询量的剧增。而本发明应用实例就是根据盗号者这一行为特征,有效保护薄弱登录入口(很多大的互联网公司,旗下有各种各样的产品线,为了更高效率和更高安全标准管理,每个产品会有自己特定标示的登录入口),进而保护网站帐号的安全。

[0047] 本发明应用实例是一种基于登录口集中程度与否为基础的检测和处理盗取网站帐号的方法。运用聚类分析(聚类分析又称群分析,它是研究(样品或指标)分类问题的一种统计分析方法,同时也是数据挖掘的一个重要算法。聚类(Cluster)分析是由若干模式(Pattern)组成的,通常,模式是一个度量(Measurement)的向量,或者是多维空间中的一个点。聚类分析以相似性为基础,在一个聚类中的模式之间比不在同一聚类中的模式之间具有更多的相似性)方法,当一定时间特定或者有规律的一批IP下,所有的登录口都集中在一个或者有限几个。即在单个IP下,1分钟内登录成功了超过10个网站帐号,在这些所有登录成功的帐号,所有的帐号一共登录了不超过3个登录口,其中90%的帐号是登录是一个登录口。则将该登录IP视为盗号IP,而对该IP进行限制登录的处理。同时,对已登录成功的帐号,设置一个用于指示所述网站账号被盗的标记,并根据网站账号的用户属性和操作类型分别进行相应处理:如果所述网站账号的用户属性为浏览属性用户,当其操作类型为浏览操作时,相应处理为允许浏览操作,当其操作类型为敏感行为操作时,相应处理为密码之外额外验证身份后允许敏感行为操作;所述敏感行为操作包括如下行为操作:更改资料、支付、发布消息、发邮件等,所述密码之外额外验证身份的方式包括:手机短信验证码验证。

[0048] 以盗号者利用手里已经掌握的一批帐号和密码组合来尝试登录某一大型网站来举例,常用使用的IP为“8.8.1.1”“8.8.1.2”,尝试登录的网站子产品/服务为邮箱产品和博客,其具体方案如下:

[0049] a.盗号者使用邮箱特有的允许第三方调用POP3自动登录方式,即登录口为“邮箱POP3登录”;

[0050] b.盗号者在“8.8.1.1”分别尝试了100个帐号,登录邮箱产品。。

[0051] c.本发明实现的系统,发现“8.8.1.1”一分钟内登录了超过了10个帐号登系统会自动收集收集这个IP下所有登录成功的帐号。

[0052] d.系统同时会会计算绝大部分一分钟登录帐号数超过10个的IP的登录情况,因为该大型网站的每个产品的用户量都非常大,同一个IP下,使用各个产品都有一定规律的分布。目前统计证明,通常一个IP下,80%的帐号登录“微博”,8%的帐号登录“邮箱P03”,5%

的帐号登录“博客”,3%的帐号登录“新浪贴吧”,5%的帐号登录其它各个产品登录口。

[0053] e.系统对比发现IP“8.8.1.1”,登录的入口和大部分的出口/公用IP的登录入口(产品)分布有着较大的差异,主要是盗号者的登录入口偏单一。

[0054] 系统对比计算方式为:

[0055] 单个IP登录成功的总帐号数为Y,其中最多的登录口登录的帐号数为X,总登录口数量为M。

[0056] 当M＜3,X/Y＞＝90%。即认为该IP为盗号IP。

[0057] f.系统判定IP“8.8.1.1”是盗号者使用的IP,则对IP进行封禁一定时间处理。

[0058] g.而对于系统发现帐号密码与本网站匹配正确的帐号,进行私信通知,同时,会对主要历史行为为浏览的帐号,允许继续登录和浏览,但是不允许发布消息、发邮件、支付等敏感行为。

[0059] 本发明应用实例技术方案带来的有益效果:可以一定程度上检测盗号行为的发生,并在处理机制上,针对不同用户不同行为进行处理。在提高安全性的同时,也保证了用户体验。

[0060] 应该明白,公开的过程中的步骤的特定顺序或层次是示例性方法的实例。基于设计偏好,应该理解,过程中的步骤的特定顺序或层次可以在不脱离本公开的保护范围的情况下得到重新安排。所附的方法权利要求以示例性的顺序给出了各种步骤的要素,并且不是要限于所述的特定顺序或层次。

[0061] 在上述的详细描述中,各种特征一起组合在单个的实施方案中,以简化本公开。不应该将这种公开方法解释为反映了这样的意图,即,所要求保护的主题的实施方案需要比清楚地在每个权利要求中所陈述的特征更多的特征。相反,如所附的权利要求书所反映的那样,本发明处于比所公开的单个实施方案的全部特征少的状态。因此,所附的权利要求书特此清楚地被并入详细描述中,其中每项权利要求独自作为本发明单独的优选实施方案。

[0062] 为使本领域内的任何技术人员能够实现或者使用本发明,上面对所公开实施例进行了描述。对于本领域技术人员来说;这些实施例的各种修改方式都是显而易见的,并且本文定义的一般原理也可以在不脱离本公开的精神和保护范围的基础上适用于其它实施例。因此,本公开并不限于本文给出的实施例,而是与本申请公开的原理和新颖性特征的最广范围相一致。

[0063] 上文的描述包括一个或多个实施例的举例。当然,为了描述上述实施例而描述部件或方法的所有可能的结合是不可能的,但是本领域普通技术人员应该认识到,各个实施例可以做进一步的组合和排列。因此,本文中描述的实施例旨在涵盖落入所附权利要求书的保护范围内的所有这样的改变、修改和变型。此外,就说明书或权利要求书中使用的术语“包含”,该词的涵盖方式类似于术语“包括”,就如同“包括,”在权利要求中用作衔接词所解释的那样。此外,使用在权利要求书的说明书中的任何一个术语“或者”是要表示“非排它性的或者”。

[0064] 本领域技术人员还可以了解到本发明实施例列出的各种说明性逻辑块(illustrative logical block),单元,和步骤可以通过电子硬件、电脑软件,或两者的结合进行实现。为清楚展示硬件和软件的可替换性(interchangeability),上述的各种说明性部件(illustrative components),单元和步骤已经通用地描述了它们的功能。这样的功

能是通过硬件还是软件来实现取决于特定的应用和整个系统的设计要求。本领域技术人员可以对于每种特定的应用,可以使用各种方法实现所述的功能,但这种实现不应被理解为超出本发明实施例保护的范围。

[0065] 本发明实施例中所描述的各种说明性的逻辑块,或单元都可以通过通用处理器,数字信号处理器,专用集成电路(ASIC),现场可编程门阵列或其它可编程逻辑装置,离散门或晶体管逻辑,离散硬件部件,或上述任何组合的设计来实现或操作所描述的功能。通用处理器可以为微处理器,可选地,该通用处理器也可以为任何传统的处理器、控制器、微控制器或状态机。处理器也可以通过计算装置的组合来实现,例如数字信号处理器和微处理器,多个微处理器,一个或多个微处理器联合一个数字信号处理器核,或任何其它类似的配置来实现。

[0066] 本发明实施例中所描述的方法或算法的步骤可以直接嵌入硬件、处理器执行的软件模块、或者这两者的结合。软件模块可以存储于RAM存储器、闪存、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、可移动磁盘、CD-ROM或本领域中其它任意形式的存储媒介中。示例性地,存储媒介可以与处理器连接,以使得处理器可以从存储媒介中读取信息,并可以向存储媒介存写信息。可选地,存储媒介还可以集成到处理器中。处理器和存储媒介可以设置于ASIC中,ASIC可以设置于用户终端中。可选地,处理器和存储媒介也可以设置于用户终端中的不同的部件中。

[0067] 在一个或多个示例性的设计中,本发明实施例所描述的上述功能可以在硬件、软件、固件或这三者的任意组合来实现。如果在软件中实现,这些功能可以存储与电脑可读的媒介上,或以一个或多个指令或代码形式传输于电脑可读的媒介上。电脑可读媒介包括电脑存储媒介和便于使得让电脑程序从一个地方转移到其它地方的通信媒介。存储媒介可以是任何通用或特殊电脑可以接入访问的可用媒体。例如,这样的电脑可读媒体可以包括但不限于RAM、ROM、EEPROM、CD-ROM或其它光盘存储、磁盘存储或其它磁性存储装置,或其它任何可以用于承载或存储以指令或数据结构和其它可被通用或特殊电脑、或通用或特殊处理器读取形式的程序代码的媒介。此外,任何连接都可以被适当地定义为电脑可读媒介,例如,如果软件是从一个网站站点、服务器或其它远程资源通过一个同轴电缆、光纤电缆、双绞线、数字用户线(DSL)或以例如红外、无线和微波等无线方式传输的也被包含在所定义的电脑可读媒介中。所述的碟片(disk)和磁盘(disc)包括压缩磁盘、镭射盘、光盘、DVD、软盘和蓝光光盘,磁盘通常以磁性复制数据,而碟片通常以激光进行光学复制数据。上述的组合也可以包含在电脑可读媒介中。

[0068] 以上所述的具体实施方式,对本发明的目的、技术方案和有益效果进行了进一步详细说明,所应理解的是,以上所述仅为本发明的具体实施方式而已,并不用于限定本发明的保护范围,凡在本发明的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

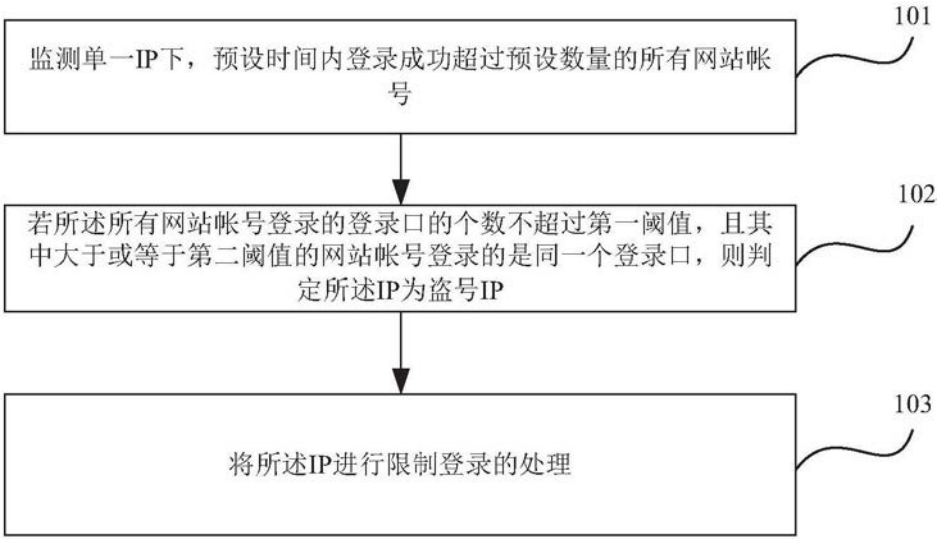

101
监测单一IP下，预设时间内登录成功超过预设数量的所有网站帐号
102
若所述所有网站帐号登录的登录口的个数不超过第一阈值，且其中大于或等于第二阈值的网站帐号登录的是同一个登录口，则判定所述IP为盗号IP
103
将所述IP进行限制登录的处理

图1

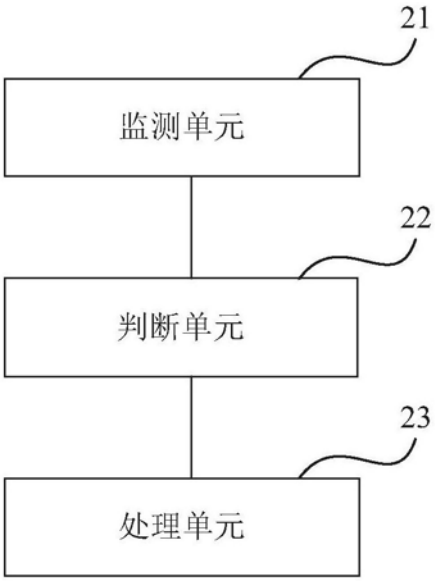

21
监测单元
22
判断单元
23
处理单元

图2

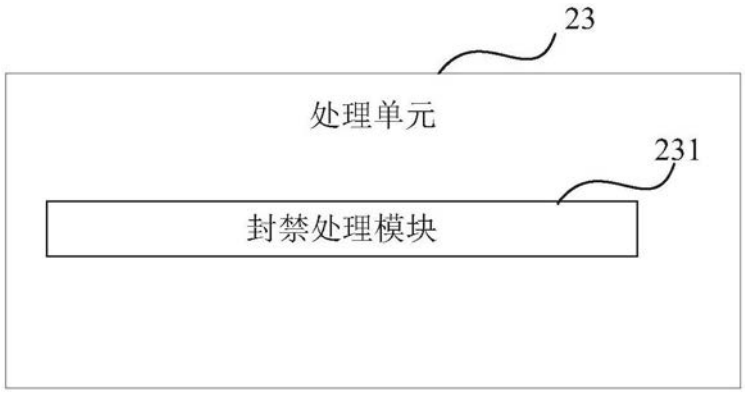


图3