基于密钥的信息隐藏技术个性化密钥交换

许润萍，　王盼卿

(解放军军械工程学院，河北石家庄 050003)

摘　要：为了实现密钥的安全传输，利用已有的信息隐藏系统，设计了个性化密密钥交换算法，并提出了具体的实现步骤。该方法增加了密钥系统的安全性，提高了信息隐藏系统的不可破译性。

关键词：网络安全；信息隐藏；个性化加密；密钥交换

中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-3516(2006)03-0048-02

现代信息系统中信息安全的核心问题是密码理论及其应用,其基础是可信信息系统的构建与评估。密码理论与技术主要包括两部分,即基于数学的密码理论与技术和非数学的密码理论与技术。最著名的 Diffie-Hellman 密钥交换是美国学者于 1976 年提出的“公开密钥体系”(public key system,PKI)[1]。此后人们相继提出了一些具体实现方案[2],我国学者也提出了一些密钥交换理论及算法[3]。信息隐藏是网络环境下把机密信息隐藏在大量信息中不让对方发觉的一种方法[4],作为一种新的信息安全技术,信息隐藏将在未来网格中保护信息免于破坏起到重要作用,特别是图象叠加、数字水印、潜信道、隐匿协议等的理论与技术的研究已经引起人们的重视[5-6]。

1　个性化加密的设计思想与实现条件

1.1　个性化加密的设计思想

一方对密钥 K 进行个性化的加密,另一方无法知道密钥 K,通过几次交换后完成对密钥 K 的安全传递,从而实现密钥 K 在公共信道上实现安全传递。其基本过程为:①发送方用个性化加密伪装函数 f_A,对密钥 k 进行加密伪装 $f_A(k)$,然后把消息发给接收方。②接收方用个性化加密伪装函数 f_B(f_A 与 f_B 可逆,且 $f_B(f_A(k))=f_A(f_B(k))$,对 $f_A(k)$ 进行再加密伪装为 $f_B(f_A(k))$,把 $f_B(f_A(k))$ 再发给发送方。③发送方再对 $f_B(f_A(k))$ 进行解除自己的个性化的加密伪装函数 f_A^{-1},$f_A^{-1}f_B(f_A(k))=f_B(k)$,然后把 $f_B(k)$ 发送给接收方。④接收方再用个性化解密函数 f_B^{-1},解密 $f_B(k)$,即 $f_B^{-1}(f_B(k))=k$,从而得到消息 k。

1.2　个性化加密函数的实现条件

假设一个信息集合为 X,秘密信息集合为 $M(M\in X)$,定义函数 $f:X\times X\to X$,并且有,①f 是 x 上的二元运算,即若 $x\in X,y\in Y$,则 $f(x,y)\in X$;②f 存在逆运算 f^{-1};③f 满足交换律,即若 $x\in X,y\in Y$,则 $f(x,y)=f(y,x)$;④f 与 f^{-1} 满足结合律,即 $ff^{-1}(x,y)=f^{-1}f(x,y)$。

2　在网络上使用个性化加密进行密钥交换的具体实现

2.1　网络上信息的表示

在网络上实现伪装通信通常采用的伪装载体有文本、图片、声音等,这些载体的信息集合空间为{0,1}。若二进制数的集合为 B,则个性化加密函数 $f:B\times B\to B$,即给定一个密钥 $k\in B$,则可加密为 $f(k)=K'$,其中 $K'\in B$,并且有 $f^{-1}(k)=k$。

收稿日期:2005-11-17
作者简介:许润萍(1963-),女,山西交城人,副教授,博士生,主要从事计算机网络安全研究.

2.2　伪装函数的设计

构建伪装函数只要让其满足个性化加密函数实现条件即可。现在把f函数定义为模2的加法运算,即f: +2,$f(k,r)=k$(其中r为二进制数域上设计实现的伪随机数产生器产生的伪随机数),即计算机实现为$k+2r=k'$。f^{-1}定义为模2的减法运算,即f^{-1}: -2,$f^{-1}(k'',r)=k''$,即计算机实现为$k''-2r=k''$。

可以看出,密钥k加密的安全性依赖于伪随机数r来确定,因此伪随机数r的安全选择是个性化加密保证安全的重要依据。设计伪随机数r应从以下两点考虑:第一,加密函数产生的伪随机数应尽可能的大(即位数多),以降低被攻破的可能。第二,加密函数产生的伪随机数在多次的伪装通信中应尽可能地不重复使用,即尽可能达到一次一个伪随机数。

在计算机上实现产生伪随机数r的设计方法是:计算机的伪随机函数产生的字符串S_1连接当前的日期时间字符串S_2及当前鼠标坐标点构成的字符串S_3,构成字符串$S_1S_2S_3$,再利用Hash函数MD5产生一个128位的二进制数r作为随机数。实现过程见图1。

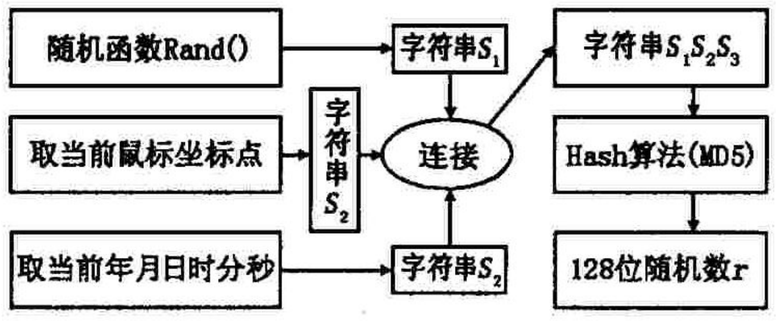

图1　随机数产生的设计实现

2.3　使用个性化加密密钥交换的具体实现步骤

根据采用的个性化加密函数f和产生的r的方法,发送和接收方实现密钥交换的具体步骤如下:①接收方首先确定一个让发送方使用的嵌入密钥k(k的产生是接收方随意定义的字符串,以及伪装通信中选择的伪装载体和嵌入算法来确定的),且转换为二进制数,记为k_2。②接收方对k进行个性加密。即接收方利用伪随机数产生器产生一个128位的二进制随机数r_{2b},然后执行个性化加密得到$K'_2=k_2+2r_{2b}$,发送K'_2给发送方。③发送方接收到K'_2后,对K'_2进行个性化加密。即发送方利用伪随机数产生器产生一个128位的二进制随机数r_{2a},然后执行个性加密得到$K''_2=k'_2+2r_b$,发送K''_2给接收方。④接收方接收到K''_2后,对K''_2进行个性解密。即用前面产生的r_{2b},进行模2减运算,得到$K'''_2=k''_2-2r_{2b}$,把K'''_2发给发送方。⑤发送方接收到K'''_2后,对K'''_2进行个性解密。即用前面产生的r_{2a},进行模2减运算,就得到$K_2=k'''_2-2r_{2a}$,再转换成字符串,就得到密钥k。

在这个过程中,会话发起者是接收秘密信息的接收方,这样进行密钥协商的好处是当消息接受到以后,可以对发送消息的发送者同时进行一次用户认证,由此提供了信息传输的机密性和完整性保证。

3　结束语

信息加密是隐藏信息的内容,而信息隐藏是隐藏信息的存在性,它不容易引起攻击者的注意,所以信息隐藏比信息加密更为安全。在网络信息传输中,对重要秘密信息的传输,将有不可替代的作用,这是未来一个重要的发展方向。本文研究了个性化加密思想,增加了密钥系统安全性,从而使系统具有极高的不可破译性。

参考文献:

[1] Diffie W, Hellmanm E. New Directions in Cryptography[J]. IEEE Trans IT, 1976, 22(6): 644 - 654.

[2] Beth T, Frisch M C. Public - Key Cryptography: State of the Art and Future Directions[M]. New York: Springer - Verlag, 1991.

[3] 韦　卫,王行刚. 密钥交换理论与算法研究[J]. 通信学报,1999,20(7):64 - 68.

[4] Bender W, Grnbl D, Morimito N, et al. Techniques for data hiding[J]. IBM Systems Journal, 1996, 35(3 - 4): 313 - 336.

[5] Swanson M. Kobayashi M. A Multimedia data embedding and watermarking technologies[J]. Pro IEEE, 1998, 86(6): 1064 - 1087.

[6] 孙启禄,殷肖川,王　宾. 一种基于离散小波域的隐藏通信中的混合型信息隐藏技术[J]. 空军工程大学学报(自然科学版),2004,(6):65 - 69.

(编辑:姚树峰)

(下转第54页)