



(12) 发明专利

(10) 授权公告号 CN 1829150 B

(45) 授权公告日 2011.06.01

(21) 申请号 200610072747.3

CN 1444386 A, 2003.09.24, 摘要、权利要求

(22) 申请日 2006.04.10

1-4.

(73) 专利权人 北京易恒信认证科技有限公司

审查员 白雪慧

地址 100011 北京市石景山区石景山路 40
号信安大厦三层 E-G 区

(72) 发明人 南相浩 赵建国

(74) 专利代理机构 北京瑞盟知识产权代理有限
公司 11300

代理人 孙民兴

(51) Int. Cl.

H04L 9/32(2006.01)

H04L 9/30(2006.01)

H04L 29/06(2006.01)

(56) 对比文件

CN 1633071 A, 2005.06.29, 摘要、说明书第
3 页第 19 行 - 第 10 页.

US 6986460 B2, 2006.01.17, 全文.

WO 02/15523 A1, 2002.02.21, 全文.

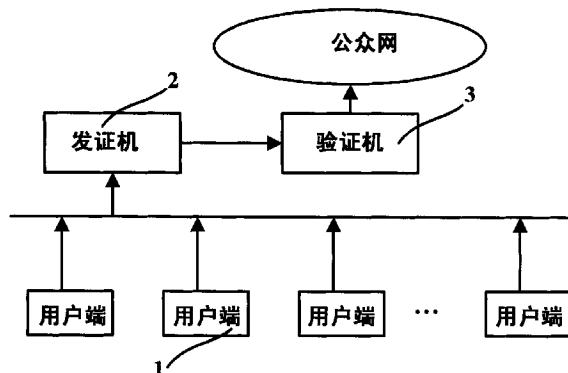
权利要求书 1 页 说明书 5 页 附图 1 页

(54) 发明名称

一种基于 CPK 的网关认证装置及方法

(57) 摘要

本发明公开了一种基于 CPK 的网关认证装
置及方法,包括用户端 (1)、发证机 (2) 和验证机
(3);所述用户端 (1),用于认证系统做好文件,并
将文件和申请书一并发送到发证机 (2);所述发
证机 (2),用于验证用户和文件的合法性,并根据
其合法性决定是否发给网关证;验证机 (3),检查
网关证的合法性,控制文件进出;本发明还提供
了一种基于 CPK 的网关认证方法,本发明实现了
大规模的公众网网关之间多个用户终端通过网络
获得独立可信认证。



1. 一种基于 CPK 组合公钥算法的网关认证装置,其特征在于,包括用户端(1)、发证机(2)和验证机(3);

所述用户端(1),包括 CPK 的 ID 证书和公钥矩阵,用于认证系统做好文件,并将文件和申请书一并发送到发证机(2),所述申请书包括发送文件的完整性码 MAC1 和发送用户对 MAC1 的签名;

所述发证机(2),包括 CPK 的 ID 证书和公钥矩阵,用于验证文件的完整性码 MAC1 和发送用户对 MAC1 的签名,以验证用户和文件的合法性,并根据其合法性决定是否给该文件发给网关证,所述网关证包括网关对文件中特定位的抽样完整性码 MAC2 的签名;

验证机(3),包括公钥矩阵,用于验证文件中特定位的抽样完整性码 MAC2 及网关对文件中特定位的抽样完整性码 MAC2 的签名,控制文件进出网关。

2. 一种基于 CPK 组合公钥算法的网关认证方法,其特征在于,包括下列步骤:

步骤 1) 用户端包括 CPK 的 ID 证书和公钥矩阵,用于认证系统做好文件,并将文件和申请书一并发送到发证机;所述申请书包括发送文件的完整性码 MAC1 和发送用户对 MAC1 的签名;

步骤 2) 发证机包括 CPK 的 ID 证书和公钥矩阵,用于验证文件的完整性码 MAC1 和发送用户对 MAC1 的签名,以验证用户和文件的合法性,并根据其合法性决定是否发给网关证;所述网关证包括网关对文件中特定位的抽样完整性码 MAC2 的签名;

步骤 3) 验证机,包括公钥矩阵,用于检查文件中特定位的抽样完整性码 MAC2 及网关对文件中特定位的抽样完整性码 MAC2 的签名,以控制文件进出网关。

3. 根据权利要求 2 所述的网关认证方法,其特征在于,所述步骤 2) 包括下列步骤:

如果发证机验证用户和文件合法,则发放网关证;否则,将不给该文件发放网关证。

4. 根据权利要求 3 所述的网关认证方法,其特征在于,所述步骤 3) 包括下列步骤:

对出关文件来说,具有合法网关证,就允许出关,如果没有网关证,这个文件就不能出关。

5. 根据权利要求 4 所述的网关认证方法,其特征在于,所述步骤 3) 还包括下列步骤:对进关文件来说,如果带有合法网关证,就允许正常进关,而没带网关证,则存储在备用服务器中,等待进一步处理。

一种基于 CPK 的网关认证装置及方法

技术领域

[0001] 本发明涉及网络安全认证技术领域,特别是涉及一种基于 CPK 的网关认证装置及方法。

背景技术

[0002] 20世纪90年代中期,随着互联网的引进,外国的防火墙技术也开始流入中国。当时中国就提出在防火墙的基础上,构建进出都能控制的保密网关的设想,并为保密系统研制出我国第一代保密网关。但是在防火墙产生的网关证与终端所产生的文件捆绑技术和规范化认证技术上碰到难点,一直搁置下来。这个问题已经成为防火墙保密网关中的瓶颈问题,成为着保密网关在实际中能否投入应用的关键问题。但是,很遗憾的是,直到目前业界还没有可行的理想产品。

[0003] 同时,随着网络技术的发展,网络安全认证正从专用信息网的被动防御为主过渡到以公众网(如国际互联网 Internet)的主动管理为主的网络世界安全的新时代。与专用信息网比较起来,公众网的特点是规模大,用户终端多,高达几千万级,甚至千亿级,地域广,遍布世界每个角落。

[0004] 一般地,随着公众网使用人员的增加,良莠不齐的网络资源也逐渐进入公众网络中,病毒、木马、恶意代码如 ROOTKIT 等常常出现在公众用户所使用的网络资源中,甚至干扰用户使用,成为用户是否使用网络资源的主要原因。

[0005] 公众网对网络的基本安全是网络的可信性,终端在使用网络资源的过程中,如何对网络资源的来源可信性认证,是公众是否使用网络的首要关心的问题。

[0006] 现有的网络安全认证可分为两类,即对称密钥技术和非对称密钥技术,其中,非对称密钥技术由于可以避免通过网络传递解密密钥即私钥而在网络安全认证中得到越来越广泛的应用。

[0007] 非对称密钥中较为常用的安全认证技术是公钥基础设施(Public Key Infrastructure, PKI)。公钥体制是目前应用最广泛的一种加密体制,在这一体制中,加密密钥与解密密钥各不相同,发送信息的人利用接收者的公钥发送加密信息,接收者再利用自己专有的私钥进行解密。这种方式既保证了信息的机密性,又能保证信息具有不可抵赖性。目前,公钥体制广泛地用于 CA 认证、数字签名和密钥交换等领域。公钥基础设施(PKI)是信息安全基础设施的一个重要组成部分,是一种普遍适用的网络安全基础设施。PKI 是 20 世纪 80 年代由美国学者提出来了的概念,实际上,授权管理基础设施、可信时间戳服务系统、安全保密管理系统、统一的安全电子政务平台等的构筑都离不开它的支持。数字证书认证中心 CA、审核注册中心 RA(Registration Authority)、密钥管理中心 KM(Key Manager) 都是组成 PKI 的关键组件。

[0008] 另一种较为具有应用前景的网络安全认证技术是基于标识的密码技术(Identity-Based Encryption, IBE),在IBE系统中,每个实体同样具有一个标识。该标识可以是任何有意义的字符串。但和传统公钥系统最大的不同是,在IBE系统中,实体的标识本

身就是实体的公开密钥。例如，可以用 Email 地址、姓名、职位、时间等甚至它们的组合作为实体的标识和公钥。该系统极大的方便了公开密码的管理。例如，发送方想发送一封 Email 到 mike@network. com，他可以直接使用该 Email 地址作为接收方的公钥进行加密。甚至，一方可以发信的同时指定接收方只能在特定的时间才能解密。

[0009] 但是，现有的这些非对称网络安全认证加密技术都需要维护具有大量数据的数据库存储，占用大量的存储空间，运行时的效率不高，处理速度很慢，无法在公众网络网关这样的网络设备中使用。

发明内容

[0010] 本发明的目的在于克服上述缺陷而提供的一种基于 CPK 的网关认证装置及方法，其实现大规模的公众网网关之间多个用户终端通过网络获得独立可信认证。

[0011] 为实现本发明目的而提供的一种基于 CPK 的网关认证装置，包括用户端、发证机和验证机；

[0012] 所述用户端，用于认证系统做好文件，并将文件和申请书一并发送到发证机；

[0013] 所述发证机，用于验证用户和文件的合法性，并根据其合法性决定是否发给网关证；

[0014] 验证机，检查网关证的合法性，控制文件进出。

[0015] 所述用户端包括 CPK 的 ID 证书和公钥矩阵。

[0016] 所述申请书的内容包括发送文件的完整性码和发送用户的签名。

[0017] 所述发证机包括包括 CPK 的 ID 证书和公钥矩阵。

[0018] 所述发证机包括网关证，用于检查用户是否合法用户和用户对文件的责任性，并根据检查结果判断是否发给网关证。

[0019] 为实现本发明目的又提供了一种基于 CPK 的网关认证方法，包括下列步骤：

[0020] 步骤 1) 用户端认证系统做好文件，并将文件和申请书一并发送到发证机；

[0021] 步骤 2) 发证机验证用户和文件的合法性，并根据其合法性决定是否发给网关证；

[0022] 步骤 3) 验证机检查网关证的合法性，并控制进出文件。

[0023] 所述步骤 2) 可以包括下列步骤：

[0024] 如果发证机验证用户和文件合法，则发放网关证；否则，将不给该文件发放网关证。

[0025] 所述网关证包括包括网关抽样完整性码的签名。

[0026] 所述步骤 3) 可以包括下列步骤：

[0027] 对出关文件来说，具有合法网关证，就允许出关，如果没有网关证，这个文件就不能出关。

[0028] 所述步骤 3) 还可以包括下列步骤：

[0029] 对进口文件来说，如果带有合法网关证，就允许正常进关，而没有网关证，则存储在备用服务器中，等待进一步处理。

[0030] 本发明的有益效果是：基于 CPK 的网关认证装置及方法，为实现规模化的网间可信创造了可行的技术方法，在公众网络中，在内部网与公众网之间设置网关，以认证技术和验证技术在各内部网或者企业网之间实现可信连接，可以在数千万各内部网之间实现任何

网关对任何网关之间的认证,构建网络间可信连接的基础设施 - 网关。本发明的基于 CPK 的网关认证方法,不需要维护具有大量数据的数据库存在,而且只有一些公用参数占用小量的存储空间,由于以标识生成私钥,并将公钥公开,因此其运行时的效率很高,处理速度很快,在公众网络网关这样的网络设备中可以得到广泛使用。其在可信网络世界的建设中,将同可信计算、可行应用一起组成网络技术影响全局发展的基础技术。

附图说明

- [0031] 图 1 为本发明的网关认证发送过程示意图 ;
[0032] 图 2 为本发明的网关认证接受过程示意图。

具体实施方式

[0033] 下面结合附图 1 和 2 进一步详细说明本发明的一种基于 CPK 的网关认证装置及方法。

[0034] 组合公钥算法 (Combined Public Key,CPK) 是基于标识的公钥算法,其密钥管理中心生成生成彼此对应的私钥计算参数 (私钥计算基) 和公钥计算参数 (公钥计算基); 根据第一用户提供的标识,利用所述私钥计算参数计算第一用户的私钥,并将所产生的私钥提供给第一用户; 以及公布所述公钥计算参数,以使得第二用户在获得第一用户的标识后,可根据第一用户的标识,利用所述的公钥计算参数,计算第一用户的公钥。

[0035] 网关 (Gateway) 又称网间连接器、协议转换器。网关在传输层上以实现网络互连,是最复杂的网络互连设备,仅用于两个高层协议不同的网络互连。网关的结构也和路由器类似,不同的是互连层。网关既可以用于广域网互连,也可以用于局域网互连。

[0036] 本发明实施例中的基于 CPK 的网关认证装置,由用户端 1 、发证机 2 和验证机 3 构成。

[0037] 用户端 1 :具有 CPK 的 ID 证书和公钥矩阵,本发明中的具有 CPK 的 ID 证书和公钥矩阵的产生,在申请人的中国发明专利申请 2005100021564 基于标识的密钥产生装置及方法中具体实施方式所述,在本发明中全文引用。 ID 证书提供认证所需所有参数和协议,公钥矩阵能计算任何实体的公钥。设 : 内部网 A 的用户 Y1 给内部网 B 的用户 Y2 发送文件 X 。用户端 1 用于定义的认证系统 (如 CPK_email 认证系统) 做好文件,并将文件和申请书一并发送到发证机 2 。申请书的格式可以自行定义,因为申请书只在本内部网发证机 2 和各个用户之间起作用,只要本内部网的发证机 2 认可就行。申请书的内容包括发送文件 X 的完整性码 MAC1 和发送用户的签名 :SIG_{Y1}(MAC1), 以确认用户 Y1 的合法性,并确认文件 X 是用户 Y1 的所为。

[0038] 发证机 2 :具有 CPK 的 ID 证书和公钥矩阵,用于验证用户 Y1 和文件 X 的合法性。各内部网可能有不同的安全策略,对保密系统而言,可能发生保密系统和保密系统相连接,发送等级秘密文件的情况,也可能发生保密系统和非保密系统连接的情况,因此,各内部网需要制定满足不同需求的合理的安全策略。各内部网的安全策略可能不相同,但其共同的基本要求是必须检查用户是否合法用户和用户对文件的责任性 (对文件 X 的完整性码 MAC1 和网关 A 的数字签名) 。如该文件是否用户权限范围,该加密的文件是否加了密等。如果不符合条件,则不给该文件发放网关证。因为网关证将在全网范围起作用,因此网关证必须标

准化。网关证的核心内容只有一项 : $SIG_A(MAC2)$;

[0039] MAC2 是文件 X 中特定位的抽样完整性码。抽样位由文件长度给出。设文件长度为 n, 第一个抽样位为 $n^*(1/3)$, 抽取一分组长度码, 第二抽样位位 $n^*(2/3)$, 再抽取一分组长度码, MAC2 是这两组 HASH 函数 (完整性码)。MAC2 为网关证和数据的一体性提供证明。

[0040] 本发明的网关证的标准化设计, 网关证在全网互认, 且提供文件和该网关证的一体性、该内部网关的合法性、该网关对文件的责任性等证明。

[0041] 验证机 3 :可以在目前的防火墙上实现, 只配置公钥矩阵, 不配置私钥, 用于检查来自任何网关的网关证。验证机 3 主要任务是检查网关证的合法性, 并控制进出文件。对出关文件来说, 具有合法网关证, 就允许出关, 如果没有网关证, 这个文件就不能出关。就进口文件来说, 如果带有合法网关证, 就允许正常进关, 而没有网关证, 则存储在备用服务器中, 等待进一步处理。为了提高验证机 3 的处理效率, 验证机 3 只检查抽样完整性码 MAC2 和网关的数字签名。

[0042] 本发明的验证机 3 适应各种不同安全策略, 处理好各种关系, 不影响现有系统的秩序, 适用于 : 有认证网关的内部网到有认证网关的内部网; 有认证网关的内部网到没有认证网关的内部网或单机; 单机到有认证网关; 单机分配备 CPK 认证系统和没有配备 CPK 认证系统两种情况。

[0043] 下面详细描述本发明的基于 CPK 的网关认证方法, 其包括下列步骤 :

[0044] 步骤 1) 用户端 1 认证系统做好文件, 并将文件和申请书一并发送到发证机 2;

[0045] 用户端 1 具有 CPK 的 ID 证书和公钥矩阵, ID 证书提供认证所需所有参数和协议, 公钥矩阵能计算任何实体的公钥。用户端 1 认证系统 (如 CPK_email 认证系统) 做好文件, 并将文件和申请书一并发送到发证机 2。申请书的格式可以自行定义, 因为申请书只在本内部网发证机 2 和各个用户之间起作用, 只要本内部网的发证机 2 认可就行。申请书的内容包括发送文件 X 的完整性码 MAC1 和发送用户的签名 : $SIG_{Y1}(MAC1)$, 以确认用户 Y1 的合法性, 并确认文件 X 是用户 Y1 的所为。

[0046] 步骤 2) 发证机 2 验证用户和文件的合法性, 并根据其合法性决定是否发给网关证;

[0047] 发证机 2 具有 CPK 的 ID 证书和公钥矩阵, 验证用户 Y1 和文件 X 的合法性。发证机 2 检查用户是否合法用户和用户对文件的责任性 (对文件 X 的完整性码 MAC1 和网关 A 的数字签名)。如该文件是否用户权限范围, 该加密的文件是否加了密等 1。如果不符条件, 则不给该文件发放网关证。网关证的核心内容只有一项 : $SIG_A(MAC2)$;

[0048] MAC2 是文件 X 中特定位的抽样完整性码。抽样位由文件长度给出。设文件长度为 n, 第一个抽样位为 $n^*(1/3)$, 抽取一分组长度码, 第二抽样位位 $n^*(2/3)$, 再抽取一分组长度码, MAC2 是这两组 HASH 函数 (完整性码)。MAC2 为网关证和数据的一体性提供证明。

[0049] 如果发证机 2 验证用户和文件合法, 则发放网关证; 否则, 将不给该文件发放网关证。

[0050] 步骤 3) 验证机 3 检查网关证的合法性, 并控制进出文件。

[0051] 在本实施例中验证机 3 是在防火墙上实现, 只配置公钥矩阵, 不配置私钥, 其检查来自任何网关的网关证。验证机 3 检查网关证的合法性, 并控制进出文件。对出关文件来说, 具有合法网关证, 就允许出关, 如果没有网关证, 这个文件就不能出关。就进口文件来

说,如果带有合法网关证,就允许正常进关,而没有网关证,则存储在备用服务器中,等待进一步处理。为了提高验证机3的处理效率,验证机3只检查抽样完整性码MAC2和网关的数字签名。

[0052] 本实施例是使本领域普通技术人员理解本发明,而对本发明所进行的详细描述,但可以想到,在不脱离本发明的权利要求所涵盖的范围内还可以做出其它的变化和修改,这些变化和修改均在本发明的保护范围内。

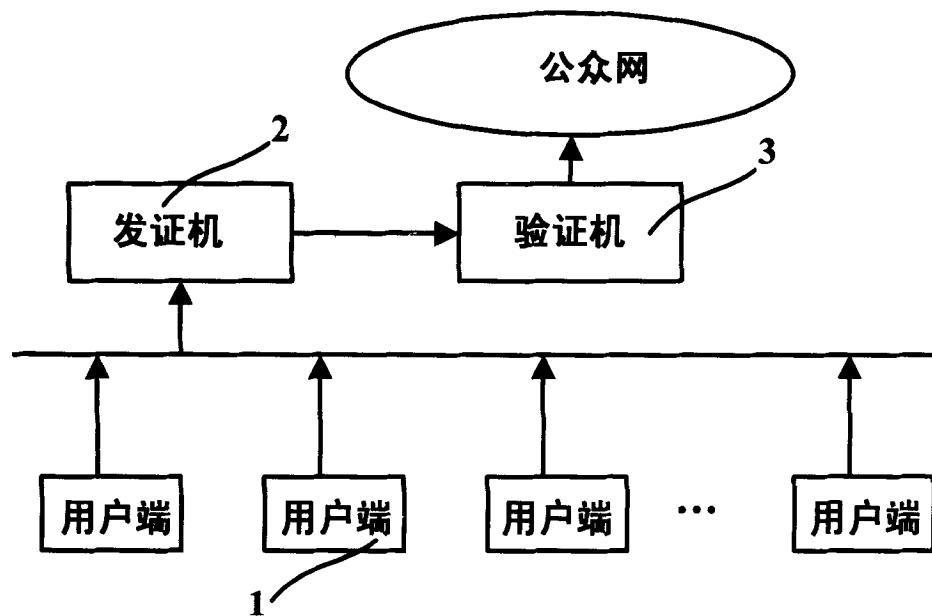


图 1

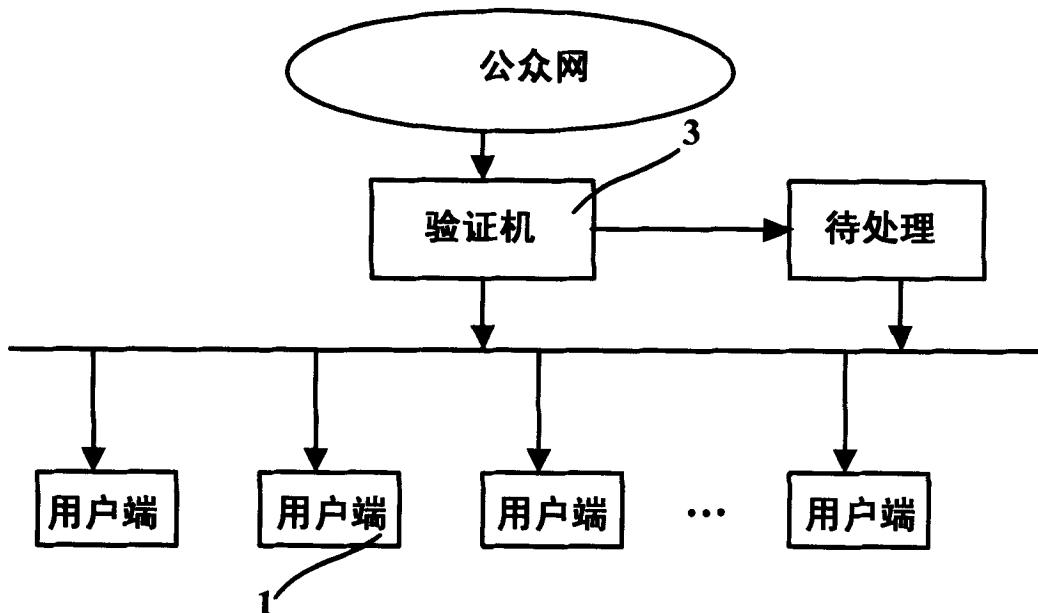


图 2