文章编号:1674-2869(2012)11-0065-03

结合公钥密码的密钥协商协议

蔡 琼,方 旋,方 兰
(武汉工程大学计算机科学与工程学院,湖北 武汉 430074)

摘 要:针对目前公钥密码体制的计算代价大,并且需要一个可信的数字证书认证机构才能保证密码体制的安全性,同时证书的维护也是安全方面的隐患等问题,提出一种结合动态公钥密码的密钥协商协议.在认证阶段,将生成的随机数同双方事先约定好的信息串接起来计算其哈希值,把此哈希值和随机数一同发送给对方,哈希函数的单向性使得该随机数能够被正确地传输.在加解密阶段,通过结合对方传输过来的随机数来动态改变公钥算法的密钥对,以实现通信过程中的一次一密.相比传统的通过重新生成大素数来改变密钥对的方法提高了效率,最后通过三种最常用的网络攻击手段验证了协议的安全性.

关键词:公钥密码;密钥协商协议;一次一密
中图分类号:TN118.1　　**文献标识码**:A　　**doi**:10.3969/j.issn.1674-2869.2012.11.014

0 引 言

密钥协商协议分为两种模式:证书型和无证书型.证书型是指在会话密钥的产生过程中,由一个可信的证书中心(CA)给参与密钥协商的各方各分发一个证书,此证书中含有此方的公钥,ID 及其他信息.证书型密钥协商协议的优点是提供认证,其中 PKI(公钥密码体制)广泛部署比较成熟,应用面广,并且由它管理密钥对有利于证书的统一管理,其缺点是计算代价大,需要一个可信的 CA,同时证书还需要维护.无证书型是指各方在进行会话密钥的协商过程中不需要证书的参与,优点是不需要 CA 的参与,减少了计算量,尤其是在低耗环境下应用的更多,同时安全性也不比证书型弱.本文提出的协议属于后者,通信双方不需要第三方的认证,由于每次通信中所用的密钥对都是动态生成的,不存在对密钥的更新、撤销等管理问题[1].由于公钥密码算法比对称密码算法的速率慢很多,主要原因是涉及大量复杂的运算,像 PKI 体制中用到的 RSA 算法要生成大素数、素性检测、指数模运算都是影响运算速率的因素,要生成新的密钥对比较费时,但长时间不更新密钥对又会有安全隐患[2],本文结合认证阶段生成的随机数来更新密钥对,未涉及到生成大素数和素性检测运算,速率较快、安全性高.

1 RSA 算法描述

密钥生成:

(1) 生成两个大素数 p 和 q.

(2) 求得 $n=pq$,$\phi(n)=(p-1)(q-1)$.

(3) 选择一个随机数 e,e 介于 1 和 $\phi(n)$ 之间,并且使得 $\gcd(e,\phi(n))=1$.

(4) 计算 $d\equiv e^{-1} \bmod \phi(n)$,即 d 为 e 在模 $\phi(n)$ 下的乘法逆元.

(5) 公钥为 (n,e),私钥为 d[3].

加密方式为 $c\equiv m^e \bmod n$,m 为明文,c 为密文.

解密方式为 $m\equiv c^d \bmod n$.

2 协议说明

假设 A 为用户,B 为服务器,A 的用户名表示为 ID_A,密码为 PW_A,函数 $H()$ 为一种 Hash 函数.可用文献[4]中改进的算法代替.A、B 之间事先共享了 ID_A 和 $h_{pw}=H(ID_A,PW_A)$,并选定了 RSA 算法的一对密钥对 (n,e) 和 d.A 保存一个数 s_a,B 保存一个数 s_b,保证 $s_a+s_b=n$.

2.1 认证及密钥交换阶段

(1) 用户 A 首先生成两个随机数 x_a 和 r_a,计算 $H(h_{pw})\oplus x_a$ 和 $H(h_{pw},r_a)$,其中⊕表示异或操作,$H(h_{pw},r_a)$ 表示将 h_{pw} 和 r_a 合并后计算其 Hash 值,之后 A 将 AU=$\{ID_A,H(h_{pw})\oplus x_a,r_a,H(h_{pw},r_a)\}$发送给 B.

(2) B 首先在数据库中搜寻是否有 ID_A,若无,则放弃通信,若有,则取出 r_a,将其和 ID_A 对应的 h_{pw} 合并后计算 $H'(h_{pw},r_a)$,若 $H'(h_{pw},r_a)\neq H(h_{pw},r_a)$,则放弃通信,若相等,则保留 r_a,并计算

收稿日期:2012-09-18
作者简介:蔡 琼(1961-),女,湖北武汉人,副教授,硕士.研究方向:网络数据库及数据挖掘.

$H(h_{pw})$，将其与接受到的 AU 的第二部分 $H(h_{pw})\oplus x_a$ 作一次异或运算，得到 x_a，然后 B 生成两个随机数 x_b 和 r_b，并计算 $H(h_{pw}\oplus x_a)$，$H(h_{pw},r_a,r_b)$，$H(h_{pw},r_b)\oplus x_b$，将 $BU=\{H(h_{pw}\oplus x_a),H(h_{pw},r_a,r_b)r_b,H(h_{pw},_{r_b})\oplus x_b\}$ 发送给 A.

(3) A 先利用自己知道的 h_{pw} 和 x_a 计算 $H'(h_{pw}\oplus x_a)$，若 $H'(h_{pw}\oplus x_a)\neq H(h_{pw}\oplus x_a)$，则放弃通信，若相等，则 A 确信 B 收到了自己发送的 x_a，然后取出 r_b，将其与 h_{pw}，r_a 合并后计算 $H'(h_{pw},r_a,r_b)$，若 $H'(h_{pw},r_a,r_b)\neq H(h_{pw},r_a,r_b)$，则放弃通信，若相等，则接下来计算 $H(h_{pw},r_a)$，并将其与接收到的 BU 的第四部分 $H(h_{pw},r_a)\oplus x_b$ 作一次异或运算，得到 x_b，最后计算 $H(h_{pw}\oplus x_b)$ 并发送给 B.

(4) B 利用自己知道的 h_{pw} 和 x_b 计算 $H(h_{pw}\oplus x_b)$，若 $H'(h_{pw}\oplus x_b)\neq h(h_{pw}\oplus x_b)$，放弃通信，若相等，则 B 确信 A 收到了 x_b，结束认证[5].

认证及密钥交换阶段的流程图如下：

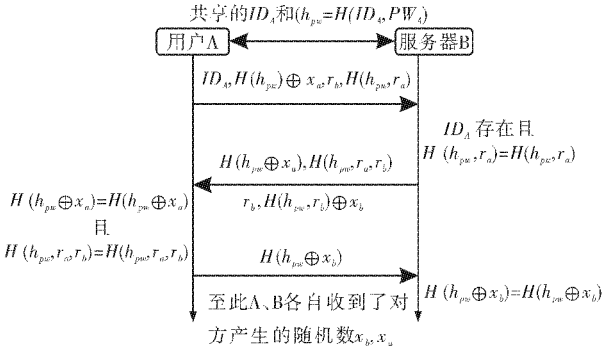

图 1 认证阶段流程图

Fig. 1 flow chart of authentication phase

2.2 加密与解密阶段

RSA 算法一般用于交换对称加密算法的密钥，数字签名，并不直接用来加密数据，因此本节所讲的加、解密本质上是为了在不安全信道上传递对称加密算法的密钥，真正对原始数据的加密由对称加密算法来完成. 加、解密过程如下[6-7]：

(1)加密

$c\equiv(m^e+t_a)\bmod n$

其中 $t_a\equiv s_a(x_a+x_b)\bmod n$.

(2)解密

$m\equiv(c+t_b)^d\bmod n$

其中 $t_b\equiv s_b(x_a+x_b)\bmod n$.

(3)算法证明

主要看解密方程能否还原原文，因 $c\equiv(m^e+t_a)\bmod n$，令 $c=(m^e+t_a)-y^*n$，$y\in Z$ 由解密公式推导原文过程如下：

$$D(c)=(c+t_b)^d \bmod n\equiv$$
$$(m^e+t_a-y^*n+t_b)^d \bmod n\equiv$$
$$(m^e+(x_a+x_b)(s_a+s_b)-y^*n)^d \bmod n\equiv$$
$$(m^e+(x_a+x_b-y)n)^d \bmod n\equiv$$
$$(C_d^0((x_a+x_b-y)n))^0 m^{ed}+$$
$$C_d^1((x_a+x_b-y)n)^1 m^{e(d-1)}+$$
$$L+C_d^d((x_a+x_b-y)n)^d m^{e(d-d)} \bmod n\equiv$$
$$m^{ed} \bmod n=m$$

最后一步由 Euler 定理可证.

3 安全性分析

对协议的攻击种类繁多，这里选取了三种主流的攻击方法来分析本协议的安全性[8].

3.1 中间人攻击

在 2.1 的(a)步骤中，假设中间人 C 截获了 A 发送给 B 的消息 $AU=\{ID_A,H(h_{pw})\oplus x_a,r_a,H(h_{pw},r_a)\}$，C 首先是没必要修改 ID_A 的；其次，由于 C 不知道 h_{pw}，因此 C 无法找到一对 r_c 和 $H(x,r_c)$(其中 x 为中间人任意做出的字符串)，使得 $H(h_{pw},r_a)=H(x,r_c)$. 这是由 hash 函数的弱抗碰撞性来保证的. 所以 C 不能把 r_a 和 $H(h_{pw},r_c)$ 替换为自己的 r_c 和 $H(x,r_c)$；最后，如果 C 将 $H(h_{pw})\oplus x_a$ 换成自己设计的字符串 T_c，在(b)步骤中 B 将回传 $H(h_{pw}\oplus H(h_{pw})\oplus T_c)$，在(c)步骤中 A 将验证回传的字符串是否等于 $H(h_{pw}\oplus x_a)$，因为 h_{pw} 和 x_a 是 C 不知道的两个数，即 C 无法知道 $H(h_{pw}\oplus x_a)$ 的值，因此 C 也不能对回传的字符串进行替换，否则 A 和 B 将发现中间人的 C 的存在，将采取相应措施，C 顶多能做的是把 A 的消息原封不动的传给 B，这样 C 达不到中间人攻击的目的. 其他步骤的分析同上所述.

3.2 重放攻击

攻击者 C 将 2.1 的(a)步骤中 A 发送给 B 的消息 $AU=\{ID_A,H(h_{pw})\oplus x_a,r_a,H(h_{pw},r_a)\}$ 保留，在将来的某个时点重新发送给 B，此时 C 可以通过第一步认证，但 C 无法从 B 回传的 $H(h_{pw},x_b)\oplus x_b$ 中还原出 x_b，因此 C 无法在以往的数据包中找到 x_b 与 $H(h_{pw},x_b)$ 的对应关系，于是在认证阶段的第三步，C 无法回传一个正确的 $H(h_{pw},x_b)$ 给 B. 最终也无法通过认证.

3.3 平行会话攻击

在平行会话攻击中，在攻击者的特意安排下，一个协议的两个或者更多的运行并发执行. 并发的多个协议使得攻击者可能从一个运行中得到另外某个运行中困难问题的答案. 由于该协议每次通信时双方要各自产生随机数互传，每次产生的随机数相等的概率很小，并且双方传输的数据包

格式不同,不可能从另一个运行协议中得到本次协议要回传给对方的数据包.

4　结　语

在认证阶段,通过传输像 $r, H(h_{pw}, r)$ 这样的消息对,使得 r 和 $H(h_{pw}, r)$ 在传输过程中不可被修改,因为很难找到一个 $r'(r' \neq r)$,使得 $H(h_{pw}, r') = H(h_{pw}, r)$,这得益于 Hash 函数的单向性和弱抗碰撞.通过交换各自产生的随机数之后,结合双方选定的 RSA 算法的密钥对,生成一组动态的密钥:A 的私钥 $\{s_a, x_a\}$,B 的公钥 $\{n, e\}$,B 的私钥 $\{s_b, x_b, d\}$,其中 x_a 和 x_b 在每次通信的认证阶段动态生成并相互交换,以实现通信过程中的一次一密.并且并未重新生成大素数而改变密钥对,只是在原有加解密过程中多出一步加法、乘和模运算就生成了新的密钥对,这样既保留了 RSA 算法的安全性,也加入了一次一密的思想,使得破解该动态 RSA 的难度更大.不过此协议适用于通信双方已事先保存了各自的身份信息和选定了一个 RSA 算法的情况,例如金融机构与客户之间的通信,其他情况下的通信还有待进一步研究.

参考文献:

[1] 郑华,郝孟一,王国强. PKI-CA 认证体系在实际应用中的优缺点讨论[J]. 网络安全技术与应用, 2002(3): 16-21.

[2] 廖晓峰,肖迪,陈勇,等. 混沌密码学原理及其应用[M]. 北京:科学出版社, 2009: 18-26.

[3] Douglas R. Stinson. 密码学原理与实践[M]. 冯登国,译. 北京:电子工业出版社, 2003: 131-144.

[4] 蔡琼,彭涛,叶杨. 一种混沌序列加密算法的密码分析[J]. 武汉工程大学学报,2011,33(6):94-97.

[5] Xiang feny Guo, Jiashu zhang. Secure qroup key agreement protocol based on chaotic Hash [J]. Information Sciences, 2010(10):4069-4074.

[6] 张蓓,孙世良. 基于 RSA 的一次一密加密技术[J]. 计算机安全, 2009(3): 53-55.

[7] 齐晓虹. RSA 公开密钥密码体制的密钥生成研究[J]. 武汉理工大学学报,2010,32(6):37-40.

[8] 束妮娜,王亚弟. 关于密码协议攻击的研究[J]. 计算机工程, 2005(19): 148-150.

Key agreement protocol combine with public key cryptography

CAI Qiong , FANG Xuan , FANG Lan

(School of Computer Science and Engineering, Wuhan Institute of Technology, Wuhan 430074,China)

Abstract: Aiming at the problems that computational cost of the public key infrastructure is large and a trusted certificate authority is prerequisite to ensure the security of the cryptosystem, the maintenance of the certificate is also the hidden danger, a key agreement protocol combined with a dynamic public key cryptography was proposed. During the authentication phase ,the prior shared information and the random number which generated by sender were concatenated and calculated their hash values, then, the hash values and the random number were transmitted to the receiver, the unidirectional hash function ensures the random number being transmitted correctly. During the encryption and decryption phase, the random numbers transmitted from each other was used to change keys of public key algorithm dynamically. This method achieves the one-time pad in the communication, it makes more efficiency than the method which regenerates the large prime numbers to change the keys. The safety of this agreement is verified by using three techniques which are commonly used on the network attack.

Key words: public key cryptography; key agreement protocol; one-time pad

本文编辑:陈小平