(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 108462713 A
(43)申请公布日 2018.08.28

(21)申请号 201810241978.5

(22)申请日 2018.03.22

(71)申请人 北京可信华泰信息技术有限公司
地址 100097 北京市海淀区蓝靛厂金源时代购物中心B区2号B座705、706室

(72)发明人 孙瑜 杨秩

(74)专利代理机构 北京安博达知识产权代理有限公司 11271
代理人 徐国文

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

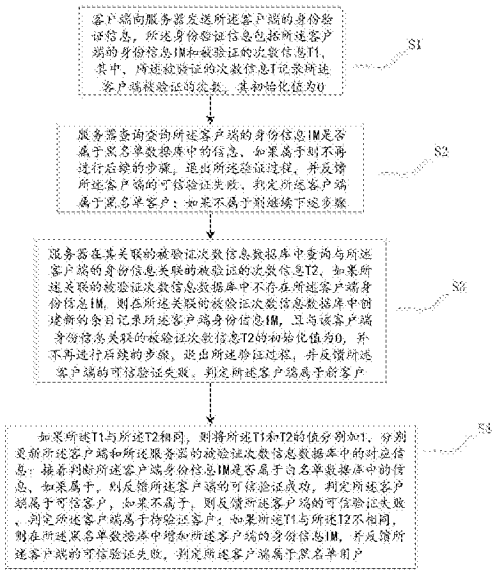
权利要求书2页 说明书4页 附图1页

(54)发明名称

一种客户端进行可信验证的方法和系统

(57)摘要

本发明公开了一种客户端进行可信验证的方法和系统，通过客户端身份验证信息与服务器保存的对应信息的比较来进行可信验证，另外，利用黑名单、白名单机制对不同客户端进行验证管理，以提高可信验证的安全性。



CN 108462713 A

1.一种客户端进行可信验证的方法,其特征在于包括下述步骤:

(1)客户端向服务器发送所述客户端的身份验证信息,所述身份验证信息包括所述客户端的身份信息IM和被验证的次数信息T1,其中,所述被验证的次数信息T记录所述客户端被验证的次数,其初始化值为0;

(2)服务器查询查询所述客户端的身份信息IM是否属于黑名单数据库中的信息,如果属于则不再进行后续的步骤,退出所述验证过程,并反馈所述客户端的可信验证失败、判定所述客户端属于黑名单客户;如果不属于则继续下述步骤;

(3)服务器在其关联的被验证次数信息数据库中查询与所述客户端的身份信息关联的被验证的次数信息T2,如果所述关联的被验证次数信息数据库中不存在所述客户端身份信息IM,则在所述关联的被验证次数信息数据库中创建新的条目记录所述客户端身份信息IM,且与该客户端身份信息关联的被验证次数信息T2的初始化值为0,并不再进行后续的步骤,退出所述验证过程,并反馈所述客户端的可信验证失败、判定所述客户端属于新客户;

(4)如果所述T1与所述T2相同,则将所述T1和T2的值分别加1,分别更新所述客户端和所述服务器的被验证次数信息数据库中的对应信息;接着判断所述客户端身份信息IM是否属于白名单数据库中的信息,如果属于,则反馈所述客户端的可信验证成功,判定所述客户端属于可信客户,如果不属于,则反馈所述客户端的可信验证失败,判定所述客户端属于待验证客户;

如果所述T1与所述T2不相同,则在所述黑名单数据库中增加所述客户端的身份信息IM,并反馈所述客户端的可信验证失败,判定所述客户端属于黑名单用户。

2.如权利要求1所述的方法,其特征在于所述客户端是移动客户端。

3.如权利要求2所述的方法,其特征在于所述客户端的身份信息IM为移动手机号。

4.如权利要求2所述的方法,其特征在于所述客户端的身份信息IM为移动手机的国际移动设备身份码IMEI值。

5.如权利要求4所述的方法,其特征在于当所述客户端被判定为待验证客户,服务器则向服务器管理者发送所述客户端的身份验证信息,由所述管理者进一步确定验证结果,如果验证为可信客户,则所述白名单数据库增加所述客户端的身份信息,如果验证为不可信客户,则所述黑名单数据库增加所述客户段的身份信息。

6.一种客户端进行可信验证的系统,其特征在于包括下述模块:

发送模块,用于客户端向服务器发送所述客户端的身份验证信息,所述身份验证信息包括所述客户端的身份信息IM和被验证的次数信息T1,其中,所述被验证的次数信息T记录所述客户端被验证的次数,其初始化值为0;

查询模块,用于服务器查询查询所述客户端的身份信息IM是否属于黑名单数据库中的信息,如果属于则不再进行后续的步骤,退出所述验证过程,并反馈所述客户端的可信验证失败、判定所述客户端属于黑名单客户;如果不属于则继续下述步骤;

第一验证模块,用于服务器在其关联的被验证次数信息数据库中查询与所述客户端的身份信息关联的被验证的次数信息T2,如果所述关联的被验证次数信息数据库中不存在所述客户端身份信息IM,则在所述关联的被验证次数信息数据库中创建新的条目记录所述客户端身份信息IM,且与该客户端身份信息关联的被验证次数信息T2的初始化值为0,并不再进行后续的步骤,退出所述验证过程,并反馈所述客户端的可信验证失败、判定所述客户端

属于新客户；

第二验证模块，用于如果所述T1与所述T2相同，则将所述T1和T2的值分别加1，分别更新所述客户端和所述服务器的被验证次数信息数据库中的对应信息；接着判断所述客户端身份信息IM是否属于白名单数据库中的信息，如果属于，则反馈所述客户端的可信验证成功，判定所述客户端属于可信客户，如果不属于，则反馈所述客户端的可信验证失败，判定所述客户端属于待验证客户；如果所述T1与所述T2不相同，则在所述黑名单数据库中增加所述客户端的身份信息IM，并反馈所述客户端的可信验证失败，判定所述客户端属于黑名单用户。

7.如权利要求6所述的系统，其特征在于所述客户端是移动客户端。

8.如权利要求7所述的系统，其特征在于所述客户端的身份信息IM为移动手机号。

9.如权利要求7所述的系统，其特征在于所述客户端的身份信息IM为移动手机的国际移动设备身份码IMEI值。

10.如权利要求9所述的系统，其特征在于还包括第三验证模块，用于当所述客户端被判定为待验证客户，服务器则向服务器管理者发送所述客户端的身份验证信息，由所述管理者进一步确定验证结果，如果验证为可信客户，则所述白名单数据库增加所述客户端的身份信息，如果验证为不可信客户，则所述黑名单数据库增加所述客户段的身份信息。

一种客户端进行可信验证的方法和系统

【技术领域】

[0001] 本发明涉及计算机可信验证技术领域，具体涉及一种客户端进行可信验证的方法和系统。

【背景技术】

[0002] 有关可信计算的概念，在ISO/IEC 15408标准中给出了以下定义：一个可信的组件、操作或过程的行为在任意操作条件下是可预测的，并能很好地抵抗应用程序软件、病毒以及一定的物理干扰造成的破坏。可信计算的基本思路是在硬件平台上引入安全芯片(可信平台模块)来提高终端系统的安全性，也就是说在每个终端平台上植入一个信任根，让计算机从BIOS到操作系统内核层，再到应用层都构建信任关系；以此为基础，扩大到网络上，建立相应的信任链，从而进入计算机免疫时代。当终端受到攻击时，可实现自我保护、自我管理和自我恢复。

[0003] 但是，目前方案和手段都是以安全芯片的方式对计算机内部的部件进行可信验证，但随着大数据，云计算的兴起，网络中任意一台计算机都都相当于过去的一个计算机部件，因此，需要有新的手段对网络中的计算机进行可信验证。

【发明内容】

[0004] 为了解决上述问题，本发明提出了一种客户端进行可信验证的方法和系统，包括下述步骤：

[0005] (1)客户端向服务器发送所述客户端的身份验证信息，所述身份验证信息包括所述客户端的身份信息IM和被验证的次数信息T1，其中，所述被验证的次数信息T记录所述客户端被验证的次数，其初始化值为0；

[0006] (2)服务器查询查询所述客户端的身份信息IM是否属于黑名单数据库中的信息，如果属于则不再进行后续的步骤，退出所述验证过程，并反馈所述客户端的可信验证失败、判定所述客户端属于黑名单客户；如果不属于则继续下述步骤；

[0007] (3)服务器在其关联的被验证次数信息数据库中查询与所述客户端的身份信息关联的被验证的次数信息T2，如果所述关联的被验证次数信息数据库中不存在所述客户端身份信息IM，则在所述关联的被验证次数信息数据库中创建新的条目记录所述客户端身份信息IM，且与该客户端身份信息关联的被验证次数信息T2的初始化值为0，并不再进行后续的步骤，退出所述验证过程，并反馈所述客户端的可信验证失败、判定所述客户端属于新客户；

[0008] (4)如果所述T1与所述T2相同，则将所述T1和T2的值分别加1，分别更新所述客户端和所述服务器的被验证次数信息数据库中的对应信息；接着判断所述客户端身份信息IM是否属于白名单数据库中的信息，如果属于，则反馈所述客户端的可信验证成功，判定所述客户端属于可信客户，如果不属于，则反馈所述客户端的可信验证失败，判定所述客户端属于待验证客户；

[0009] 如果所述T1与所述T2不相同，则在所述黑名单数据库中增加所述客户端的身份信息IM，并反馈所述客户端的可信验证失败，判定所述客户端属于黑名单用户。

[0010] 在上述技术方案的基础上，所述客户端是移动客户端。

[0011] 在上述技术方案的基础上，所述客户端的身份信息IM为移动手机号。

[0012] 在上述技术方案的基础上，所述客户端的身份信息IM为移动手机的国际移动设备身份码IMEI值。

[0013] 在上述技术方案的基础上，当所述客户端被判定为待验证客户，服务器则向服务器管理者发送所述客户端的身份验证信息，由所述管理者进一步确定验证结果，如果验证为可信客户，则所述白名单数据库增加所述客户端的身份信息，如果验证为不可信客户，则所述黑名单数据库增加所述客户段的身份信息。

[0014] 本发明还提出了一种客户端进行可信验证的系统，包括下述模块：

[0015] 发送模块，用于客户端向服务器发送所述客户端的身份验证信息，所述身份验证信息包括所述客户端的身份信息IM和被验证的次数信息T1，其中，所述被验证的次数信息T记录所述客户端被验证的次数，其初始化值为0；

[0016] 查询模块，用于服务器查询查询所述客户端的身份信息IM是否属于黑名单数据库中的信息，如果属于则不再进行后续的步骤，退出所述验证过程，并反馈所述客户端的可信验证失败、判定所述客户端属于黑名单客户；如果不属于则继续下述步骤；

[0017] 第一验证模块，用于服务器在其关联的被验证次数信息数据库中查询与所述客户端的身份信息关联的被验证的次数信息T2，如果所述关联的被验证次数信息数据库中不存在所述客户端身份信息IM，则在所述关联的被验证次数信息数据库中创建新的条目记录所述客户端身份信息IM，且与该客户端身份信息关联的被验证次数信息T2的初始化值为0，并不再进行后续的步骤，退出所述验证过程，并反馈所述客户端的可信验证失败、判定所述客户端属于新客户；

[0018] 第二验证模块，用于如果所述T1与所述T2相同，则将所述T1和T2的值分别加1，分别更新所述客户端和所述服务器的被验证次数信息数据库中的对应信息；接着判断所述客户端身份信息IM是否属于白名单数据库中的信息，如果属于，则反馈所述客户端的可信验证成功，判定所述客户端属于可信客户，如果不属于，则反馈所述客户端的可信验证失败，判定所述客户端属于待验证客户；如果所述T1与所述T2不相同，则在所述黑名单数据库中增加所述客户端的身份信息IM，并反馈所述客户端的可信验证失败，判定所述客户端属于黑名单用户。

[0019] 在上述技术方案的基础上，所述客户端是移动客户端。

[0020] 在上述技术方案的基础上，所述客户端的身份信息IM为移动手机号。

[0021] 在上述技术方案的基础上，所述客户端的身份信息IM为移动手机的国际移动设备身份码IMEI值。

[0022] 在上述技术方案的基础上，还包括第三验证模块，用于当所述客户端被判定为待验证客户，服务器则向服务器管理者发送所述客户端的身份验证信息，由所述管理者进一步确定验证结果，如果验证为可信客户，则所述白名单数据库增加所述客户端的身份信息，如果验证为不可信客户，则所述黑名单数据库增加所述客户段的身份信息。

【附图说明】

[0023] 此处所说明的附图是用来提供对本发明的进一步理解，构成本申请的一部分，但并不构成对本发明的不当限定，在附图中：

[0024] 图1是本发明提出的一种用于客户端和服务器之间的对所述客户端进行可信验证的方法的流程图。

【具体实施方式】

[0025] 下面将结合附图以及具体实施例来详细说明本发明，其中的示意性实施例以及说明仅用来解释本发明，但并不作为对本发明的不当限定。

[0026] 参见图1，为本发明提出的用于客户端和服务器之间的对所述客户端进行可信验证的方法的流程图，在S01中，客户端向服务器发送所述客户端的身份验证信息，所述身份验证信息包括所述客户端的身份信息IM和被验证的次数信息T1，其中，所述被验证的次数信息T记录所述客户端被验证的次数，其初始化值为0。

[0027] 在S02中，服务器查询查询所述客户端的身份信息IM是否属于黑名单数据库中的信息，如果属于则不再进行后续的步骤，退出所述验证过程，并反馈所述客户端的可信验证失败、判定所述客户端属于黑名单客户；如果不属于则继续下述步骤。通过黑名单机制，直接将不可信的客户端排除，并且，黑名单数据库中的信息是根据客户端的访问行为动态生成的(参见后续的步骤)，同时，服务器的管理者也定期对黑名单数据库进行调整和清理。

[0028] 在S03中，服务器在其关联的被验证次数信息数据库中查询与所述客户端的身份信息关联的被验证的次数信息T2，如果所述关联的被验证次数信息数据库中不存在所述客户端身份信息IM，则在所述关联的被验证次数信息数据库中创建新的条目记录所述客户端身份信息IM，且与该客户端身份信息关联的被验证次数信息T2的初始化值为0，并不再进行后续的步骤，退出所述验证过程，并反馈所述客户端的可信验证失败、判定所述客户端属于新客户。对于被验证次数信息数据库中不存在客户端身份信息IM，说明所述客户端是首次参与可信验证，则需要服务器管理者做进一步的判断。

[0029] 在S04中，如果所述T1与所述T2相同，则将所述T1和T2的值分别加1，分别更新所述客户端和所述服务器的被验证次数信息数据库中的对应信息；接着判断所述客户端身份信息IM是否属于白名单数据库中的信息，如果属于，则反馈所述客户端的可信验证成功，判定所述客户端属于可信客户，如果不属于，则反馈所述客户端的可信验证失败，判定所述客户端属于待验证客户；

[0030] 如果所述T1与所述T2不相同，则在所述黑名单数据库中增加所述客户端的身份信息IM，并反馈所述客户端的可信验证失败，判定所述客户端属于黑名单用户。通过该步骤中能够限制访问所述服务器的客户端具有唯一性，降低通过被复制了身份验证信息所带来的风险，为了便于理解，通过一个简单的例子说明，当第一客户端通过了所述服务器的可信验证，与所述第一客户端的身份验证信息都将被服务器的相关数据库(如：被验证次数信息数据库)记录，如果存在第二客户端通过复制第一客户端的身份信息进行了与所述服务器的可信验证，虽然有可能通过，但是，当当第一客户端再次进行可信验证时，由于第一客户端保存的身份验证信息中的被验证的次数信息则与服务器的被验证次数信息数据库对应的

次数信息则不能保持一致(这是由于第二客户端冒充第一客户端进行身份验证时,使被验证次数信息数据库对应的次数信息更新了,而第一客户端的被验证次数信息并没有更新)数据,这就说明第一客户端的身份验证信息存在被复制给其他客户端的情况,并被其他客户端进行了可信验证的行为,而这种行为是被禁止的,因此可通过黑名单的机制反馈与所述第一客户端具有相同身份信息的客户端为不可信任的客户端,从而强化了客户端可信验证的安全性。

[0031] 本领域普通技术人员可以理解上述实施例的全部或部分步骤可以使用计算机程序流程来实现,所述计算机程序可以存储于一计算机可读存储介质中,所述计算机程序在相应的硬件平台上(如系统、设备、装置、器件等)执行,在执行时,包括方法实施例的步骤之一或其组合。可选地,上述实施例的全部或部分步骤也可以使用集成电路来实现,这些步骤可以被分别制作成一个个集成电路模块,或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。上述实施例中的装置/功能模块/功能单元可以采用通用的计算装置来实现,它们可以集中在单个的计算装置上,也可以分布在多个计算装置所组成的网络上。上述实施例中的装置/功能模块/功能单元以软件功能模块的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。上述提到的计算机可读取存储介质可以是只读存储器,磁盘或光盘等。

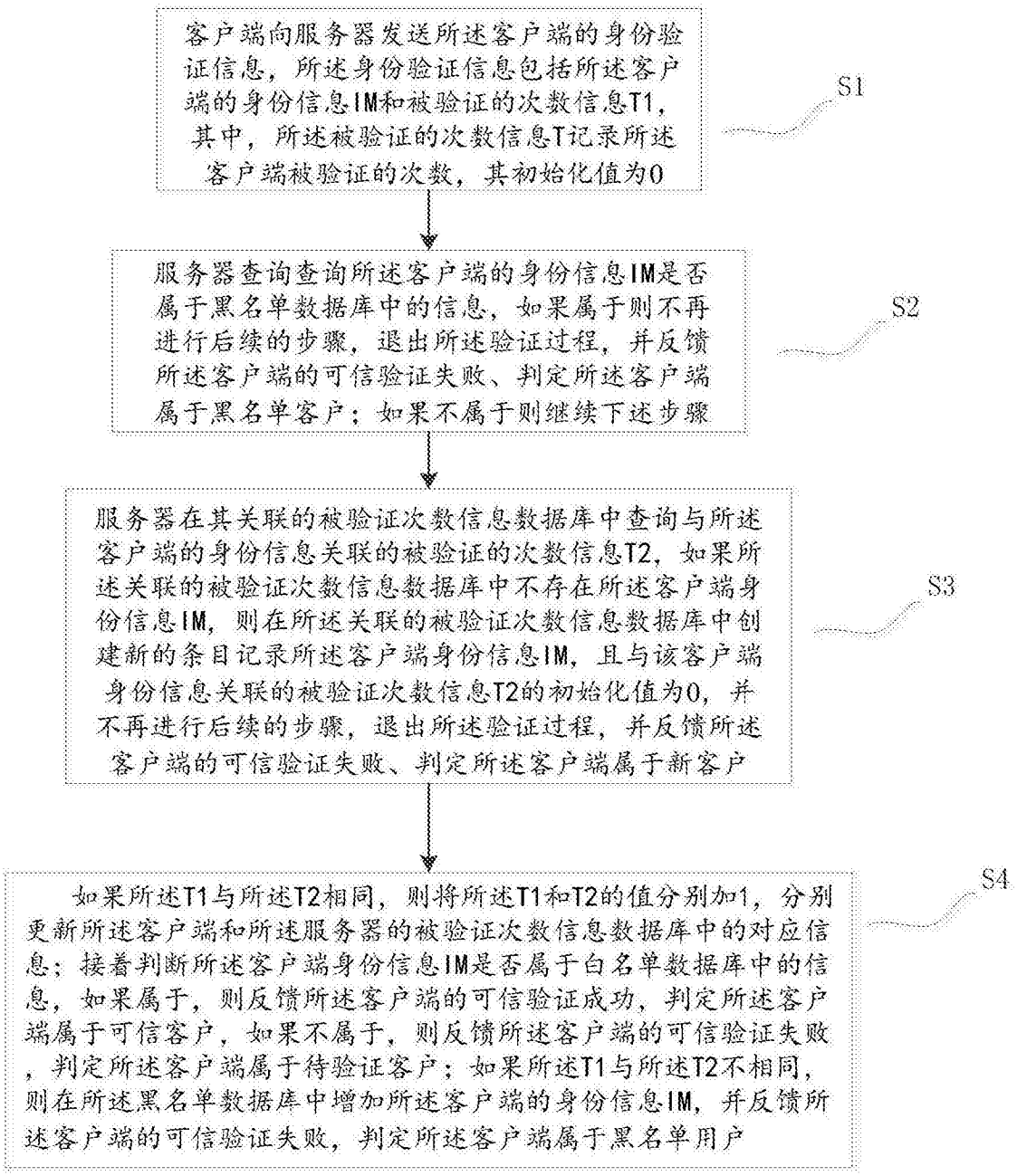

客户端向服务器发送所述客户端的身份验证信息，所述身份验证信息包括所述客户端的身份信息IM和被验证的次数信息T1，其中，所述被验证的次数信息T记录所述客户端被验证的次数，其初始化值为0
S1
服务器查询查询所述客户端的身份信息IM是否属于黑名单数据库中的信息，如果属于则不再进行后续的步骤，退出所述验证过程，并反馈所述客户端的可信验证失败、判定所述客户端属于黑名单客户；如果不属于则继续下述步骤
S2
服务器在其关联的被验证次数信息数据库中查询与所述客户端的身份信息关联的被验证的次数信息T2，如果所述关联的被验证次数信息数据库中不存在所述客户端身份信息IM，则在所述关联的被验证次数信息数据库中创建新的条目记录所述客户端身份信息IM，且与该客户端身份信息关联的被验证次数信息T2的初始化值为0，并不再进行后续的步骤，退出所述验证过程，并反馈所述客户端的可信验证失败、判定所述客户端属于新客户
S3
如果所述T1与所述T2相同，则将所述T1和T2的值分别加1，分别更新所述客户端和所述服务器的被验证次数信息数据库中的对应信息；接着判断所述客户端身份信息IM是否属于白名单数据库中的信息，如果属于，则反馈所述客户端的可信验证成功，判定所述客户端属于可信客户，如果不属于，则反馈所述客户端的可信验证失败，判定所述客户端属于待验证客户；如果所述T1与所述T2不相同，则在所述黑名单数据库中增加所述客户端的身份信息IM，并反馈所述客户端的可信验证失败，判定所述客户端属于黑名单用户
S4

图1