安全信道的建立及应用研究*)

Security Channel and it's Application Research

朱树人　李伟琴

(长沙电力学院　长沙410077)(北京航空航天大学　北京100083)

Abstract　This paper discusses the disadvantage of the authentication system based on symmetrical crypt, and an authentication system based on the RSA encryption is provided, and it's feasibility and security are analyzed and discussed in details.

Keywords　Authentication, Cryptography, DES, Security channel

1　安全信道的建立

所谓安全信道，指的是信息以加密的形式经过网络传播，网络破坏者虽然可以截获网络上传输的所有数据，但他无法得到数据中包含的真正信息。安全信道的建立主要有两项任务：一是通过验证身份确立相互的信任关系；一是协商确定安全信道中所使用的加密密钥。

下面讨论基于主密钥(Master Key)的安全信道的建立过程。主密钥用于在用户登录时在用户和服务中心中之间建立安全通道，保证传输密钥和信息认证密钥初始化的安全。该密钥的生成主动权在用户，由用户方指定两位负责人员，分别独立地产生一个64位的整数。在系统开始运行时由这两位负责人员到中心分别输入他们所掌握的密钥，系统将这两个密钥分别以对方作为密钥进行 DES 加密，将结果异或生成对该用户的主密钥。由于用户的主密钥只有用户自己和服务中心知道，所以通过测试对方是否知道这一主密钥就可以判断对方的身份。而安全信道中所用的加密密钥可以用主密钥加密后通过网络发送，因此，双方可以协商确定安全信道的加密密钥而不用担心该密钥被其他人知道。安全信道的建立过程如图1所示。

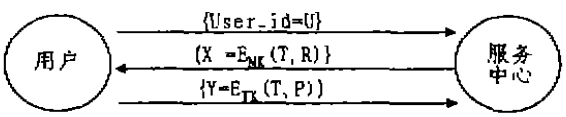

图1　用户登录过程

(1)用户系统与服务中心建立普通的网络连接后，以明文向中心发送信息：

{User_id=U}

其中 U 为用户编号，每个参加通信的用户都被分配一个唯一的编号。

(2)中心确定该用户的编号是合法的编号后，向用户返回信息：

$\{X=E_{MK}(T,R)\}$

其中 T 是当前的日期和时间。R 是中心生成的随机数，函数 E_{MK} 表示用该用户的主密钥进行 DES 加密。

(3)用户收到中心的信息后，用其主密钥解密，如果能得到当前时间 T，说明该信息的加密是正确的，用户可以据此确信对方是服务中心。用户随后将 R 保存起来用以生成传输密钥和认证密钥。用户首先用 R 生成一个传输密钥 TK，向中心发送信息：

$\{Y=E_{TK}(T,P)\}$

其中 T 是当前时间，P 是用户的口令。E_{TK} 表示用用户的传输密钥加密。

(4)中心收到信息后，用和用户同样的方法生成的传输密钥解密信息，得到 T 和 P。如果 T 是当前时间，说明发信者必是合法用户，中心将 P 用某个单向函数(如 UNIX 系统的 crypt()函数)处理后与事先保存的值比较，如果比较正确，用户就成功登录了。

从第二步起每条信息都包含信息认证码，认证码的产生使用用户的主密钥。完成这些程序后，安全信道就建立了。

2　安全信道的安全性分析

该安全信道系统采用 DES 算法和乱码方法进行数据通信的加密，以实现安全信道。DES 算法是一种

*)国家863计划资助项目，课题号：863-306-ZT05-05-6。朱树人　在职博士生，主要研究方向：计算机网络安全与计算机信息系统。李伟琴　教授，博导，主要研究方向：计算机网络信息安全技术和网络管理技术的研究。

安全性很好的加密算法，到目前为止没有发现任何设计上的漏洞。

经过二十年的实践证明 DES 算法完全可以经受密文攻击，但乱码方法被证明是无法经受密文攻击的，所以攻击者很有可能会解密乱码加密信息从而得到密钥。

目前对 DES 算法进行已知明文攻击的手段主要是强行搜索所有密钥空间，平均需要搜索2^{55}次，一台价值百万美元的并行计算机运行2-3小时就可以完成所有搜索。所以如果攻击者可以进行已知明文攻击的话，DES 加密的保密时间仅有2小时。虽然我们对每条信息都采用不同的密钥，但从上面分析的安全因素的依赖性可知，攻击者只要击破连续的两条信息就可以击破整个会话的所有信息，这只需4小时。

对于选择明文攻击，如果攻击者能够在合法的设备上输入他事先确定的信息，那么他可以先用2小时的时间将用所有可能密钥加密该信息的结果计算出来，再在合法设备上输入该信息，随后根据得到的密文查表就可以得到密钥。如果对 DES 算法加密的进行选择明文攻击，需要事先存储的信息将有512MG 字节，在目前大多数情况下都是无法满足的，所以目前 DES 仍然可以说是能够经受选择明文攻击的。

由于从登录的第二条信息开始，每条信息都有信息认证码，保证可以查出信息是否被修改，每条信息都有唯一的标识，系统不承认连续的重复信息，所以攻击者也无法将原来的合法信息再次发送。那么，唯一的问题是这种信息认证算法本身是否安全，是否能象传输密钥一样无法承受已知明文的攻击。从信息认证码的生成过程可知，每一次 DES 运算的输入值都与前面所有运算的输入值相关。攻击者要获得 DES 算法的明文必须回溯到整条信息的开始，而攻击者能得到的密文只有最后的认证码，这就大大增加了攻击的难度，而且信息越长，难度越大，与单一 DES 明文攻击的难度比为：信息长度(字节数)/8，所以信息认证密钥在一定程度上是可以承受已知明文攻击的。

3 改进的信息加密及认证方法

从安全性分析中发现安全信道的加密方法存在容易被已知明文攻击的问题。另外采用 DES 与乱码混合方式加密的主要意图是用 DES 加密全部明文速度太慢，但在进行信息认证码的生成时，又必须将所有明文用 DES 处理一遍。如果将加密和生成信息认证码的过程结合起来一遍扫描完成，就既可以增加安全程度，又可以提高效率。基于该思想，改进的信息加密及认证算法如下。

3.1 算法

(1)加密仍采用 DES 算法。每条信息都使用不同的密钥，但与原设计不同的是，不需要使用一个常数表来产生一个个密钥，首先需要修改上面的身份认证过程，将 RC 变为四个64位的随机数 R1、R2、R3、R4。在中心一方，各个密钥的产生使用公式：

$K_1=DES_{R2}(R1)$

$K_{n+1}=DES_{R2}(K_n \oplus R1)\ n=1,\cdots,N$

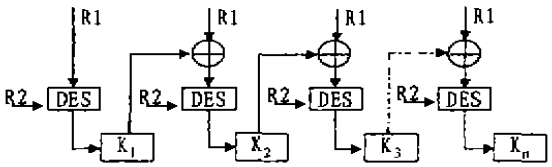

图2 密钥生成序列

其中 DES_{R2}表示用 R2作为密钥进行 DES 加密。在用户方密钥产生与中心的相同，只是用 R3、R4替代 R1、R2。

(2)信息加密及加信息认证码的过程使用如下公式：

$E_0=K(R_S);D_0=0$

$E_n=D_n \oplus D_{n-1} \oplus K(R_S \oplus E_{n-1});n=1,\cdots,N$

$MAC=K \oplus D_N \oplus K(R_S \ominus E_N)$

明文为：

$\{D_1,D_2,\cdots,D_n\}$

加密后对应的信息为：

$\{E_0,E_2,\cdots,MAC\}$

其中 E_n：第 n 块密文；D_n 第 n 块明文；R_S：随机数；K()：以 K 为密钥进行 DES 加密；MAC：信息认证码；D_N：最后一块明文；E_N：最后一块密文；D_1：第一块明文。

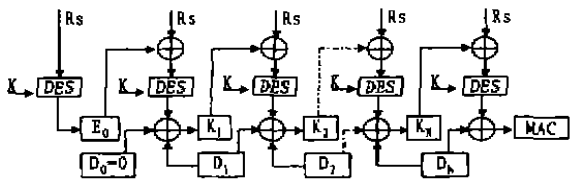

图3 加密及信息验证方法

(3)接收方解密信息使用如下公式：

$R_S=K(E_0);D_0=0$

$D_n=E_n \oplus D_{n-1} \oplus K(R_S \oplus E_{n-1});n=1,\cdots,N$

(4)接收方通过计算 $MAC \oplus D_N \oplus K(R_S \oplus E_N)$进行信息认证。如果结果得到 K，说明信息没有被修改。因为 D_n 的解密密钥依赖 D_{n-1}，如果某一块 E_m 被修改，D_m 解密将得到错误的结果，并会导致其后所有的明文 $D_{m+1}\cdots D_N$ 的错误，最后导致 K 的解密错误。

3.2 算法的安全性分析

前面已经讨论原安全信道中信息加密的主要缺陷在于因 DES 算法无法承受明文攻击，而安全系统中又没能防止猜测明文的可能。为了保证系统的效率，改进的算法也使用 DES 算法，但在具体的应用中努力使明文不被暴露，以使明文攻击变得不可能。

从新的密钥生成公式可以看出，只要保证 R1、R2 是秘密的，攻击者即使获得了 K_0、K_1、…、K_m，也由于无法获得 DES 加密的明文而不能实施明文攻击，从而无法得到 K_{m+1}，而 R1、R2由于是随机数，并且其安全性是由 RSA 算法保证的，只要选择足够长的密钥就能很好地保证 R1、R2的秘密。

同样，在信息加密的过程中，每次 DES 加密使用的输入数据中都包括随机数 Rs，这将使攻击者无法得到 DES 加密的输入，也就无法进行已知明文攻击，攻击者如果采用强硬攻击(依次试探所有 K 和 Rs)，其难度将是2^{112}，也就是说，如果在2小时内能够使用明文攻击攻破普通 DES 加密的话，攻破这种加密方式将需要2×2^{56}小时，所以称之为不可能。

至于其他类型的攻击，该方法与原算法的承受能力是相同的，在此不再讨论。

3.3 算法的效率

改进后的算法对一条 N 字节长度的信息进行加密生成密钥需要一次 DES 运算，加密和生成 MAC 共需要 N/8+1次 DES 运算(忽略 N 不能被8整除时需要补位的情况)，总共需要进行 $N/8+1+1=N/8+2$次 DES 运算，至于算法中的 XOR 运算，同 DES 的时间复杂性相比可以忽略不计。

用原设计的算法对信息加密及生成 MAC 码，设需要 DES 加密的字节总数为 M，M<N，则加密需要 M/8次 DES 运算，生成 MAC 需要 N/8次运算，总共需要 N/8+M/8次运算。

所以，只要 M/8>2，改进后算法的效率就优于原来的算法，而大多数通信中，都会有 M/8>2，因此，改进后算法的效率要优于原来的算法。

结论 本文通过分析一个安全信道系统建立的实例，发现其加密方法存在着容易被已知明文攻击的缺陷。为此，我们通过将加密和生成信息认证码的过程结合起来一遍扫描完成的方法，既增强了其承受已知明文攻击的能力，又提高了其运算效率。该安全信道系统，对通信安全要求高的应用具有一定的参考价值。

参 考 文 献

1 RSA Laboratories, PKCS #1: RSA Encryption Standard, NIST/OSI Implementors' Workshop Document SEC-SIG-91-18

2 FIPS PUB 186: DIGITAL SIGNATURE STANDARD (DSS) Federal Information Processing Standards Publication, 1994

3 Kaliski B, RFC1319 The MD2 Message-Digest Algorithm. RSA Laboratories, April 1992

4 Rivest R RFC1320. The MD4 Message-Digest Algorithm. MIT Laboratory for Computer Science and Data Security, Inc. April 1992

5 Rivest R. RFC1321. The MD5 Message-Digest Algorithm, MIT Laboratory for Computer Science and Data Security, Inc. April 1992

6 Kohl & Neuman. RFC1510: The Kerberos Network Authentication Service(V5)

(上接第45页)

HASH 机制使得被篡改的报文将被发现。协议中引入的 cookie 具有的方向性使得反射攻击失败，cookie 具有的时效性使得重放攻击失败。中间人可以在中间欺骗通信的双方完成协议的[1]—[4]，但由于不知道 Initiator 的 RSA 私钥，无法完成伪造 Initiator 的数字签名，[5]无法通过 Responder 的检验，协议将不能完成，从而抵抗中间人攻击。

结束语 如何安全地动态生成与分发会话密钥是在 IP 环境下实现虚拟专用网的关键问题。本文描述的 IKE 协议依靠采用算法的安全性，协议机制的完备性及 cookie 机制能够实现安全的密钥交换，并具备抵抗可能攻击的能力。当然随着密码学的进展，采用算法的安全性将受到考验。同时在 IP 环境下各种新的攻击方式不断出现，而服务拒绝攻击永远不可能消除。

参 考 文 献

1 RFC 2047. The Internet IP Security Domain of Interpretation for ISAKMP

2 RFC 2408 Internet Security Association and Key Management Protocol(ISAKMP)

3 RFC 2409. The Internet Key Exchange(IKE)

4 FRC 2412. The OAKLEY Key Determination Protocol

5 RFC 2522. Photuris: Session-Key Management Protocol

6 Schneier. Applied Cryptography, Protocols, Algorithms, and Source Code in C

7 王育民，刘建伟 通信网的安全——理论与技术. 西安电子科技出版社，1998