(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 109981611 A
(43)申请公布日 2019.07.05

(21)申请号 201910175420.6

(22)申请日 2019.03.08

(71)申请人 北京顺丰同城科技有限公司
地址 100083 北京市海淀区学清路10号院1号楼A座15层1501

(72)发明人 张彤宇

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 王庆龙 周永君

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

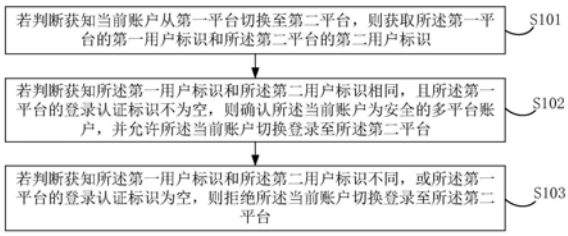
权利要求书2页 说明书6页 附图1页

(54)发明名称

一种多平台账户的安全防御方法及装置

(57)摘要

本发明实施例公开了一种多平台账户的安全防御方法及装置，方法包括：若判断获知当前账户从第一平台切换至第二平台，则获取第一平台的第一用户标识和第二平台的第二用户标识；若判断获知第一用户标识和第二用户标识相同，且第一平台的登录认证标识不为空，则允许当前账户切换登录至第二平台；若判断获知第一用户标识和第二用户标识不同，或第一平台的登录认证标识为空，则拒绝当前账户切换登录至第二平台。通过判断第一平台和第二平台的用户标识确定两个平台是否共用同一多平台账户，通过判断第一平台的登录认证标识是否为空确定第一平台是否是通过正常的登录界面登录，以防止XSS的多平台账户的泄露，更好地对各网站进行安全防御。



CN 109981611 A

1.一种多平台账户的安全防御方法,其特征在于,包括:

若判断获知当前账户从第一平台切换至第二平台,则获取所述第一平台的第一用户标识和所述第二平台的第二用户标识;

若判断获知所述第一用户标识和所述第二用户标识相同,且所述第一平台的登录认证标识不为空,则确认所述当前账户为安全的多平台账户,并允许所述当前账户切换登录至所述第二平台;

若判断获知所述第一用户标识和所述第二用户标识不同,或所述第一平台的登录认证标识为空,则拒绝所述当前账户切换登录至所述第二平台。

2.根据权利要求1所述的方法,其特征在于,所述若判断获知所述第一用户标识和所述第二用户标识不同,或所述第一平台的登录认证标识为空,则拒绝所述当前账户切换登录至所述第二平台之后,还包括:

生成第一授权提示信息,并将所述第一授权提示信息发送至目标终端;

若接收到所述目标终端反馈的第一授权信息,则允许所述当前账户切换登录至所述第二平台。

3.根据权利要求1所述的方法,其特征在于,所述若判断获知当前账户从第一平台切换至第二平台,则获取所述第一平台的第一用户标识和所述第二平台的第二用户标识之前,还包括:

若判断获知所述当前账户根据第一平台标识通过登录页面登录所述第一平台,则对所述第一平台的登录认证标识进行赋值。

4.根据权利要求3所述的方法,其特征在于,所述若判断获知所述当前账户根据第一平台标识通过登录页面登录所述第一平台,则对所述第一平台的登录认证标识进行赋值之后,还包括:

若判断获知所述当前账户的账户登录信息与历史登录信息不匹配,则生成第二授权提示信息,并将所述第二授权提示信息发送至目标终端;

若接收到所述目标终端反馈的第二授权信息,则允许所述当前账户登录至所述第一平台;

其中,所述历史登录信息包括所述目标终端的位置、IP地址和MAC地址。

5.根据权利要求4所述的方法,其特征在于,所述若接收到所述目标终端反馈的第二授权信息,则允许所述当前账户登录至所述第一平台之后,还包括:

若接收到所述目标终端反馈的拒绝授权信息,则向通信终端发送验证码请求;

若接收到所述通信终端返回的验证码,则根据所述验证码允许所述当前账户登录至所述第一平台。

6.根据权利要求1所述的方法,其特征在于,所述若判断获知所述第一用户标识和所述第二用户标识相同,且所述第一平台的登录认证标识不为空,则确认所述当前账户为安全的多平台账户,并允许所述当前账户切换登录至所述第二平台之后,还包括:

根据预设时间段对所述当前账户进行重新登录认证;

或,

若判断获知当前终端锁屏或重启,则对所述当前账户进行重新登录认证。

7.一种多平台账户的安全防御装置,其特征在于,包括:

标识获取模块，用于若判断获知当前账户从第一平台切换至第二平台，则获取所述第一平台的第一用户标识和所述第二平台的第二用户标识；

允许登录模块，用于若判断获知所述第一用户标识和所述第二用户标识相同，且所述第一平台的登录认证标识不为空，则确认所述当前账户为安全的多平台账户，并允许所述当前账户切换登录至所述第二平台；

拒绝登录模块，用于若判断获知所述第一用户标识和所述第二用户标识不同，或所述第一平台的登录认证标识为空，则拒绝所述当前账户切换登录至所述第二平台。

8.根据权利要求7所述的装置，其特征在于，所述装置还包括：

授权提示模块，用于生成第一授权提示信息，并将所述第一授权提示信息发送至目标终端；

切换登录模块，用于若接收到所述目标终端反馈的第一授权信息，则允许所述当前账户切换登录至所述第二平台。

9.一种电子设备，其特征在于，包括：

至少一个处理器；以及

与所述处理器通信连接的至少一个存储器，其中：

所述存储器存储有可被所述处理器执行的程序指令，所述处理器调用所述程序指令能够执行如权利要求1至6任一所述的方法。

10.一种非暂态计算机可读存储介质，其特征在于，所述非暂态计算机可读存储介质存储计算机程序，所述计算机程序使所述计算机执行如权利要求1至6任一所述的方法。

一种多平台账户的安全防御方法及装置

技术领域

[0001] 本发明实施例涉及网络安全技术领域，具体涉及一种多平台账户的安全防御方法及装置。

背景技术

[0002] 随着互联网的风靡和发展，人人都需要在互联网中留下自己的账户凭证以轻松地管理自己的信息，财务等资产。而每一家公司的产品，最重要的部分之一也一定是账户系统。与此同时，账户逐渐变得十分有价值，网络黑客有利可图，则使用各种技术尝试攻破账户系统以获取利益。国家也将互联网安全作为互联网发展的第一要务。

[0003] 常见的账号窃取，攻破方式有:XSS(Cross Site Scripting，跨站脚本攻击)，SQL(Structured Query Language，结构化查询语言)注入攻击，撞库、强破等等。XSS攻击全称跨站脚本攻击，为了不和层叠样式表(Cascading Style Sheets，CSS)的缩写混淆，故将跨站脚本攻击缩写为XSS，XSS是一种在web应用中的计算机安全漏洞，它允许恶意web用户将代码植入到提供给其它用户使用的页面中。而该代码具备获取加密的登录标识，由此则可以不获取用户明文信息的情况下伪装该用户使用网站服务，甚至直接攻破使用该账号系统的所有平台。SQL注入攻击是黑客对数据库进行攻击的常用手段之一，随着B/S模式应用开发的发展，使用这种模式编写应用程序的程序员也越来越多，但是由于程序员的水平及经验也参差不齐，相当大一部分程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据，这就是所谓的SQL Injection，即SQL注入。如:某个网站的登录验证的SQL查询代码为:strSQL＝"SELECT*FROM users WHERE(name＝"'+userName+"')and(pw＝""+passWord+"');"恶意填入userName＝"1'OR'1'＝'1";与passWord＝"1'OR'1'＝'1";时，将导致原本的SQL语句被填为strSQL＝"SELECT*FROM users WHERE(name＝'1'OR'1'＝'1')and(pw＝'1'OR'1'＝'1');"也就是实际上运行的SQL命令会变成下面这样的strSQL＝"SELECT*FROM users;"因此达到无账号密码，亦可登录网站。所以SQL注入攻击被俗称为黑客的填空游戏;在获取到了用户登录信息后，则可以进行撞库，大部分人在使用互联网账户时，使用的密码都近乎一致，对此则有机可乘，在获取到一定量账户信息时，则可以对更多的网站进行尝试，这就是撞库攻击;而强破是使用机器对一个已知用户名的账户进行无限次密码尝试。

[0004] 现有的互联网环境中，很多网站都无法对多平台账户的泄露进行很好地识别，导致XSS安全防御失败。

发明内容

[0005] 由于现有方法存在上述问题，本发明实施例提出一种多平台账户的安全防御方法及装置。

[0006] 第一方面，本发明实施例提出一种多平台账户的安全防御方法，包括：

[0007] 若判断获知当前账户从第一平台切换至第二平台，则获取所述第一平台的第一用户标识和所述第二平台的第二用户标识；

[0008] 若判断获知所述第一用户标识和所述第二用户标识相同，且所述第一平台的登录认证标识不为空，则确认所述当前账户为安全的多平台账户，并允许所述当前账户切换登录至所述第二平台；

[0009] 若判断获知所述第一用户标识和所述第二用户标识不同，或所述第一平台的登录认证标识为空，则拒绝所述当前账户切换登录至所述第二平台。

[0010] 第二方面，本发明实施例还提出一种多平台账户的安全防御装置，包括：

[0011] 标识获取模块，用于若判断获知当前账户从第一平台切换至第二平台，则获取所述第一平台的第一用户标识和所述第二平台的第二用户标识；

[0012] 允许登录模块，用于若判断获知所述第一用户标识和所述第二用户标识相同，且所述第一平台的登录认证标识不为空，则确认所述当前账户为安全的多平台账户，并允许所述当前账户切换登录至所述第二平台；

[0013] 拒绝登录模块，用于若判断获知所述第一用户标识和所述第二用户标识不同，或所述第一平台的登录认证标识为空，则拒绝所述当前账户切换登录至所述第二平台。

[0014] 第三方面，本发明实施例还提出一种电子设备，包括：

[0015] 至少一个处理器；以及

[0016] 与所述处理器通信连接的至少一个存储器，其中：

[0017] 所述存储器存储有可被所述处理器执行的程序指令，所述处理器调用所述程序指令能够执行上述方法。

[0018] 第四方面，本发明实施例还提出一种非暂态计算机可读存储介质，所述非暂态计算机可读存储介质存储计算机程序，所述计算机程序使所述计算机执行上述方法。

[0019] 由上述技术方案可知，本发明实施例通过判断第一平台和第二平台的用户标识确定两个平台是否共用同一多平台账户，通过判断第一平台的登录认证标识是否为空确定第一平台是否是通过正常的登录界面登录，以防止XSS的多平台账户的泄露，更好地对各网站进行安全防御。

附图说明

[0020] 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，还可以根据这些图获得其他的附图。

[0021] 图1为本发明一实施例提供的一种多平台账户的安全防御方法的流程示意图；

[0022] 图2为本发明一实施例提供的一种多平台账户的安全防御装置的结构示意图；

[0023] 图3为本发明一实施例提供的电子设备的逻辑框图。

具体实施方式

[0024] 下面结合附图，对本发明的具体实施方式作进一步描述。以下实施例仅用于更加清楚地说明本发明的技术方案，而不能以此来限制本发明的保护范围。

[0025] 图1示出了本实施例提供的一种多平台账户的安全防御方法的流程示意图，包括：

[0026] S101、若判断获知当前账户从第一平台切换至第二平台，则获取所述第一平台的第一用户标识和所述第二平台的第二用户标识。

[0027] 其中，所述第一平台和所述第二平台是可以共用一个登录账户进行登录的两个不同的平台。例如：某个应用程序和另一领用程序都通过微信账号登录；再比如：百度账号可以同时登录百度外卖和百度网盘两个平台。

[0028] 用户标识为平台的登录账户的标识。

[0029] 举例来说，百度外卖平台的用户标识为百度账号，百度网盘平台的用户标识也是百度账号。

[0030] S102、若判断获知所述第一用户标识和所述第二用户标识相同，且所述第一平台的登录认证标识不为空，则确认所述当前账户为安全的多平台账户，并允许所述当前账户切换登录至所述第二平台。

[0031] 其中，所述登录认证标识为平台通过登录页面登录后获得的标识，用于判断当前账户是否通过登录页面登录。

[0032] 举例来说，用户通过登录页面登录了百度外卖平台，因此获得了百度外卖平台的登录认证标识；当用户需要切换至百度网盘平台时，由于共用一个百度账号，且具有登录认证标识，因此是安全的切换，允许当前账户直接切换登录至百度网盘平台，而无需重新登录。

[0033] S103、若判断获知所述第一用户标识和所述第二用户标识不同，或所述第一平台的登录认证标识为空，则拒绝所述当前账户切换登录至所述第二平台。

[0034] 举例来说，用户通过登录页面，用百度账户登录了百度外卖平台，现在想切换至快递寄件平台，该快递寄件平台使用快递寄件账户登录，无法使用百度账户登录，因此无法直接切换登录，必须重新登录快递寄件平台。

[0035] 再比如，用户从百度地图平台切换登录了百度外卖平台，因此未获得百度外卖平台的登录认证标识；当用户需要切换至百度网盘平台时，由于不具有登录认证标识，可能前一次是非法的切换登录，因此认为是不安全的切换，拒绝当前账户直接切换登录至百度网盘平台，需要重新登录。

[0036] 在实际执行过程中，即使采用严密的防御及时，也依然有攻破的可能，而止损方案则是分散认证，由于XSS攻击仅仅可以拿到当前域名的登录加密标识，因此为不同的一级域名拥有自己的一个辅助验证的平台标识，称之为“PlatformToken”，而用户加密信息的用户标识称之为“USERTOKEN”，在登录域名上，再加入一个登录认证标识“PassToken”。设置规则为：“PlatformToken+USERTOKEN＝仅本二级域名登录通过；USERTOKEN+PassToken＝账号系统域名登录通过”，攻击者若侥幸攻破一个平台，他可以拿到USERTOKEN和PlatformToken，此时他期望使用两个标志访问其他同一级域名不同二级域名的服务，是无法使用的，因此实现了良好的止损。

[0037] 本实施例通过判断第一平台和第二平台的用户标识确定两个平台是否共用同一多平台账户，通过判断第一平台的登录认证标识是否为空确定第一平台是否是通过正常的登录界面登录，以防止XSS的多平台账户的泄露，更好地对各网站进行安全防御。

[0038] 进一步地，在上述方法实施例的基础上，S103之后，还包括：

[0039] S104、生成第一授权提示信息，并将所述第一授权提示信息发送至目标终端。

[0040] S105、若接收到所述目标终端反馈的第一授权信息，则允许所述当前账户切换登录至所述第二平台。

[0041] 具体地，当终端拒绝所述当前账户切换登录至所述第二平台后，生成第一授权提示信息，并将所述第一授权提示信息发送至目标终端，其中，目标终端可以为用户之前授权的终端，也可以为首次注册终端。

[0042] 通过用户的实时授权，确保当前账户未被攻击，是安全的切换登录。

[0043] 进一步地，在上述方法实施例的基础上，S101之前，还包括：

[0044] S1000、若判断获知所述当前账户根据第一平台标识通过登录页面登录所述第一平台，则对所述第一平台的登录认证标识进行赋值。

[0045] S1001、若判断获知所述当前账户的账户登录信息与历史登录信息不匹配，则生成第二授权提示信息，并将所述第二授权提示信息发送至目标终端。

[0046] S1002、若接收到所述目标终端反馈的第二授权信息，则允许所述当前账户登录至所述第一平台。

[0047] S1003、若接收到所述目标终端反馈的拒绝授权信息，则向通信终端发送验证码请求。

[0048] S1004、若接收到所述通信终端返回的验证码，则根据所述验证码允许所述当前账户登录至所述第一平台。

[0049] 其中，所述历史登录信息包括所述目标终端的位置、IP地址和MAC地址。

[0050] 所述平台标识为当前平台的标识，例如百度外卖平台和百度网盘平台具有不同的平台标识，用以区分不同的平台。

[0051] 具体地，当目标终端由于误操作等原因反馈拒绝授权信息，而实际上是安全账户，则可以向通信终端发送验证码请求，其中，通信终端可以为用户之前授权的终端，也可以为首次注册终端。

[0052] 通过验证码方式授权，防止用户在第一次授权操作时的误操作。

[0053] 进一步地，在上述方法实施例的基础上，S102之后，还包括：

[0054] 根据预设时间段对所述当前账户进行重新登录认证；或，若判断获知当前终端锁屏或重启，则对所述当前账户进行重新登录认证。

[0055] 具体地，对于已经攻破的平台，若数据足够敏感，账号系统并不能让他一直使用服务。可以依据账号数据的敏感性，设置不同的验证时间段。同时，当设备锁屏再开启时，重新验证账号密码；当设备重启时，重新验证账号密码。当访问到十分敏感的数据前，或执行十分敏感的操作前，进行账号密码验证，以保证平台的安全性。

[0056] 具体来说，本实施例提供的多平台账户的安全防御方法包括以下步骤：

[0057] A1、在用户使用服务时收集以下信息：用户位置，IP地址，MAC物理地址，以及最近浏览器访问记录。

[0058] A2、若用户位置，IP地址，MAC地址突然发生变化，则给首次登陆的浏览器或终端进行警告和授权提示，确定是否为允许使用的浏览器或终端。用户允许则继续切换登录，并将允许的浏览器信息记录以备下次直接授权；若用户不允许则直接禁止操作。

[0059] A3、增加申诉机制，即不被授权的浏览器端，可以使用手机验证码登录，即可认为

新登录人为真实账户拥有者，否则禁止原浏览器操作。

[0060] A4、设置规则为："PlatformToken+USERTOKEN＝仅本二级域名登录通过；USERTOKEN+PassToken＝账号系统域名登录通过"，攻击者若侥幸攻破一个平台，他可以拿到USERTOKEN和PlatformToken，但无法使用别的二级域名的服务，实现了良好的止损。

[0061] A5、依据账号数据敏感性，有一些验证时间段；当设备锁屏再开启时，重新验证账号密码；当设备重启时，重新验证账号密码；当访问到十分敏感的数据前，或执行十分敏感的操作前，进行账号密码验证。

[0062] 本实施例能够保证用户不被XSS攻击窃取信息，进行敏感操作，同时对XSS攻击的用户进行了告警和及时止损，保证了各平台的安全。

[0063] 图2示出了本实施例提供的一种多平台账户的安全防御装置的结构示意图，所述装置包括：标识获取模块201、允许登录模块202和拒绝登录模块203，其中：

[0064] 所述标识获取模块201用于若判断获知当前账户从第一平台切换至第二平台，则获取所述第一平台的第一用户标识和所述第二平台的第二用户标识；

[0065] 所述允许登录模块202用于若判断获知所述第一用户标识和所述第二用户标识相同，且所述第一平台的登录认证标识不为空，则确认所述当前账户为安全的多平台账户，并允许所述当前账户切换登录至所述第二平台；

[0066] 所述拒绝登录模块203用于若判断获知所述第一用户标识和所述第二用户标识不同，或所述第一平台的登录认证标识为空，则拒绝所述当前账户切换登录至所述第二平台。

[0067] 具体地，所述标识获取模块201若判断获知当前账户从第一平台切换至第二平台，则获取所述第一平台的第一用户标识和所述第二平台的第二用户标识；所述允许登录模块202若判断获知所述第一用户标识和所述第二用户标识相同，且所述第一平台的登录认证标识不为空，则确认所述当前账户为安全的多平台账户，并允许所述当前账户切换登录至所述第二平台；所述拒绝登录模块203若判断获知所述第一用户标识和所述第二用户标识不同，或所述第一平台的登录认证标识为空，则拒绝所述当前账户切换登录至所述第二平台。

[0068] 本实施例通过判断第一平台和第二平台的用户标识确定两个平台是否共用同一多平台账户，通过判断第一平台的登录认证标识是否为空确定第一平台是否是通过正常的登录界面登录，以防止XSS的多平台账户的泄露，更好地对各网站进行安全防御。

[0069] 进一步地，在上述装置实施例的基础上，所述装置还包括：

[0070] 授权提示模块，用于生成第一授权提示信息，并将所述第一授权提示信息发送至目标终端；

[0071] 切换登录模块，用于若接收到所述目标终端反馈的第一授权信息，则允许所述当前账户切换登录至所述第二平台。

[0072] 进一步地，在上述装置实施例的基础上，所述装置还包括：

[0073] 赋值模块，用于若判断获知所述当前账户根据第一平台标识通过登录页面登录所述第一平台，则对所述第一平台的登录认证标识进行赋值。

[0074] 进一步地，在上述装置实施例的基础上，所述装置还包括：

[0075] 信息发送模块，用于若判断获知所述当前账户的账户登录信息与历史登录信息不匹配，则生成第二授权提示信息，并将所述第二授权提示信息发送至目标终端。

[0076] 平台登录模块，用于若接收到所述目标终端反馈的第二授权信息，则允许所述当前账户登录至所述第一平台。

[0077] 其中，所述历史登录信息包括所述目标终端的位置、IP地址和MAC地址。

[0078] 进一步地，在上述装置实施例的基础上，所述装置还包括：

[0079] 验证码发送模块，用于若接收到所述目标终端反馈的拒绝授权信息，则向通信终端发送验证码请求。

[0080] 验证码返回模块，用于若接收到所述通信终端返回的验证码，则根据所述验证码允许所述当前账户登录至所述第一平台。

[0081] 进一步地，在上述装置实施例的基础上，所述装置还包括：

[0082] 重新认证模块，用于根据预设时间段对所述当前账户进行重新登录认证，或，若判断获知当前终端锁屏或重启，则对所述当前账户进行重新登录认证。

[0083] 本实施例所述的多平台账户的安全防御装置可以用于执行上述方法实施例，其原理和技术效果类似，此处不再赘述。

[0084] 参照图3，所述电子设备，包括：处理器(processor)301、存储器(memory)302和总线303；

[0085] 其中，

[0086] 所述处理器301和存储器302通过所述总线303完成相互间的通信；

[0087] 所述处理器301用于调用所述存储器302中的程序指令，以执行上述各方法实施例所提供的方法。

[0088] 本实施例公开一种计算机程序产品，所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算机程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，计算机能够执行上述各方法实施例所提供的方法。

[0089] 本实施例提供一种非暂态计算机可读存储介质，所述非暂态计算机可读存储介质存储计算机指令，所述计算机指令使所述计算机执行上述各方法实施例所提供的方法。

[0090] 以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

[0091] 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各实施方式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。基于这样的理解，上述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计算机可读存储介质中，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，或者网络设备等)执行各个实施例或者实施例的某些部分所述的方法。

[0092] 应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

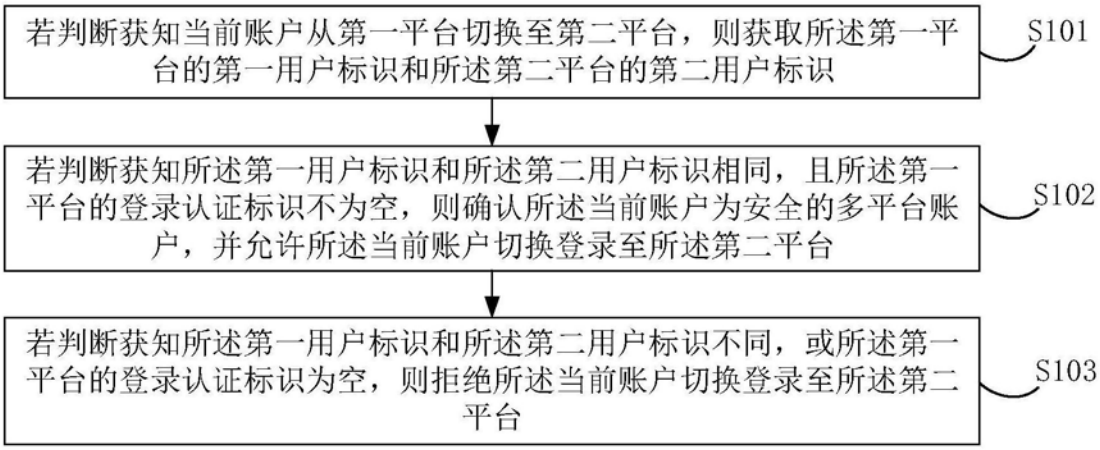

若判断获知当前账户从第一平台切换至第二平台，则获取所述第一平台的第一用户标识和所述第二平台的第二用户标识
S101
若判断获知所述第一用户标识和所述第二用户标识相同，且所述第一平台的登录认证标识不为空，则确认所述当前账户为安全的多平台账户，并允许所述当前账户切换登录至所述第二平台
S102
若判断获知所述第一用户标识和所述第二用户标识不同，或所述第一平台的登录认证标识为空，则拒绝所述当前账户切换登录至所述第二平台
S103

图1

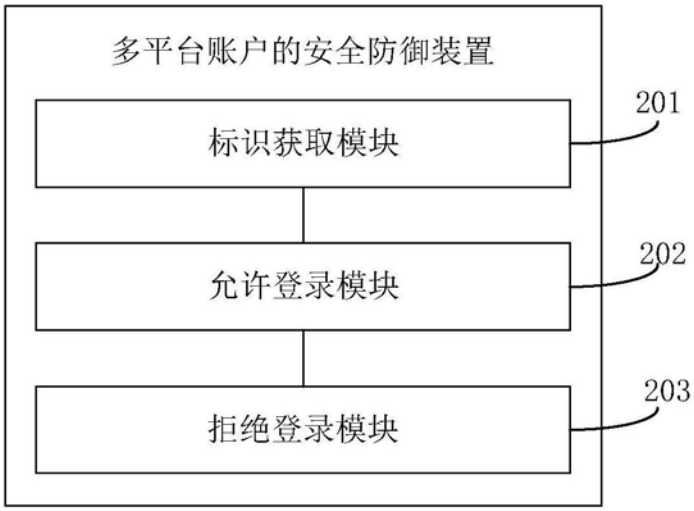

多平台账户的安全防御装置
标识获取模块
201
允许登录模块
202
拒绝登录模块
203

图2

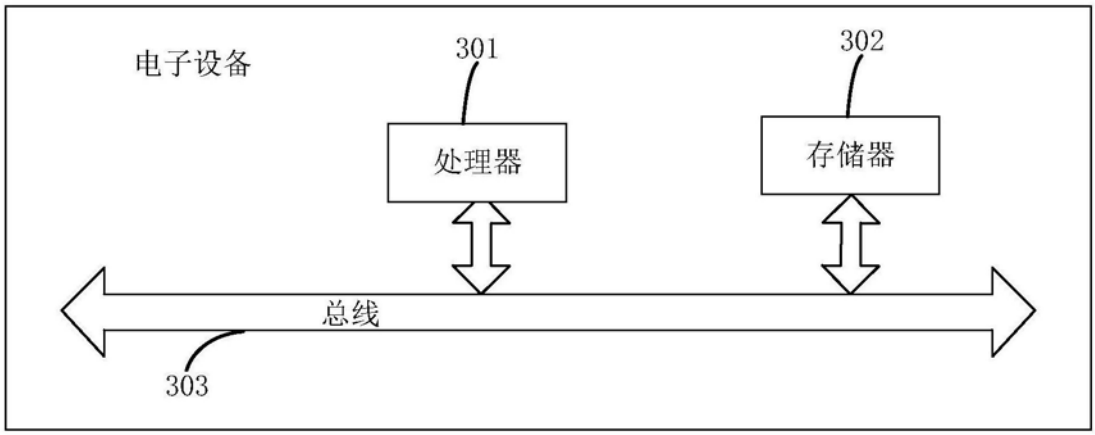

电子设备
301
处理器
302
存储器
总线
303

图3