一种基于数字签名的IKE协议的实现与分析

One IKE Protocol Based on Digital Signature and its Analysis

程朝辉　顾文刚　凌　力　朱　洪
（复旦大学计算机科学系　上海200433）

Abstract　This document describes one protocol which uses Diffie-Hellman algorithm and part of Session-Key Management Protocol in conjunction with ISAKMP to obtain keying materials authenticated by RSA digital signature for use with ISAKMP and for other security association such as AH and ESP for the IETF IPsec DOI. Also this document analyzes the protocol is how to resist some forms of attacks

Keywords　IKE

一　引言

现在的虚拟专用网络主要采用两种技术实现：一种技术是采用配置物理设备的方法，使得数据包在被认为安全的路由上进行明文传输，另一种技术是将数据进行加密，然后在开放的网络上进行密文传输。在采用加密方式的虚拟专用网中，关键是如何实现动态产生及分发新鲜的会话密钥，密钥分发过程是必须是安全的，能够有效地抵抗可能的攻击，这是任何一种因特网密钥交换协议(IKE)需要解决的主要问题。

二　背景知识

为了在IP环境下实现数据的安全传输，IETF提出了IPsec体系结构，该体系结构主要包括四个部分：安全协议(AH,ESP)，安全连接(Security Association：SA)密钥交换(Internet Key Exchange：IKE)及认证与加密算法。在IPsec体系下，要进行安全通信的两个实体必须先根据安全策略建立一个或多个安全连接(SA)，一个安全连接是一种安全协议的相关属性，如：采用的加密或认证算法，参数等的集合体，它能提供一种或多种安全服务(数据源认证，加密，数据完整性检测等)，用户的数据在安全连接(SA)提供的安全服务的保护下进行传输。IPsec体系中的安全连接与密钥管理协议(ISAKMP[1])提出在两个实体间建立一个安全连接(SA)要分成两个阶段：阶段一建立一个ISAKMP SA，该SA主要是提供对安全协议SA的建立过程的保护，阶段二在ISAKMP SA提供的安全服务的保护下协商建立与具体安全服务相关的安全协议SA。之所以要分成两个阶段是基于以下三个考虑：1)安全协议SA的建立过程需要保护；2)为了保证会话密钥的新鲜性，可能需要频繁地建立安全协议SA；3)两实体为实现一种安全策略可能需要建立多个安全协议SA，分为两个阶段后，多个安全协议SA的建立过程可以复用阶段一的ISAKMP SA。但ISAKMP侧重于安全连接及密钥的管理，仅就密钥交换提出了一个框架，所以需要另外的IKE协议来实现密钥的动态生成与分发。本文将描述一种具体的IKE协议，但将注重于协议的过程，而认为采用的算法的安全性是强的。

协议中采用了如下算法：HASH算法：MD5算法[6]；数字签名算法：RSA算法[6]；加密算法：3DES-CBC算法[6]；密钥生成算法：Diffie-Hellman算法[6]。

三　协议描述

本IKE协议采用Diffie-Hellman算法交换半密钥共同决定会话密钥信息，为了抵抗中间人攻击采用RSA数字签名进行认证，采用MD5算法保证数据的完整性，采用3DES-CBC算法进行数据加密，保证分发的密钥信息的秘密性，并采用cookie[5]机制保证协议在IP环境下的健壮性。协议在建立安全连接的两实体都具有对方的公钥或证书的前提下实现，遵循ISAKMP提出的IKE框架。协议两阶段的具体过程如下：

阶段一协商建立ISAKMP SA的策略、算法、参数等属性，通过Diffie-Hellman算法生成共享密钥信息，

程朝辉　硕士研究生，研究方向：计算机网络与分布式计算。顾文刚　硕士研究生，研究方向：计算机网络与分布式计算。凌　力　副教授，研究方向　计算机网络与分布式数据库。朱　洪　教授，博士生导师，研究方向，算法复杂性。

建立 ISAKMP SA、阶段成果：建立 ISAKMP SA 及由(CKY_I,CKY_R)标识的3类密钥信息。

Initiator

[1]CKY_I,0,GRP,EHAO

[3]CKY_I,CKY_R,g∧x,Ni

[5]CKY_I,CKY_R,E{IDii,SIG_I}Kir

Responder

[2]CKY_I,CKY_R,GRP,EHAS

[4]CKY_I,CKY_R,g∧y,Nr

[6]CKY_I,CKY_R,E{IDir,SIG_R}Kir

阶段二协商建立其它安全协议(AH、ESP)SA 的策略、算法、参数、会话密钥信息等属性，建立安全协议 SA。阶段成果，建立安全协议 SA 及会话密钥信息 KEYMAT。

Initiator

[7]CKY_I,CKY_R,E{HASH(1)|SAi|Ni}Kir

[9]CKY_I,CKY_R,E{HASH(3)}Kir

Responder

[8]CKY_I,CKY_R,E{HASH(2)|SAr|Nr}Kir

其中，

·A|B：表示数据 A 与数据 B 连接。

·CKY_I,CKY_R：用于标识一个 ISAKMP SA，同时对该协议抵抗攻击有重要作用，具体分析见第五节攻击分析。

·GRP：用于指定 Diffie-Hellman 算法中的公开密钥(g,n)[4]。

·EHAO：Initiator 提出的关于 ISAKMP SA 可供选择的属性[4]，协议协商是 IPsec 体系结构的要求。

·EHAS：Responder 对 Initiator 提出的 ISAKMP SA 属性的响应[4]，协议协商是 IPsec 体系结构的要求。

·g∧x,g∧y：Diffie-Hellman 算法中交换的半密钥，分别为 g 的 x 次方，g 的 y 次方。

·Ni,Nr：分别由双方产生的随机数。

·IDii,IDir：分别是双方实体的标识[1]。

·SIG_I=S{HASH_I}Ki：采用 Initiator 的 RSA 私密钥 Ki 对 HASH_I 进行加密作为数字签名。

·SIG_R=S{HASH_R}Kr：采用 Responder 的 RSA 私密钥 Kr 对 HASH_R 进行加密作为数字签名。

·HASH_I=HMAC-MD5(SKEYID,g∧x|g∧y|CKY_I|CKY_R|SAi|IDii)：Initiator 作的报文摘要。

·HASH_R=HMAC-MD5(SKEYID,g∧x|g∧y|CKY_I|CKY_R|SAr|IDir)：Responder 作的报文摘要。

·SKEYID=HMAC-MD5(Ni|Nr,g∧xy)。

·SAi,SAr：指在阶段一中 ISAKMP SA 对该 SA 的相关参数的建议及选择，包括如：GRP，EHAO，EHAS 等[4]。

·E{X}Kir：采用 Kir 为密钥对数据 X 进行3DES-CBC 加密。

·Kir=K1|K2：ISAKMP SA 的加密密钥，因3DES 需要的密钥长度超过 HMAC-MD5的输出时，采用级联反馈方式生成密钥。

·K1=HMAC-MD5(SKEYID_e,0)

·K2=HMAC-MD5(SKEYID_e,K1)

·IV=MD5(g∧x|g∧y)：3DES 算法的初始向量

·SKEYID_e=HMAC-MD5(SKEYID,SKEYID_a|g∧xy|CKY_I|CKY_R|2)

·HASH(1)=HMAC-MD5(SKEYID_a,M_ID|SAi|Ni)

·HASH(2)=HMAC-MD5(SKEYID_a,M_ID|SAr|Ni|Nr)

·HASH(3)=HMAC-MD5(SKEYID_a,0|M_ID|Ni|Nr)

·SKEYID_a=HMAC-MD5(SKEYID,SKEYID_d|g∧xy|CKY_I|CKY_R|1)

·SAi,SAr：指在阶段二中安全协议 SA 对该 SA 的相关参数的建议及选择，包括如：安全协议标识，算法等[1]

·KEYMAT=K1|K2|K3……：安全协议 SA 的密钥信息，当 SA 需求的密钥长度超过 HMAC-MD5的输出时，采用级联反馈方式生成密钥

·K1=HMAC-MD5(SKEYID_d,protocol|SPI|Ni|Nr)

·K2=HMAC-MD5(SKEYID_d,K1|protocol|SPI|Ni|Nr)

·K3=HMAC-MD5(SKEYID_d,K2|protocol|SPI|Ni|Nr)

……

·IV=MD5(阶段一的最后一个加密输出块|M_ID)：ESP 协议中的加密算法的初始向量。

·SKEYID_d=HMAC-MD5(SKEYID,g∧xy|CKY_I|CKY_R|0)

·protocol：安全协议(AH,ESP)的标识[1]

·SPI：与 protocol 一起标识一个安全协议 SA[1]

·M_ID：报文的类型[1]

四 协议分析

步骤[1]、[2]是协商ISAKMP SA的相关信息。由Initiator提出可供选择的内容：FAHO中包括可以使用的加密算法，HASH算法，认证算法，GRP指定Diffie-Hellman算法可以使用的公钥信息(g,n)。Responder对Initiator提出的建议作出选择，选择的结果放在EAHS与GRP中。该协议中双方使用3DES-CBC加密算法，MD5作HASH算法，RSA数字签名算法。到此双方已确定了由GRP指定的Diffie-Hellman算法的公钥(g,n)。

步骤[3]、[4]双方交换各自的半密钥g∧x、g∧y，同时交换各自生成的随机数Ni、Nr。到此双方共同生成了秘密信息：g∧xy mod(n)，该信息可用于派生ISAKMP SA中的各类密钥(SKEYID、SKEYID_a、SKEYID_d、SKEYID_e、Kir等)。随机数的作用是提供认证的材料并保持密钥的新鲜性。

步骤[5]、[6]使用RSA算法实现相互的认证，并对步骤[1]—[6]的数据完整性进行检查。Initiator使用自己的RSA私钥对摘要信息HASH_I加密进行签名，由Responder采用Initiator的公钥对签名解密，然后将自己计算的HASH_I与报文中的HASH_I匹配。如果匹配成功则证明步骤[5]是Initiator发出的报文，由于HASH_I是采用SKEYID作密钥对g∧x|g∧y|CKY_I|CKY_R|SAi|IDii生成的消息认证码，所以HASH_I是与CKY_I、SAi、g∧x、Ni、IDii相关联的，从而证明步骤[1]、[3]、[5]都是Initiator发出。Initiator对Responder的认证过程相同，从而证明步骤[2]、[4]、[6]都是Responder发出。这样实现了双方的数据源认证，保证了只有双方才拥有秘密信息g∧xy mod(n)，ISAKMP SA中的各类密钥都是由SKEYID作密钥的消息认证码，而SKEYID是采用Ni|Nr作密钥的g∧xy消息认证码，所以SKEYID是双方才共享的秘密，从而保证ISAKMP SA中的各类密钥的秘密性。Ni、Nr引入保证了密钥的新鲜性，加大了密码分析的难度。又由于HASH_I、HASH_R都与CKY_I、CKY_R、g∧x、g∧y相关，从而将步骤[1]—[6]连接起来，并由两个摘要函数保证了步骤[1]—[6]的数据完整性。这两个步骤的报文是在以SKEYID_e为密钥加密后采用密文传输，提供了对信息的保密性。

步骤[7]、[8]是协商安全协议(AH、ESP)SA的相关信息：由Initiator在SAi中提出可供选择的内容，Responder对Initiator提出的建议作出选择放在SAr中。同时双方分别提供一随机数Ni、Nr，两随机数用于为每一SA生成一独特的密钥信息，从而保证密钥的新鲜性。步骤[7]、[8]采用隐含的方式相互认证，阶段1中完成的数据源认证保证了只有通信双方才知道密钥消息Kir，Responder通过解密E(HASH(1)|SAi|Ni，Kir)，然后将自己计算的HASH(1)与报文中的HASH(1)匹配，如果匹配成功可以证明步骤[7]是Initiator发出的报文，同理可以对步骤[8]、[9]作数据源认证。

步骤[9]使得协议是完整封闭的，为阶段2提供一个明确的结束报文。

五 抵抗攻击分析

作为一种在IP环境下，尤其是可能在开放的网络环境下使用的协议需要有必要的保护机制来抵抗可能出现的各种攻击。本协议综合协议过程，算法安全性和一种称为cookie的机制来实现协议保护。以下是协议对一些通常攻击方式的抵抗原理分析。

·**抗服务拒绝攻击** 可以看到该协议有大量的数学运算，每一方在阶段一要作：1次RSA加密运算，1次3DES运算，1次Diffie-Hellman运算，至少7次MD5运算。阶段二要作：至少1次3DES，至少2次MD5运算。所以一定要有机制防止大量的伪装的报文消耗CPU资源。该协议中引入CKY_*(cookie[5])机制，在进行大量数学运算前尽量检测出不合法报文。为达到检测出伪装报文的要求，cookie的生成应采用以下的原则：(1)cookie的生成信息与通信的特定方有关，(2)任何其他人无法生成能被另一方接受的cookie，(3)cookie应具有时效性，(4)必须能快速生成与验证cookie。本协议中采用以下方法生成两个cookie：

CKY_I=MD5(secreti，源IP|目的IP|源UDP端口号|目的UDP端口号|时戳i)

CKY_R=MD5(secretr，源IP|目的IP|源UDP端口号|目的UDP端口号|时戳r|CKY_I|)

该方法使用源与目的IP，CKY_R中加入CKY_I的摘要信息来满足原则1，采用秘密secreti、secretr来满足原则2，加入时戳信息来满足原则3，MD5算法的快速性满足原则4。例如攻击者回放一个以前使用过的步骤[5]的报文，Responder先检查CKY_R，发现该报文已经过时，仅简单地抛弃，而不会进行3DES解密，HASH_I，SIG_I运算。

·**抗连接插入攻击** 该协议采用先交换SA相关信息、密钥信息，在步骤[5]、[6]才进行数据源认证，并且如步骤[5]、[6]的协议分析中指出的那样，步骤[1]—[6]有信息关联，从而使得攻击者无法进行连接插入攻击。

·**抗中间人攻击** 封闭完整的协议机制使得中间人在插入，删除报文时协议将无法完成。协议中的

(下转第52页)

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