(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110012011 A
(43)申请公布日 2019.07.12

(21)申请号 201910267464.1

(22)申请日 2019.04.03

(71)申请人 北京奇安信科技有限公司
地址 100088 北京市西城区新街口外大街28号102号楼3层332号

(72)发明人 聂君

(74)专利代理机构 北京英特普罗知识产权代理有限公司 11015
代理人 程超

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/46(2006.01)

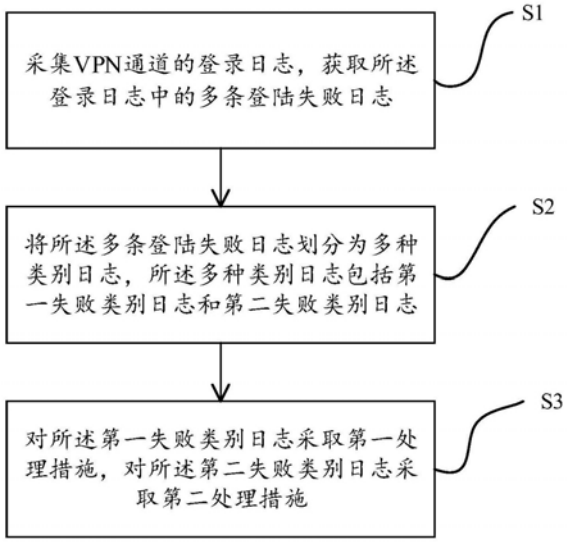
权利要求书2页 说明书8页 附图3页

(54)发明名称

防止恶意登录的方法、装置、计算机设备及存储介质

(57)摘要

本发明提供一种防止恶意登录的方法、装置、计算机设备及计算机存储介质，所述方法包括：采集VPN通道的登录日志，获取所述登录日志中的多条登陆失败日志；将所述多条登陆失败日志划分为多种类别日志，所述多种类别日志包括第一失败类别日志和第二失败类别日志；对所述第一失败类别日志采取第一处理措施，对所述第二失败类别日志采取第二处理措施。本发明对于恶意登陆失败事件，通过设置防火墙隔离等措施禁止恶意登录事件再次发生；对于善意登陆失败事件，通过向用户发送动态口令的方式，允许用户通过动态口令进行登录，从而最大程度保障正常用户利益，提升用户体验。



CN 110012011 A

1.一种防止恶意登录的方法,其特征在于,包括:

采集VPN通道的登录日志,获取所述登录日志中的多条登陆失败日志;

将所述多条登陆失败日志划分为多种类别日志,所述多种类别日志包括第一失败类别日志和第二失败类别日志;

对所述第一失败类别日志采取第一处理措施,对所述第二失败类别日志采取第二处理措施。

2.根据权利要求1所述的防止恶意登录的方法,其特征在于,所述采集VPN通道的登录日志,获取所述登录日志中的多条登陆失败日志的步骤包括:

获取所述多条登陆失败日志中的IP地址的属性信息;

将具有公共出口属性的IP地址所对应的登陆失败日志从所述多条登陆失败日志中删除。

3.根据权利要求2所述的防止恶意登录的方法,其特征在于,所述将所述登陆失败日志划分为多种类别日志,所述多种类别日志包括第一失败类别日志和第二失败类别日志的步骤包括:

从所述多条登陆失败日志中采集具有相同源地址的多条同源日志,获取所述多条同源日志中所包含的全部账户个数;

当所述全部账户个数大于第一阈值时,确定所述多条同源日志为第一失败类别日志;

从所述多条登录失败日志中提取包含相同账户的多条同账户日志,计算所述多条同账户日志的登录失败频率;

将登录失败频率大于第二阈值的所述多条同账户日志确定为第一失败类别日志;将登录失败频率不大于第二阈值的所述多条同账户日志确认为第二失败类别日志。

4.根据权利要求3所述的防止恶意登录的方法,其特征在于,所述对所述第一失败类别日志采取第一处理措施,对所述第二失败类别日志采取第二处理措施的步骤包括:

将所述第一失败类别日志中的源地址进行标记,并将所述第一失败类别日志中的源地址设置防火墙隔离;以及

向所述第二类别失败日志中的对应账户发送动态口令,以供所述第二类别失败日志中的对应账户根据所述动态口令进行登录。

5.根据权利要求3所述的防止恶意登录的方法,其特征在于,所述向所述第二类别失败日志中的对应账户发送动态口令,以供所述对应账户根据所述动态口令进行登录的步骤包括:

向所述第二类别失败日志中的对应账户相关联的移动设备发送动态口令,以供所述对应账户根据预留口令和所述动态口令的组合作为登录密码进行登录。

6.一种防止恶意登录的装置,其特征在于,包括:

日志采集模块,适用于实时采集VPN通道的登录日志,获取所述登录日志中的多条登陆失败日志;

日志分类模块,适用于将所述多条登陆失败日志划分为多种类别日志,所述多种类别日志包括第一失败类别日志和第二失败类别日志;

日志处理模块,适用于对所述第一失败类别日志采取第一处理措施,对所述第二失败类别日志采取第二处理措施。

7.根据权利要求6所述的防止恶意登录的装置，其特征在于，所述日志分类模块包括：

第一分类子模块，适用于从所述多条登陆失败日志中采集具有相同源地址的多条同源日志，获取所述多条同源日志中所包含的全部账户个数；当所述全部账户个数大于第一阈值时，确定所述多条同源日志为第一失败类别日志；

第二分类子模块，适用于从所述多条登录失败日志中提取包含相同账户的多条同账户日志，计算所述多条同账户日志的登录失败频率；将登录失败频率大于第二阈值的所述多条同账户日志确定为第一失败类别日志；将登录失败频率不大于第二阈值的所述多条同账户日志确认为第二失败类别日志。

8.根据权利要求7所述的防止恶意登录的装置，其特征在于，所述日志处理模块包括：

第一处理子模块，适用于将所述第一失败类别日志中的源地址进行标记，并将所述第一失败类别日志中的源地址设置防火墙隔离；

第二处理子模块，适用于向所述第二类别失败日志中的对应账户发送动态口令，以供所述第二类别失败日志中的对应账户根据所述动态口令进行登录。

9.一种计算机设备，包括存储器、处理器以及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现权利要求1至5任一项所述方法的步骤。

10.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现权利要求1至5任一项所述方法的步骤。

防止恶意登录的方法、装置、计算机设备及存储介质

技术领域

[0001] 本发明涉及网络安全技术领域，特别涉及一种防止恶意登录的方法、装置、计算机设备及存储介质。

背景技术

[0002] 目前很多企业为了方便员工远程办公，采用了VPN(虚拟专用网络)方案。VPN通常使用公网(如互联网)将远程分支机构或员工连接至企业网。当前的远程接入解决方案通常是依赖于身份认证系统，该系统实施一次或多次基于用户身份和密码组合的认证。这种认证方式很容易遭受到恶意的暴力攻击，例如暴力猜解。为了防止这类恶意攻击，现有技术往往采用对登录失败超过若干次数的账户进行锁定，即一段时间内禁止该账户进行任何登录操作。然而，这种简单粗暴的账户锁定可能会给善意登陆失败的用户带来很大困扰，因为有很多登录失败是由于用户想不起来密码而多次尝试造成的。因此，如何准确区分不同原因造成的远程账户登陆失败，并且对不同的登陆失败类型采取不同的处理措施，成为本领域技术人员亟待解决的问题。

发明内容

[0003] 本发明的目的是提供一种防止恶意登录的方法、装置、计算机设备及存储介质，以解决现有技术中存在的上述问题。

[0004] 为实现上述目的，本发明提供一种防止恶意登录的方法，包括以下步骤：

[0005] 采集VPN通道的登录日志，获取所述登录日志中的多条登陆失败日志；

[0006] 将所述多条登陆失败日志划分为多种类别日志，所述多种类别日志包括第一失败类别日志和第二失败类别日志；

[0007] 对所述第一失败类别日志采取第一处理措施，对所述第二失败类别日志采取第二处理措施。

[0008] 根据本发明提出的防止恶意登录的方法，其中，所述采集VPN通道的登录日志，获取所述登录日志中的多条登陆失败日志的步骤包括：

[0009] 获取所述多条登陆失败日志中的IP地址的属性信息；

[0010] 将具有公共出口属性的IP地址所对应的登陆失败日志从所述多条登陆失败日志中删除。

[0011] 根据本发明提出的防止恶意登录的方法，其中，所述将所述登陆失败日志划分为多种类别日志，所述多种类别日志包括第一失败类别日志和第二失败类别日志的步骤包括：

[0012] 从所述多条登陆失败日志中采集具有相同源地址的多条同源日志，获取所述多条同源日志中所包含的全部账户个数；

[0013] 当所述全部账户个数大于第一阈值时，确定所述多条同源日志为第一失败类别日志；

[0014] 从所述多条登录失败日志中提取包含相同账户的多条同账户日志，计算所述多条同账户日志的登录失败频率；

[0015] 将登录失败频率大于第二阈值的所述多条同账户日志确定为第一失败类别日志；将登录失败频率不大于第二阈值的所述多条同账户日志确认为第二失败类别日志。

[0016] 根据本发明提出的防止恶意登录的方法，其中，所述对所述第一失败类别日志采取第一处理措施，对所述第二失败类别日志采取第二处理措施的步骤包括：

[0017] 将所述第一失败类别日志中的源地址进行标记，并将所述第一失败类别日志中的源地址设置防火墙隔离；以及

[0018] 向所述第二类别失败日志中的对应账户发送动态口令，以供所述第二类别失败日志中的对应账户根据所述动态口令进行登录。

[0019] 根据本发明提出的防止恶意登录的方法，其中，所述向所述第二类别失败日志中的对应账户发送动态口令，以供所述对应账户根据所述动态口令进行登录的步骤包括：

[0020] 向所述第二类别失败日志中的对应账户相关联的移动设备发送动态口令，以供所述对应账户根据预留口令和所述动态口令的组合作为登录密码进行登录。

[0021] 为实现上述目的，本发明还提出一种防止恶意登录的装置，包括：

[0022] 日志采集模块，适用于实时采集VPN通道的登录日志，获取所述登录日志中的多条登陆失败日志；

[0023] 日志分类模块，适用于将所述多条登陆失败日志划分为多种类别日志，所述多种类别日志包括第一失败类别日志和第二失败类别日志；

[0024] 日志处理模块，适用于对所述第一失败类别日志采取第一处理措施，对所述第二失败类别日志采取第二处理措施。

[0025] 根据本发明提出的防止恶意登录的装置，其中，所述日志分类模块包括：

[0026] 第一分类子模块，适用于从所述多条登陆失败日志中采集具有相同源地址的多条同源日志，获取所述多条同源日志中所包含的全部账户个数；当所述全部账户个数大于第一阈值时，确定所述多条同源日志为第一失败类别日志；

[0027] 第二分类子模块，适用于从所述多条登录失败日志中提取包含相同账户的多条同账户日志，计算所述多条同账户日志的登录失败频率；将登录失败频率大于第二阈值的所述多条同账户日志确定为第一失败类别日志；将登录失败频率不大于第二阈值的所述多条同账户日志确认为第二失败类别日志。

[0028] 根据本发明提出的防止恶意登录的装置，其中，所述日志处理模块包括：

[0029] 第一处理子模块，适用于将所述第一失败类别日志中的源地址进行标记，并将所述第一失败类别日志中的源地址设置防火墙隔离；

[0030] 第二处理子模块，适用于向所述第二类别失败日志中的对应账户发送动态口令，以供所述第二类别失败日志中的对应账户根据所述动态口令进行登录。

[0031] 为实现上述目的，本发明还提供一种计算机设备，包括存储器、处理器以及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现上述方法的步骤。

[0032] 为实现上述目的，本发明还提供计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现上述方法的步骤。

[0033] 本发明提供的防止恶意登录的方法、装置、计算机设备及计算机存储介质，提供了精确判断登录失败事件并有针对性地提供相应处理措施的方案。通过分析大量登陆失败日志中包含的信息，本发明将登陆失败事件划分为第一失败类别和第二失败类别，即恶意登陆失败事件和善意登陆失败事件。对于恶意登陆失败事件，通过设置防火墙隔离等措施禁止恶意登录事件再次发生；对于善意登陆失败事件，通过向用户发送动态口令的方式，允许用户通过动态口令进行登录，从而最大程度保障正常用户利益，提升用户体验。

附图说明

[0034] 图1为本发明的防止恶意登录的方法实施例一的流程图；

[0035] 图2为本发明的防止恶意登录的装置实施例一的程序模块示意图；

[0036] 图3为本发明的防止恶意登录的装置实施例一的硬件结构示意图；

[0037] 图4为本发明的防止恶意登录的方法实施例二的流程图；

[0038] 图5为本发明的防止恶意登录的装置实施例二的程序模块示意图。

具体实施方式

[0039] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。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。

[0040] 本发明提供的防止恶意登录的方法、装置、计算机设备及计算机存储介质，提供了精确判断登录失败事件并有针对性地提供相应处理措施的方案。通过分析大量登陆失败日志中包含的信息，本发明将登陆失败事件划分为第一失败类别和第二失败类别，即恶意登陆失败事件和善意登陆失败事件。对于恶意登陆失败事件，通过设置防火墙隔离等措施禁止恶意登录事件再次发生；对于善意登陆失败事件，通过向用户发送动态口令的方式，允许用户通过动态口令进行登录，从而最大程度保障正常用户利益，提升用户体验。

[0041] 实施例一

[0042] 请参阅图1，本实施例提出一种防止恶意登录的方法，具体包括以下步骤：

[0043] S1:采集VPN通道的登录日志，获取所述登录日志中的多条登陆失败日志。

[0044] 本发明主要应用于通过VPN服务器接入网络来访问企业的应用、服务和数据的场景，例如客户端通过VPN服务器访问某远程终端上的信息管理系统。其中，VPN服务器可实施为专用物理机和嵌入式系统、托管在计算服务器节点上的软件元素、托管在虚拟机上的软件元素等。本发明可应用于多种VPN技术和协议，如点对点隧道协议(Point to Point Tunneling Protocol，PPTP)VPN、二层隧道协议(Layer 2Tunnerling Protocol，L2TP)VPN，因特网协议安全协议(Internet Protocol security，IPsec)VPN和安全套接层(Secure Sockets Layer，SSL)VPN等。

[0045] 通过远程终端的操作系统日志可以获取到外部客户端对于该远程终端的登录访问情况，例如是否登陆成功或者登录失败，本发明关注的仅仅是登陆失败日志。本发明采集远程终端上的操作系统登录日志，从操作系统登录日志中获取所有的登陆失败日志。上述采集操作系统登录日志的过程可以是实时进行的，也可以是按照固定时间点进行的，本发

明对此不做限定。

[0046] 在获取到多条登陆失败日志后，本发明需要进行过滤处理，去掉无法辨明失败类型的登陆失败日志，例如来自具有公共出口属性的IP地址的登陆失败日志。具有公共出口属性的IP地址一般是小型局域网的统一对外IP地址，这种统一对外IP地址实际上可能对应几十、上百或者上千个客户端口，所有客户端口发出的数据包含有相同的对外IP地址，例如某企业的共同对外IP地址，某网吧的共同对外IP地址等。从这种类型的IP地址发出的数据具有相同的源地址，但实际上是从多个客户端发出的，因此无法确切统计数据到底来自哪台或者哪几台计算机。基于上述原因，本发明首先去除来自公共出口属性的IP地址的登陆失败日志，避免对统计结果造成误导。

[0047] S2:将所述多条登陆失败日志划分为多种类别日志，所述多种类别日志包括第一失败类别日志和第二失败类别日志。

[0048] 本步骤根据源地址、账户个数以及账户发送频率来确定登陆失败事件时属于恶意登录失败还是善意登录失败。所谓恶意登录失败指的是黑客通过攻击进程频繁攻击账户的登录形式，例如通过暴力猜解的方式试图登录进入远程终端的管理系统；所谓善意登陆失败指的是正常用户因为记错密码、忘记密码、输错账户名等等原因造成无法成功登录的情况。在实际应用中，区分善意登录和恶意登陆失败，并分别采取不同的处理措施具有非常重要的意义，一方面有利于对恶意攻击进程及时发现处理，另一方面能够保障正常用户的合理利益，避免由于输入密码错误而造成损失。

[0049] 具体的，本发明首先从多条登陆失败日志中采集具有相同源地址的多条同源日志，获取所述多条同源日志中所包含的全部账户个数。登陆失败日志中至少包含源地址、目的地址、登录账户名、登陆时间等字段，通过登陆失败日志中的源地址字段有利于及时发现恶意攻击程序。

[0050] 当同一个IP源地址短时间内产生对多个账户登陆失败事件时，则怀疑有可能是恶意攻击程序试图破解账户名和密码来入侵系统。因此提取具有相同源地址的多条同源日志，获取多条同源日志中的所有登录账户名，当登录账户名的个数超过第一阈值时，确定所述多条同源日志为恶意登录失败日志，即第一失败类别日志。

[0051] 另外，针对同一个登录账户，如果短时间内多次发生登陆失败事件，则有可能有恶意程序正在试图破解该账户的密码。因此，本发明还可以从多条登录失败日志中获取具有同一登录用户名的多条同账户日志，若所述多条同账户日志的登录失败频率大于第二阈值，则将所述多条同账户日志确定为恶意登录失败日志，即第一失败类别日志。

[0052] S3:对所述第一失败类别日志采取第一处理措施，对所述第二失败类别日志采取第二处理措施。

[0053] 本步骤用于对恶意登录失败日志采取隔离或清理等方式消除隐患，对善意登陆失败日志则提供对应的补救办法保证正常用户能够登陆成功。

[0054] 对于确定为恶意登录失败日志的，本发明会将第一失败类别日志中涉及到的源地址进行标记，并根据源地址设置防火墙，隔离来自该源地址的所有数据。

[0055] 请继续参阅图2，示出了一种大数据平台的数据同步装置，在本实施例中，防止恶意登录的装置10可以包括或被分割成一个或多个程序模块，一个或者多个程序模块被存储于存储介质中，并由一个或多个处理器所执行，以完成本发明，并可实现上述防止恶意登录

的方法。本发明所称的程序模块是指能够完成特定功能的一系列计算机程序指令段，比程序本身更适合于描述防止恶意登录的装置10在存储介质中的执行过程。以下描述将具体介绍本实施例各程序模块的功能：

[0056] 日志采集模块11，适用于实时采集VPN通道的登录日志，获取所述登录日志中的多条登陆失败日志；

[0057] 日志分类模块12，适用于将所述多条登陆失败日志划分为多种类别日志，所述多种类别日志包括第一失败类别日志和第二失败类别日志；

[0058] 日志处理模块13，适用于对所述第一失败类别日志采取第一处理措施，对所述第二失败类别日志采取第二处理措施。

[0059] 其中，所述日志分类模块12包括：

[0060] 第一分类子模块121，适用于从所述多条登陆失败日志中采集具有相同源地址的多条同源日志，获取所述多条同源日志中所包含的全部账户个数；当所述全部账户个数大于第一阈值时，确定所述多条同源日志为第一失败类别日志；

[0061] 第二分类子模块122，适用于从所述多条登录失败日志中提取包含相同账户的多条同账户日志，计算所述多条同账户日志的登录失败频率；将登录失败频率大于第二阈值的所述多条同账户日志确定为第一失败类别日志；将登录失败频率不大于第二阈值的所述多条同账户日志确认为第二失败类别日志。

[0062] 其中，所述日志处理模块13包括：

[0063] 第一处理子模块131，适用于将所述第一失败类别日志中的源地址进行标记，并将所述第一失败类别日志中的源地址设置防火墙隔离；

[0064] 第二处理子模块132，适用于向所述第二类别失败日志中的对应账户发送动态口令，以供所述第二类别失败日志中的对应账户根据所述动态口令进行登录。

[0065] 本实施例还提供一种计算机设备，如可以执行程序的智能手机、平板电脑、笔记本电脑、台式计算机、机架式服务器、刀片式服务器、塔式服务器或机柜式服务器(包括独立的服务器，或者多个服务器所组成的服务器集群)等。本实施例的计算机设备20至少包括但不限于：可通过系统总线相互通信连接的存储器21、处理器22，如图3所示。需要指出的是，图3仅示出了具有组件21-22的计算机设备20，但是应理解的是，并不要求实施所有示出的组件，可以替代的实施更多或者更少的组件。

[0066] 本实施例中，存储器21(即可读存储介质)包括闪存、硬盘、多媒体卡、卡型存储器(例如，SD或DX存储器等)、随机访问存储器(RAM)、静态随机访问存储器(SRAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、可编程只读存储器(PROM)、磁性存储器、磁盘、光盘等。在一些实施例中，存储器21可以是计算机设备20的内部存储单元，例如该计算机设备20的硬盘或内存。在另一些实施例中，存储器21也可以是计算机设备20的外部存储设备，例如该计算机设备20上配备的插接式硬盘，智能存储卡(Smart Media Card,SMC)，安全数字(Secure Digital,SD)卡，闪存卡(Flash Card)等。当然，存储器21还可以既包括计算机设备20的内部存储单元也包括其外部存储设备。本实施例中，存储器21通常用于存储安装于计算机设备20的操作系统和各类应用软件，例如实施例一的防止恶意登录的装置10的程序代码等。此外，存储器21还可以用于暂时地存储已经输出或者将要输出的各类数据。

[0067] 处理器22在一些实施例中可以是中央处理器(Central Processing Unit,CPU)、

控制器、微控制器、微处理器、或其他数据处理芯片。该处理器22通常用于控制计算机设备20的总体操作。本实施例中，处理器22用于运行存储器21中存储的程序代码或者处理数据，例如运行防止恶意登录的装置10，以实现实施例一的防止恶意登录的方法。

[0068] 本实施例还提供一种计算机可读存储介质，如闪存、硬盘、多媒体卡、卡型存储器(例如，SD或DX存储器等)、随机访问存储器(RAM)、静态随机访问存储器(SRAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、可编程只读存储器(PROM)、磁性存储器、磁盘、光盘、服务器、App应用商城等等，其上存储有计算机程序，程序被处理器执行时实现相应功能。本实施例的计算机可读存储介质用于存储防止恶意登录的10，被处理器执行时实现实施例一的防止恶意登录的方法。

[0069] 实施例二

[0070] 请参阅图4，本实施例的防止恶意登录的方法，包括以下步骤：

[0071] S1:采集VPN通道的登录日志，获取所述登录日志中的多条登陆失败日志。

[0072] 本发明主要应用于通过VPN服务器接入网络来访问企业的应用、服务和数据的场景，例如客户端通过VPN服务器访问某远程终端上的信息管理系统。其中，VPN服务器可实施为专用物理机和嵌入式系统、托管在计算服务器节点上的软件元素、托管在虚拟机上的软件元素等。本发明可应用于多种VPN技术和协议，如点对点隧道协议(Point to Point Tunneling Protocol，PPTP)VPN、二层隧道协议(Layer 2Tunnerling Protocol，L2TP)VPN，因特网协议安全协议(Internet Protocol security，IPsec)VPN和安全套接层(Secure Sockets Layer，SSL)VPN等。

[0073] 通过远程终端的操作系统日志可以获取到外部客户端对于该远程终端的登录访问情况，例如是否登陆成功或者登录失败，本发明关注的仅仅是登陆失败日志。本发明采集远程终端上的操作系统登录日志，从操作系统登录日志中获取所有的登陆失败日志。上述采集操作系统登录日志的过程可以是实时进行的，也可以是按照固定时间点进行的，本发明对此不做限定。

[0074] 在获取到多条登陆失败日志后，本发明需要进行过滤处理，去掉无法辨明失败类型的登陆失败日志，例如来自具有公共出口属性的IP地址的登陆失败日志。具有公共出口属性的IP地址一般是小型局域网的统一对外IP地址，这种统一对外IP地址实际上可能对应几十、上百或者上千个客户端口，所有客户端口发出的数据包含有相同的对外IP地址，例如某企业的共同对外IP地址，某网吧的共同对外IP地址等。从这种类型的IP地址发出的数据具有相同的源地址，但实际上是从多个客户端发出的，因此无法确切统计数据到底来自哪台或者哪几台计算机。基于上述原因，本发明首先去除来自公共出口属性的IP地址的登陆失败日志，避免对统计结果造成误导。

[0075] S2:将所述多条登陆失败日志划分为多种类别日志，所述多种类别日志包括第一失败类别日志和第二失败类别日志。

[0076] 本步骤根据源地址、账户个数以及账户发送频率来确定登陆失败事件是属于恶意登录失败还是善意登录失败。所谓恶意登录失败指的是黑客通过攻击进程频繁攻击账户的登录形式，例如通过暴力猜解的方式试图登录进入远程终端的管理系统；所谓善意登陆失败指的是正常用户因为记错密码、忘记密码、输错账户名等等原因造成无法成功登录的情况。在实际应用中，区分善意登录和恶意登陆失败，并分别采取不同的处理措施具有非常重

要的意义，一方面有利于对恶意攻击进程及时发现处理，另一方面能够保障正常用户的合理利益，避免由于输入密码错误而造成损失。

[0077] 具体的，本发明首先从多条登陆失败日志中采集具有相同源地址的多条同源日志，获取所述多条同源日志中所包含的全部账户个数。登陆失败日志中至少包含源地址、目的地址、登录账户名、登陆时间等字段，通过登陆失败日志中的源地址字段可以判断登陆失败时间是否为善意登陆失败。这是因为，正常用户针对一个系统或者应用程序而言，大多只注册一个账户，最多也不会超过五个或者十个，二如果施工及程序恶意破解账户名密码，则有可能短时间内对成百上千个账户名进行暴力猜解，因此可以通过登录失败的账户名个数来判断是恶意登录还是善意登录。另外，针对同一个账户名，正常用户只会尝试有限次数的登录，如果几次登录都失败则可能会另想它法，不会不休止地不停尝试，因此也可以根据同一个账户名的登录频率来判断善意登录还是恶意登录。

[0078] 基于上述原则，本发明提取具有相同源地址的多条同源日志，获取多条同源日志中的所有登录账户名，当登录账户名的个数不超过第一阈值时，确定所述多条同源日志为善意登录失败日志，即第二失败类别日志。

[0079] 另外，本发明还可以从多条登录失败日志中获取具有同一登录用户名的多条同账户日志，若所述多条同账户日志的登录失败频率不大于第二阈值，则将所述多条同账户日志确定为善意登录失败日志，即第二失败类别日志。

[0080] S3:对所述第一失败类别日志采取第一处理措施，对所述第二失败类别日志采取第二处理措施。

[0081] 本步骤用于对恶意登录失败日志采取隔离或清理等方式消除隐患，对善意登陆失败日志则提供对应的补救办法保证正常用户能够登陆成功。

[0082] 对于确定为善意登录失败日志的，可以采取如下措施：例如通过修改FreeRadius认证代码，每个用户创建账户时在后台数据库保存一个只有自己知道PIN码，而当用户登录认证失败的时候，系统只将当前动态口令发送给客户的预设联系方式，例如以短信方式发送给用户手机，或者以邮件方式发送至用户邮箱等等，用户通过组合PIN码+动态口令来实现登录。本发明通过PIN码+动态口令的方式为远程VPN登录提供了双重保障，一方面由于PIN码是用户预留的，因此只有真正用户才知道该PIN码的具体形式；另外动态口令是通过用户预留的联系方式进行发送，因此也只有真正的用户才可以接收到动态口令。通过上述组合方式，可以提高用户重新登录账户的安全性，为用户忘记登录密码时提供安全可靠的补救措施。

[0083] 请继续参阅图5，本实施例的防止恶意登录的装置30以实施例一为基础，用以实现实施例二的防止恶意登录的方法，其包括的各程序模块的功能：

[0084] 日志采集模块31，适用于实时采集VPN通道的登录日志，获取所述登录日志中的多条登陆失败日志；

[0085] 日志分类模块32，适用于将所述多条登陆失败日志划分为多种类别日志，所述多种类别日志包括第一失败类别日志和第二失败类别日志；

[0086] 日志处理模块33，适用于对所述第一失败类别日志采取第一处理措施，对所述第二失败类别日志采取第二处理措施。

[0087] 其中，所述日志分类模块32包括：

[0088] 第一分类子模块321，适用于从所述多条登陆失败日志中采集具有相同源地址的多条同源日志，获取所述多条同源日志中所包含的全部账户个数；当所述全部账户个数大于第一阈值时，确定所述多条同源日志为第一失败类别日志；

[0089] 第二分类子模块322，适用于从所述多条登录失败日志中提取包含相同账户的多条同账户日志，计算所述多条同账户日志的登录失败频率；将登录失败频率大于第二阈值的所述多条同账户日志确定为第一失败类别日志；将登录失败频率不大于第二阈值的所述多条同账户日志确认为第二失败类别日志。

[0090] 其中，所述日志处理模块33包括：

[0091] 第一处理子模块331，适用于将所述第一失败类别日志中的源地址进行标记，并将所述第一失败类别日志中的源地址设置防火墙隔离；

[0092] 第二处理子模块332，适用于向所述第二类别失败日志中的对应账户发送动态口令，以供所述第二类别失败日志中的对应账户根据所述动态口令进行登录。

[0093] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0094] 流程图中或在此以其它方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的实施例所属技术领域的技术人员所理解。

[0095] 本技术领域的普通技术人员可以理解，实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

[0096] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0097] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。

[0098] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

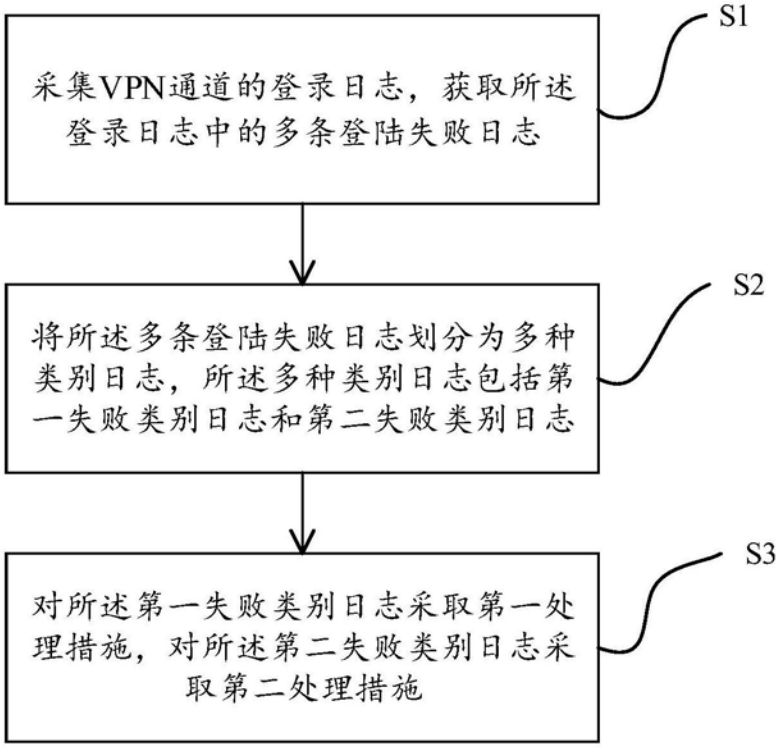

采集VPN通道的登录日志，获取所述登录日志中的多条登陆失败日志
S1
将所述多条登陆失败日志划分为多种类别日志，所述多种类别日志包括第一失败类别日志和第二失败类别日志
S2
对所述第一失败类别日志采取第一处理措施，对所述第二失败类别日志采取第二处理措施
S3

图1

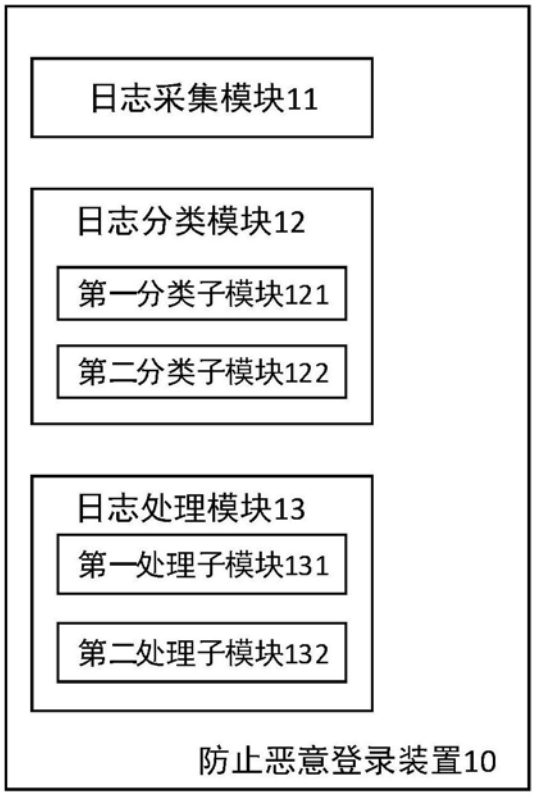

日志采集模块11
日志分类模块12
第一分类子模块121
第二分类子模块122
日志处理模块13
第一处理子模块131
第二处理子模块132
防止恶意登录装置10

图2

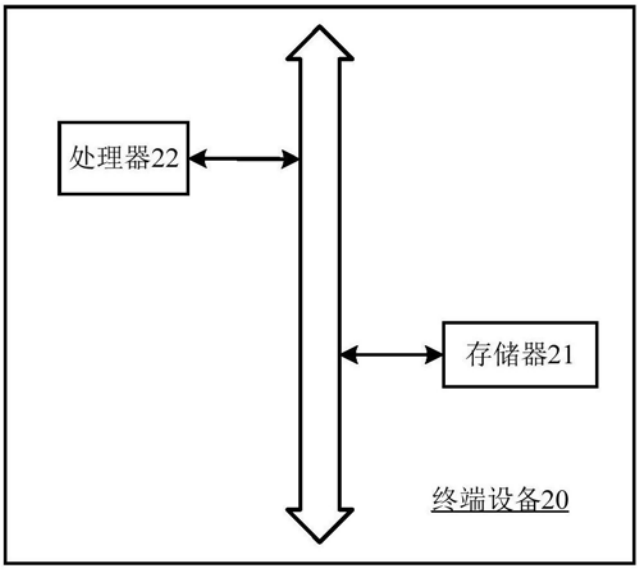

处理器22
存储器21
终端设备20

图3

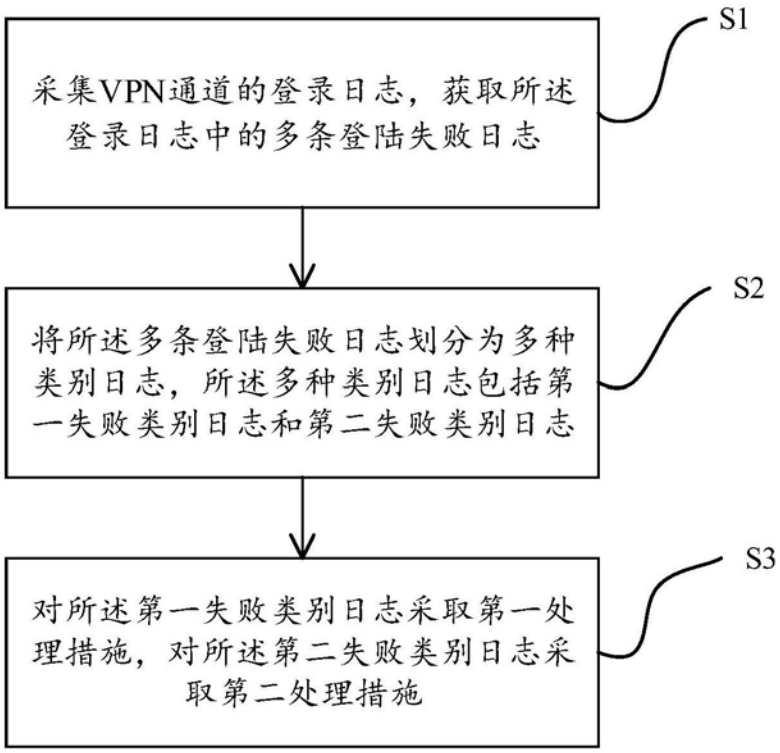

采集VPN通道的登录日志，获取所述登录日志中的多条登陆失败日志
S1
将所述多条登陆失败日志划分为多种类别日志，所述多种类别日志包括第一失败类别日志和第二失败类别日志
S2
对所述第一失败类别日志采取第一处理措施，对所述第二失败类别日志采取第二处理措施
S3

图4

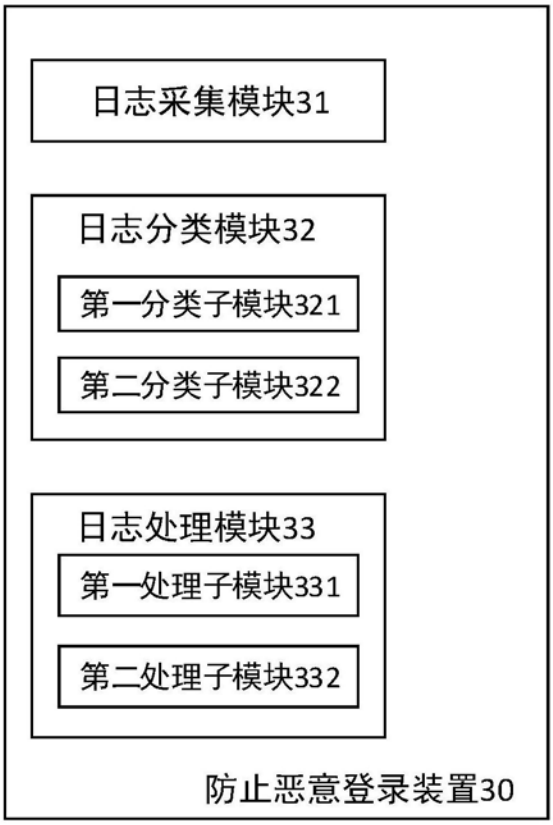

日志采集模块31
日志分类模块32
第一分类子模块321
第二分类子模块322
日志处理模块33
第一处理子模块331
第二处理子模块332
防止恶意登录装置30

图5