



(12)发明专利

(10)授权公告号 CN 105099708 B

(45)授权公告日 2018.05.15

(21)申请号 201510540195.3

(56)对比文件

(22)申请日 2015.08.28

CN 102300182 A, 2011.12.28,

(65)同一申请的已公布的文献号

CN 103002415 A, 2013.03.27,

申请公布号 CN 105099708 A

CN 104320767 A, 2015.01.28,

(43)申请公布日 2015.11.25

审查员 许婵

(73)专利权人 上海亿保健康管理有限公司

地址 201802 上海市嘉定区嘉前路688弄6  
号2115室

(72)发明人 李洋

(74)专利代理机构 杭州君度专利代理事务所  
(特殊普通合伙) 33240

代理人 诸佩艳

(51)Int.Cl.

H04L 9/32(2006.01)

H04L 29/06(2006.01)

权利要求书1页 说明书4页 附图1页

(54)发明名称

一种身份验证方法

(57)摘要

本发明公开了一种身份验证方法，用于用户通过客户端与后台服务器之间实现身份验证，首先用户发送验证请求到后台服务器，后台服务器接收到用户发来的验证请求后，查找是否存在对应的校验信息，如果存在对应的校验信息，则读取该校验信息；如果没有对应的校验信息，则生成新的校验信息，并保存；然后后台服务器将所述校验信息发送给用户，用户接收到校验信息后，将接收到的校验信息发送给后台服务器，后台服务器比较从用户处接收到的校验信息与本地保存的校验信息，如果一致则验证通过，清除对应的校验信息，否则验证失败。本发明的方法能够有效避免数据冲突导致的用户体验不好的情况。

用户发送验证请求到后台服务器

后台服务器接收到用户发来的验证请求后，查找是否存在对应的校验信息，如果存在对应的校验信息，则读取该校验信息；如果没有对应的校验信息，则生成新的校验信息，并保存

后台服务器将所述校验信息发送给用户

用户接收到校验信息后，将接收到的校验信息发送给后台服务器

后台服务器比较从用户处接收到的校验信息与本地保存的校验信息，如果一致则校验通过，清除对应的校验信息，否则校验失败

1. 一种身份验证方法,用于用户通过客户端与后台服务器之间实现身份验证,其特征在于,所述方法包括:

    用户发送验证请求到后台服务器;

    后台服务器接收到用户发来的验证请求后,查找是否存在对应的校验信息,如果存在对应的校验信息,则读取该校验信息;如果没有对应的校验信息,则生成新的校验信息,并保存;

    后台服务器将读取的校验信息或新生成的校验信息发送给用户;

    用户接收到校验信息后,将接收到的校验信息发送给后台服务器;

    后台服务器比较从用户处接收到的校验信息与本地保存的校验信息,如果一致则验证通过,清除对应的校验信息,否则验证失败;

    其中,所述校验信息还设置有对应的有效期,所述后台服务器接收到用户发来的验证请求后,查找是否存在对应的校验信息,是查找是否存在对应的有效校验信息;

    所述如果存在对应的校验信息,则读取该校验信息之后,还包括步骤:

        延长该校验信息的有效期,并将延长了有效期的该校验信息保存。

2. 根据权利要求1所述的身份验证方法,其特征在于,所述清除对应的校验信息是设置该校验信息的有效期为失效。

3. 根据权利要求1所述的身份验证方法,其特征在于,所述验证请求还包括校验信息发送所采用的通道模式,所述通道模式包括短信模式、邮件模式、微信模式。

4. 根据权利要求3所述的身份验证方法,其特征在于,所述后台服务器接收到用户发来的验证请求后,还包括步骤:

    获取验证请求中包括的通道模式,根据通道模式查找对应的校验信息或生成新的校验信息。

5. 根据权利要求4所述的身份验证方法,其特征在于,所述后台服务器将所述校验信息发送给用户,是通过验证请求中包括的通道模式发送校验信息。

6. 根据权利要求1-5任一权利要求所述的身份验证方法,其特征在于,所述校验信息保存在缓存中。

## 一种身份验证方法

### 技术领域

[0001] 本发明属于计算机安全技术领域,尤其涉及一种身份验证方法。

### 背景技术

[0002] 随着互联网的发展,以及智能手机的普及,移动互联网开始进入人们的日常生活。由于移动终端比较容易丢失,丢失的移动终端容易被他人利用来登录用户的互联网应用帐号。因此现在的互联网应用都设置有用户身份验证的环节,通过校验用户身份与手机号户主身份的关联,确认是用户本人在使用。

[0003] 目前进行身份验证的过程通常由客户端发送请求到后台服务器,后台服务器生成验证码,通过多种形式发送给用户,例如短信、邮件、微信等等,用户收到验证码后,在客户端上输入验证码发送给后台服务器,后台服务器接收到客户端发来的验证码,通过比较发来的验证码与后台服务器生成的验证码是否一致,来判断是否是用户本人在使用。

[0004] 但是目前这种方式的送达率较低,采用多次/多途径验证客户信息时,方案间会互相产生数据冲突,导致降低用户体验。例如在后台服务器生成一个验证码发送给用户后,如果用户没有在规定时间内收到,客户端则会再次发送请求,后台服务器再生成另一个验证码发送给用户,前一个验证码失效。而此时如果用户收到并填写第一个验证码,则会导致验证错误,后台服务器会再次生成并发出第三个验证码。

[0005] 显然当用户经历过多次验证错误后,会降低用户体验。

### 发明内容

[0006] 本发明的目的是提供一种身份验证方法,以避免现有技术中出现数据冲突,导致降低用户体验的问题。

[0007] 为了实现上述目的,本发明技术方案如下:

[0008] 一种身份验证方法,用于用户通过客户端与后台服务器之间实现身份验证,所述方法包括:

[0009] 用户发送验证请求到后台服务器;

[0010] 后台服务器接收到用户发来的验证请求后,查找是否存在对应的校验信息,如果存在对应的校验信息,则读取该校验信息;如果没有对应的校验信息,则生成新的校验信息,并保存;

[0011] 后台服务器将所述校验信息发给用户;

[0012] 用户接收到校验信息后,将接收到的校验信息发给后台服务器;

[0013] 后台服务器比较从用户处接收到的校验信息与本地保存的校验信息,如果一致则验证通过,清除对应的校验信息,否则验证失败。

[0014] 进一步地,所述校验信息还设置有对应的有效期,所述后台服务器接收到用户发来的验证请求后,查找是否存在对应的校验信息,是查找是否存在对应的有效校验信息。

[0015] 进一步地,所述如果存在对应的校验信息,则读取该校验信息之后,还包括步骤:

- [0016] 延长该校验信息的有效期,并将延长了有效期的该校验信息保存。
- [0017] 进一步地,所述清除对应的校验信息是设置该校验信息的有效期为失效。
- [0018] 本发明所述验证请求还包括校验信息发送所采用的通道模式,所述通道模式包括短信模式、邮件模式、微信模式。
- [0019] 进一步地,所述后台服务器接收到用户发来的验证请求后,还包括步骤:
- [0020] 获取验证请求中包括的通道模式,根据通道模式查找对应的校验信息或生成新的校验信息。
- [0021] 进一步地,所述后台服务器将所述校验信息发送给用户,是通过验证请求中包括的通道模式发送校验信息。
- [0022] 本发明所述校验信息保存在缓存中,该缓存可以是后台服务器本地的缓存,也可以是与后台服务器相连的缓存系统。
- [0023] 本发明提出的一种身份验证方法,通过在缓存中存储校验信息,在接收到用户的验证请求后,查找对应的校验信息,在存在有效的校验信息时,直接使用该有效校验信息发送给用户,能够有效避免数据冲突导致的用户体验不好的情况。

## 附图说明

- [0024] 图1为本发明一种身份验证方法流程图。

## 具体实施方式

- [0025] 下面结合附图和实施例对本发明技术方案做进一步详细说明,以下实施例不构成对本发明的限定。
- [0026] 身份验证是通过比较用户输入的校验信息与后台服务器存储的最后一次校验信息是否一致,来判断当前登录的用户确实是注册的合法用户。通常通过短信、邮件、微信等通道模式来实现验证,其实质是判断当前登录的用户确实是某个关联信息的用户,例如是注册时注册的手机号码的户主,或者是注册时注册的邮件地址、微信号的户主。
- [0027] 本实施例以短信发送校验信息(一般为验证码)为例,来对本发明的方法进行说明,对于微信、邮件通道模式的用户验证同样适用。
- [0028] 如图1所示,一种身份验证方法,包括如下步骤:
- [0029] F1、用户发送验证请求到后台服务器。
- [0030] 用户在登录互联网应用时,或在需要进行用户身份验证时,通过客户端向后台服务器发送验证请求。客户端是用户用来登录和访问互联网应用的设备,可以是安装了客户端软件的手机、平板电脑、普通PC等。
- [0031] F2、后台服务器接收到用户发来的验证请求后,查找是否存在对应的校验信息,如果存在对应的校验信息,则读取该校验信息;如果没有对应的校验信息,则生成新的校验信息,并保存。
- [0032] 本实施例的校验信息保存在缓存中,缓存可以是后台服务器本地的缓存,也可以是与后台服务器相连的缓存系统,本发明不限于缓存的具体形式。
- [0033] 后台服务器接收到用户发来的验证请求后,根据用户的ID在缓存中查找对应的验证信息。

[0034] 如果缓存中存在对应的校验信息，则读取该校验信息，从而后台服务器具有了该校验信息。如果缓存中没有对应的校验信息，则生成新的校验信息，并将该校验信息同步到缓存，在缓存中保存。

[0035] 可见通过本步骤，本发明的身份验证方法能够有效避免用户没有在规定时间内收到校验信息，而重复发送验证请求导致的后台服务器再生成另一个校验信息的问题。当用户没有在规定时间内收到校验信息，而重复发送验证请求，本实施例的方法是在缓存中查找对应的校验信息，当后台服务器第二次收到验证请求时，首先是在缓存中查找是否存在该用户对应的校验信息，由于第一次验证请求生成的校验信息没有被清除，因此就会查找到该校验信息，从而将该校验信息发送给用户，不会再生成第二个校验信息。也就不会发生用户在发送第二次验证请求后收到第一个校验信息，输入第一次的校验信息而导致的验证失败问题，即消除了数据冲突的可能，提高了校验的效率。

[0036] 需要说明的是，本发明并不限于校验信息保存的介质，可以是上述的缓存，也可以是服务器的存储器，直接将校验信息保存在数据库中。而校验信息在缓存中保存的形式通常为一条记录，该记录包括校验信息、用户ID，便于根据用户ID来查找对应的校验信息。

[0037] 本实施例的校验信息还设置有对应的有效期，例如为30分钟，该有效期高于允许用户没有收到校验信息再次发送验证请求的时长。在不设置有效期时，校验信息在缓存中长期有效。在校验信息长期有效时，当其他原因导致验证失败时，缓存中的校验信息长期有效，使得校验信息存在泄露的风险，容易被不法用户利用。设置有效期能够有效避免这种情况，即使在其他原因导致验证失败的情况下，该校验信息也很快过期，需要重新生成，促使校验信息的及时更新，避免被不法用户利用。

[0038] 进一步地，当后台服务器在缓存中查找是否存在对应的校验信息时，如果查找到对应的有效校验信息，则还包括步骤：

[0039] 延长该校验信息的有效期，并将延长了有效期的该校验信息同步到缓存，在缓存中保存。

[0040] 本实施例默认的校验信息的有效期为30分钟，而延长校验信息的有效期，是将当前校验信息的有效期再次设置为30分钟。容易理解的是，后台服务器接收到用户发来的验证请求后，查找是否存在对应的校验信息，是查找是否存在对应的有效校验信息，对于失效的校验信息不再考虑范围内，这里不再赘述。

[0041] F3、后台服务器将校验信息发送给用户。

[0042] 后台服务器读取到校验信息、或新生成校验信息后，即将校验信息发送给用户，本实施例是通过手机短信的方式发送。

[0043] F4、用户接收到校验信息后，将接收到的校验信息发送给后台服务器。

[0044] 用户通过手机短信收到校验信息后，将校验信息通过客户端发送给后台服务器进行身份验证。

[0045] F5、后台服务器比较从用户处接收到的校验信息与本地保存的校验信息，如果一致则验证通过，清除对应的校验信息，否则验证失败。

[0046] 后台服务器接收到用户输入的校验信息后，与步骤F2获取的校验信息进行比较，如果一致则表示用户是通过合法途径得到校验信息的，用户是合法用户，验证通过；否则认为用户输入错误，验证失败。

[0047] 在验证通过后,还清除缓存中对应的校验信息,可以直接删除,或设置其有效期为失效。可见,在校验正常通过的情况下,校验信息都会被清除,这种情况下校验信息是不是设置有效期,并没有什么影响。而当用户输入错误导致验证失败时,校验信息不会被清除,如果用户停止了继续验证,则该校验信息被保留,容易被其他人用于登录。因此本实施例为校验信息设置了有效期,通常为30分钟,在有效期后,该校验信息失效。而后台服务器在接收到用户的验证请求,通过查找发现缓存中的校验信息已经失效,则重新生成新的校验信息,如果还没有失效则延长其有效期,将校验信息发给用户。

[0048] 综上所述,本发明的身份验证方法,通过在缓存中存储校验信息,在接收到用户的验证请求后,查找对应的校验信息,来有效避免数据冲突导致的用户体验不好的情况。

[0049] 由于可以通过短信模式、邮件模式、微信等通道模式来实现校验信息的发送,校验信息通常为校验码,因此本实施例的验证请求还包括通道模式,后台服务器收到验证请求后,根据通道模式查找对应的校验信息或生成新的校验信息,并在后续步骤中通过该通道模式发送校验信息。当互联网应用系统仅支持一种通道模式时,验证请求中可以不包括通道模式。

[0050] 以上实施例仅用以说明本发明的技术方案而非对其进行限制,在不背离本发明精神及其实质的情况下,熟悉本领域的技术人员当可根据本发明作出各种相应的改变和变形,但这些相应的改变和变形都应属于本发明所附的权利要求的保护范围。

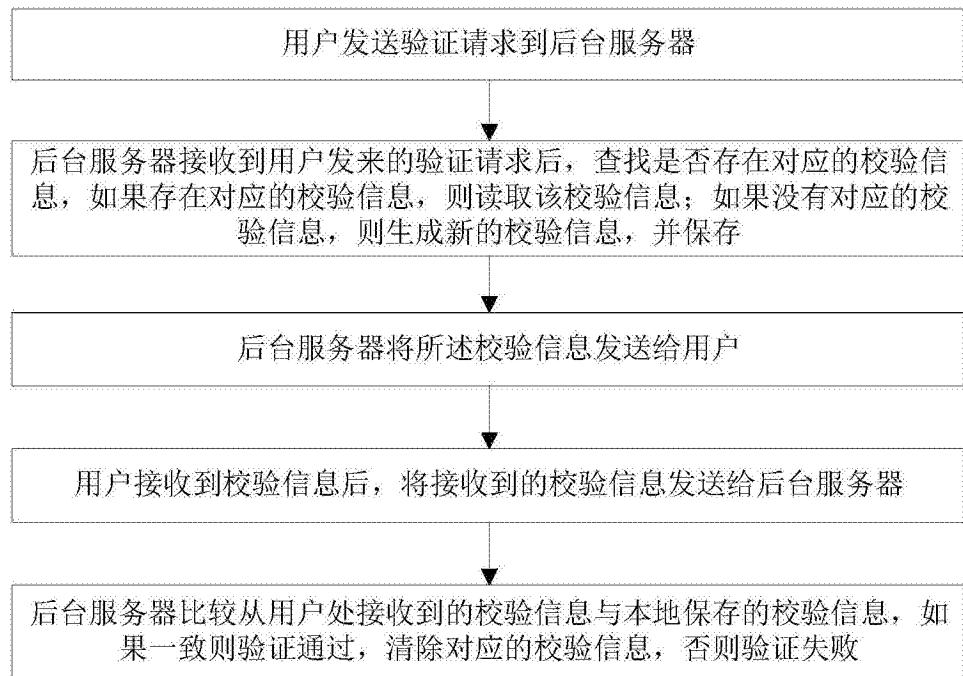


图1