(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 101848084 A
(43)申请公布日 2010.09.29

(21)申请号 200910106099.2

(22)申请日 2009.03.25

(71)申请人 黄金富
地址 100032 北京市西城区金融街 27 号投资广场 B 座 19 层

(72)发明人 黄金富

(51)Int.Cl.
H04L 9/32(2006.01)
H04W 12/06(2009.01)

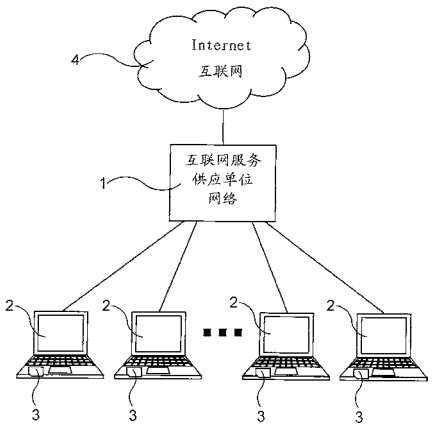
权利要求书 1 页 说明书 3 页 附图 1 页

(54)发明名称

用 SIM 卡认证用户电脑服务器 ISP 身份的方法和系统

(57)摘要

一种用 SIM 卡认证用户电脑服务器 ISP 身份的方法和系统，所述系统包括互联网服务供应单位的网络 (1)、接入该网络 (1) 的各终端 (2) 及设置于所述终端 (2) 内的 SIM 卡 (3)，终端 (2) 接入网络 (1) 时，由网络 (1) 对该接入的终端 (2) 内的 SIM 卡 (3) 进行身份鉴权认证，鉴权认证成功后网络 (1) 才允许该终端 (2) 接入。本发明是通过在计算机终端 (2) 上设置与移动电话相同的SIM卡，于计算机终端 (2) 接入网络 (1) 时，由网络 (1) 采用如移动电话网络认证接入手机的方法去认证计算机终端 (2)，由于 SIM 卡极难复制，每一 SIM 卡都可视为唯一的，可确保这些通过 SIM 卡认证的计算机终端 (2) 的身份不会被伪冒。



CN 101848084 A

1. 一种用 SIM 卡认证用户电脑服务器 ISP 身份的方法，用于认证用户电脑终端、服务器、互联网服务供应单位的身份，其特征在于，所述的方法包括在各终端 (2) 内设置用于认证身份的 SIM 卡 (3)，并在终端 (2) 接入互联网服务供应单位的网络 (1) 时，由网络 (1) 对该终端 (2) 内的 SIM 卡 (3) 进行身份鉴权认证，鉴权认证成功后网络 (1) 才允许该终端 (2) 接入，及允许该终端 (2) 通过网络 (1) 与其他接入的终端 (2) 交换信息。

2. 如权利要求 1 所述的用 SIM 卡认证用户电脑服务器 ISP 身份的方法，其特征在于，所述的身份鉴权认证包括如下步骤：

1. 终端 (2) 将 SIM 卡 (3) 卡号传送给网络 (1)，请求进行身份鉴权认证；

2. 网络 (1) 从该 SIM 卡 (3) 卡号找出密钥 Ki，然后网络 (1) 产生一个随机数 RNAD 传送给终端 (2) 内的 SIM 卡 (3)，以及，网络 (1) 将该随机数 RNAD 和密钥 Ki 通过 A3 算法运算生成出响应数 SRES；

3. SIM 卡 (3) 收到该随机数 RNAD 后，将该随机数 RNAD 和 SIM 卡 (3) 内的密钥 Ki 通过 A3 算法运算生成出响应数 SRES'，然后 SIM 卡 (3) 将该响应数 SRES'传送回网络 (1) 核对；

4. 网络 (1) 将接收到的响应数 SRES'与步骤 2 中的响应数 SRES 相核对，两者相同则鉴权认证成功，否则鉴权认证失败。

3. 如权利要求 2 所述的用 SIM 卡认证用户电脑服务器 ISP 身份的方法，其特征在于，所述的方法还包括终端 (2) 和网络 (1) 分别产生密钥 Kc 的步骤，是从该随机数 RNAD 和 SIM 卡 (3) 内的密钥 Ki 通过 A8 算法运算生成出密钥 Kc，密钥 Kc 是用于终端 (2) 接入网络 (1) 后，终端 (2) 与网络 (1) 之间交换的信息的加密解密用途。

4. 一种用 SIM 卡认证用户电脑服务器 ISP 身份的系统，用于认证用户电脑终端、服务器、互联网服务供应单位的身份，其特征在于，所述的系统包括互联网服务供应单位的网络 (1)、接入该网络 (1) 的各终端 (2) 及设置于所述终端 (2) 内的 SIM 卡 (3)，其中，所述的网络 (1) 及各终端 (2) 按预定程序运作，于终端 (2) 接入网络 (1) 时，由网络 (1) 对该接入的终端 (2) 内的 SIM 卡 (3) 进行身份鉴权认证，鉴权认证成功后网络 (1) 才允许该终端 (2) 接入，及允许该终端 (2) 通过网络 (1) 与其他已接入的终端 (2) 交换信息。

5. 如权利要求 4 所述的用 SIM 卡认证用户电脑服务器 ISP 身份的系统，其特征在于，所述的终端 (2) 包括接入该网络 (1) 的用户电脑、接入该网络 (1) 的服务器、与该网络 (1) 相连接的其他互联网服务供应单位的网络接口设备。

6. 如权利要求 4 所述的用 SIM 卡认证用户电脑服务器 ISP 身份的系统，其特征在于，所述的 SIM 卡 (3) 设置于终端 (2) 的网络卡上。

7. 如权利要求 4 所述的用 SIM 卡认证用户电脑服务器 ISP 身份的系统，其特征在于，所述的 SIM 卡 (3) 是移动电话网络所采用的 SIM 卡。

8. 如权利要求 4 所述的用 SIM 卡认证用户电脑服务器 ISP 身份的系统，其特征在于，所述的 SIM 卡 (3) 内设置有包括卡号、密钥 Ki、A3 算法、A8 算法。

用 SIM 卡认证用户电脑服务器 ISP 身份的方法和系统

【技术领域】

[0001] 本发明涉及计算机网络技术，特别是涉及一种用 SIM 卡认证用户电脑服务器 ISP 身份的方法和系统。

【背景技术】

[0002] 现时一般需要使用互联网的计算机，大部分是通过 ISP 即互联网服务供应单位提供的网络连接到互联网，接入网络的方法包括通过电话拨号、专线、ADSL 宽带、有线电视网络、光纤、无线 WIFI 等等上网，计算机接入网络时，互联网服务供应单位一般通过用户的登录名称和密码来认证用户的身份，通过认证就允许用户的计算机接入网络连接到互联网。这种采用登录名称和密码的认证方法，其他人只要取得用户的登录名称和密码，就可以使用其他的计算机假冒用户接入网络上网，继而在网络上进行一些违反互联网网络文化的行为，例如大量发送垃圾电邮、散播计算机病毒、入侵或攻击其他计算机等等，对其他互联网的使用者造成不便甚至损失。如何认证接入网络连线到互联网的计算机的身份不会被伪冒，是一个有待解决的问题。

【发明内容】

[0003] 本发明的目的，在于提供一种用 SIM 卡认证用户电脑服务器 ISP 身份的方法和系统，以实现认证接入网络连线到互联网的计算机身份的应用。

[0004] 本发明的用 SIM 卡认证用户电脑服务器 ISP 身份的方法和系统，是通过在计算机终端上设置一用于认证身份的 SIM 卡，这 SIM 卡可以采用与现时移动电话相同的 SIM 卡，于计算机终端接入网络时，由网络采用如移动电话网络认证接入手机的方法去认证计算机终端，由于 SIM 卡极难复制，每一 SIM 卡都可被视为唯一的，就可确认这些通过 SIM 卡认证的计算机终端的身份不会被伪冒。

[0005] 本发明的目的是这样实现的，采用这样一种用 SIM 卡认证用户电脑服务器 ISP 身份的系统，用于认证用户电脑终端、服务器、互联网服务供应单位的身份，其特征在于，所述的系统包括互联网服务供应单位的网络 (1)、接入该网络 (1) 的各终端 (2) 及设置于所述终端 (2) 内的 SIM 卡 (3)，其中，所述的网络 (1) 及各终端 (2) 按预定程序运作，于终端 (2) 接入网络 (1) 时，由网络 (1) 对该接入的终端 (2) 内的 SIM 卡 (3) 进行身份鉴权认证，鉴权认证成功后网络 (1) 才允许该终端 (2) 接入，及允许该终端 (2) 通过网络 (1) 与其他已接入的终端 (2) 交换信息。以及，所述的终端 (2) 包括接入该网络 (1) 的用户电脑、接入该网络 (1) 的服务器、与该网络 (1) 相连接的其他互联网服务供应单位的网络接口设备。

[0006] 以及，采用这样一种用 SIM 卡认证用户电脑服务器 ISP 身份的方法，采用如前面所述的用 SIM 卡认证用户电脑服务器 ISP 身份的系统，用于认证用户电脑终端、服务器、互联网服务供应单位的身份，其特征在于，所述的方法包括在各终端 (2) 内设置用于认证身份的 SIM 卡 (3)，并在终端 (2) 接入互联网服务供应单位的网络 (1) 时，由网络 (1) 对该终端 (2) 内的 SIM 卡 (3) 进行身份鉴权认证，鉴权认证成功后网络 (1) 才允许该终端 (2) 接入，

及允许该终端 (2) 通过网络 (1) 与其他接入的终端 (2) 交换信息。

[0007] 这样就实现了本发明的目的。

[0008] 本发明的优点是计算机终端 (2) 接入互联网服务供应单位的网络 (1) 时,无需使用登录名称和密码,也就无需用户在键盘上输入登录名称和密码的步骤,只要在计算机终端 (2) 插入 SIM 卡 (3),接入的过程就可以由终端 (2) 与互联网服务供应单位自动完成,方便快捷。

【附图说明】

[0009] 图 1 是本发明的第一实施例的系统结构示意说明图 ;

[0010] 图 2 是本发明的第二实施例的系统结构示意说明图。

[0011] 图中,相同的数字代表相同的系统、装置、部件器件,附图是示意性的,用以说明本发明的系统的构成和主要特征。

【具体实施方式】

[0012] 下面结合附图,对本发明的方法作进一步详细说明。

[0013] 参阅图 1,图 1 是本发明的第一实施例的系统结构示意说明图,图 1 中示出的系统包括互联网服务供应单位的网络 (1)、接入该网络 (1) 的各终端 (2) 及设置于所述终端 (2) 内的 SIM 卡 (3),其中,所述的网络 (1) 及各终端 (2) 按预定程序运作,于终端 (2) 接入网络 (1) 时,由网络 (1) 对该接入的终端 (2) 内的 SIM 卡 (3) 进行身份鉴权认证,鉴权认证成功后网络 (1) 才允许该终端 (2) 接入,及允许该终端 (2) 通过网络 (1) 与其他已接入的终端 (2) 交换信息。其中,所述的终端 (2) 包括接入该网络 (1) 的用户电脑、接入该网络 (1) 的服务器、与该网络 (1) 相连接的其他互联网服务供应单位的网络接口设备。

[0014] 在设置方面,互联网服务供应单位要向各用户发行用于认证用户身份的 SIM 卡 (3),这 SIM 卡 (3) 可以是移动电话网络所采用的 SIM 卡,SIM 卡 (3) 内设置有包括卡号、密钥 Ki、A3 算法、A8 算法,互联网服务供应单位同时保存所有这些 SIM 卡 (3) 的卡号、密钥 Ki、A3 算法、A8 算法等资料,并设置认证用户 SIM 卡 (3) 的程序软件。在用户方面,在用户的计算机终端 (2) 内设置有用于与网络 (1) 相网络连接的网络卡,计算机终端 (2) 内还要设置 SIM 卡读卡器,SIM 卡读卡器最理想是设置在计算机终端 (2) 内的网络卡上,这样就可将 SIM 卡 (3) 设置于终端 (2) 的网络卡上。计算机终端 (2) 还要设置有认证 SIM 卡 (3) 的程序软件,用户使用计算机终端 (2) 接入互联网服务供应单位的网络 (1) 时,要预先将 SIM 卡 (3) 放入 SIM 卡读卡器内,然后才能接入网络 (1) 连线到互联网 (4)。

[0015] 在本说明书中,所述的终端 (2) 接入网络 (1) 时,可以通过有线或无线方式接入,其中,通过有线方式接入包括使用电话拨号、专线、ADSL 宽带、有线电视网络、光纤等接入网络 (1),而通过无线方式接入包括使用 WiFi、WiMax、蓝芽、GPRS、移动电话等等各种无线通讯方式接入网络 (1),无论终端 (2) 采用有线或无线方式接入网络 (1),都可很好地实现本发明的目的,都是属于本发明的保护范围。

[0016] 继续参阅图 1,图 1 中示出的系统所采用认证终端 (2) 的方法包括在各终端 (2) 内设置用于认证身份的 SIM 卡 (3),并在终端 (2) 接入互联网服务供应单位的网络 (1) 时,由网络 (1) 对该终端 (2) 内的 SIM 卡 (3) 进行身份鉴权认证,鉴权认证成功后网络 (1) 才允

许该终端 (2) 接入，及允许该终端 (2) 通过网络 (1) 与其他接入的终端 (2) 交换信息。其中，所述的身份鉴权认证包括如下步骤：

[0017] 1. 终端 (2) 将 SIM 卡 (3) 卡号传送给网络 (1)，请求进行身份鉴权认证；

[0018] 2. 网络 (1) 从该 SIM 卡 (3) 卡号找出密钥 Ki，然后网络 (1) 产生一个随机数 RNAD 传送给终端 (2) 内的 SIM 卡 (3)，以及，网络 (1) 将该随机数 RNAD 和密钥 Ki 通过 A3 算法运算生成出响应数 SRES；

[0019] 3.SIM 卡 (3) 收到该随机数 RNAD 后，将该随机数 RNAD 和 SIM 卡 (3) 内的密钥 Ki 通过 A3 算法运算生成出响应数 SRES'，然后 SIM 卡 (3) 将该响应数 SRES' 传送回网络 (1) 核对；

[0020] 4. 网络 (1) 将接收到的响应数 SRES' 与步骤 2 中的响应数 SRES 相核对，两者相同则鉴权认证成功，否则鉴权认证失败。

[0021] 本发明的系统除了提供身份认证功能外，还可以向网络 (1) 与终端 (2) 之间传送的信息提供加密功能，是在所述的身份鉴权认步骤中，还包括终端 (2) 和网络 (1) 分别产生密钥 Kc 的步骤，是从该随机数 RNAD 和 SIM 卡 (3) 内的密钥 Ki 通过 A8 算法运算生成出密钥 Kc，密钥 Kc 是用于终端 (2) 接入网络 (1) 后，终端 (2) 与网络 (1) 之间交换的信息的加密解密用途。包括终端 (2) 使用该密钥 Kc 将发送的信息加密后才传送到网络 (1)，由网络 (1) 使用密钥 Kc 将该加密后信息解密，然后才将信息转送到目的地，以及网络 (1) 使用该密钥 Kc 将传送给终端 (2) 的信息加密后才传送到终端 (2)，由终端 (2) 使用密钥 Kc 将该加密后信息解密得出原来信息。这样可保护终端 (2) 与网络 (1) 之间的信息不会被人盗取，特别适合于一些安全性要求韵的应用，如网上银行服务等。

[0022] 参阅图 2，图 2 是本发明的第二实施例的系统结构示意说明图，第二实施例中，各个网络 (1) 除了与其客户的计算机终端 (2) 相连线外，还连接其他的网络 (1)，其中，网络 (1) 是通过终端 (2) 上的 SIM 卡 (3) 来认证终端 (2) 的身份，而网络 (1) 与网络 (1) 之间，也同样采用 SIM 卡 (3) 来认证其他互联网服务供应单位的网络 (1) 的身份，只要在两个相连接的网络 (1) 的其中一方的网络连接端，设置另一方所发行的 SIM 卡 (3)，采用如前面互联网服务供应单位认证其用户身份同样的方法，就可以实现互联网服务供应单位身份的认证。

[0023] 以上已经详细说明了本发明的系统和方法，虽然本发明以上述的实施例加以说明，但是本发明并不仅限于此，在不离开本发明的精神和所附权利要求书的范围的情况下，可以作多种改变和变化。

[0024] 通过本发明的用 SIM 卡认证用户电脑服务器 ISP 身份的方法和系统，互联网服务供应单位不单可以认证接入其网络 (1) 的终端 (2) 的身份，还可认证与该网络 (1) 连接的互联网服务供应单位的身份，只要各互联网服务供应单位都采用本发明的系统和方法，互联网 (4) 上的所有终端 (2) 包括用户上网的计算机、网站服务器、互联网服务供应单位等，都是经过身份认证的，如果有人通过互联网 (4) 发放不良信息、垃圾电邮、计算机病毒等，就可以通过互联网服务供应单位追踪到是谁发放信息的，从而阻止这些信息继续发放。本发明的实施，可改善目前互联网 (4) 的安全。

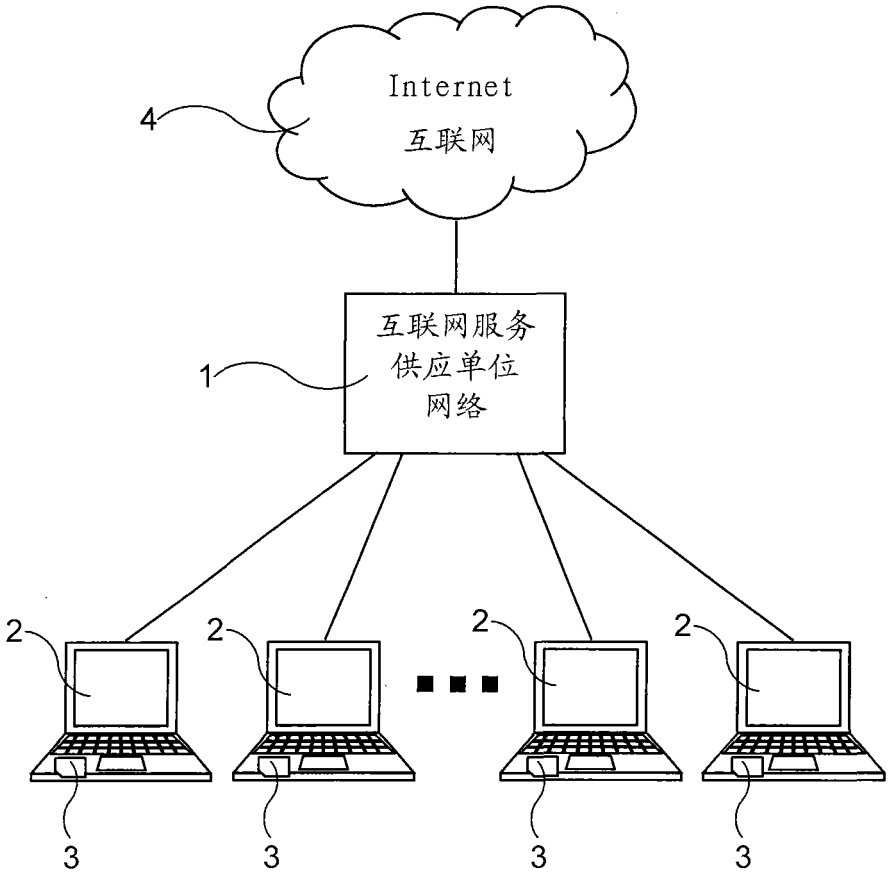


图 1

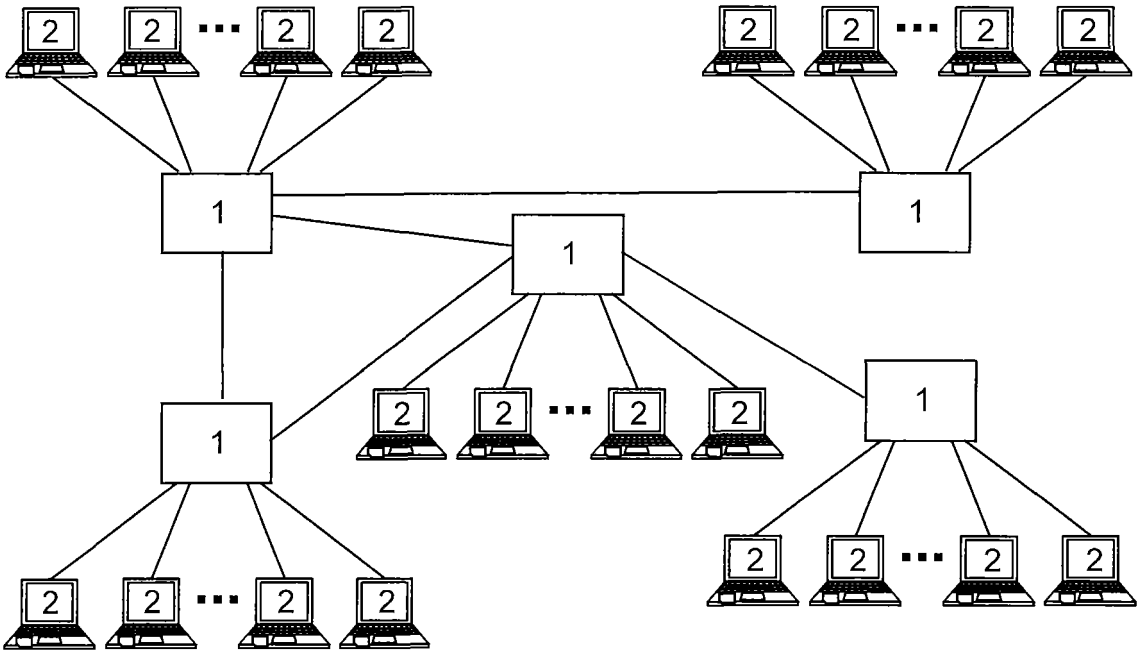


图 2