互联网密钥交换协议及其安全性分析*

范 红+

(中国科学院 研究生院 信息安全国家重点实验室,北京 100039)

An Internet Key Exchange Protocol and Its Security Analysis

FAN Hong+

(State Key Laboratory of Information Security, Graduate School, The Chinese Academy of Sciences, Beijing 100039, China)

+Corresponding author: Phn: 86-10-88258010, E-mail: pkfanhong@sina.com.cn; pkfanhong@sohu.com.cn

Received 2001-10-23; Accepted 2002-06-12

Fan H. An Internet key exchange protocol and its security analysis. *Journal of Software*, 2003,14(3):600~605.

Abstract: The complexity of Internet key exchange protocol causes some potential secure flaws. The possible attacks suffered by IKE protocol based on the in-depth analysis of its operational principle are discussed.

Key words: IKE protocol; mode; key; security analysis; attack

摘 要: 互联网密钥交换(Internet key exchange)协议的复杂性使得其存在一些安全漏洞.在深入分析 IKE 协议工作原理的基础上,探讨了其可能遭受的攻击.

关键词: IKE 协议;模式;密钥;安全性分析;攻击

中图法分类号: TP309 **文献标识码**: A

IKE 协议是 IPSec 定义的密钥交换技术,它沿用了 ISAKMP 的基础、OAKLEY 的模式以及 SKEME 的共享和密钥更新技术,从而定义出自己独一无二的验证加密材料生成技术和共享策略协商技术.IKE 协议依靠公钥密码体制、私钥密码体制和 Hash 函数,提供了诸多的交换模式和相关的选项,其最终结果是一个通过验证的密钥以及建立在双方共识基础上的安全服务——IPSec SA.

IKE 协议的复杂性使得其存在一些安全漏洞[1].本文在深入分析 IKE 协议工作原理的基础上,对其可能遭受的攻击进行了探讨.

1 IKE 协议的工作原理

IKE 协议定义了密钥协商的两个阶段和 Diffie-Hellman 交换标准密码组.在阶段 1,通信双方使用主密钥建立安全联盟 SA,协商阶段 2 使用密钥因子和各种机制(如加密算法和 Hash 函数等).在阶段 2,IKE 协议使用阶段 1 产生的安全联盟为下一步通信建立提供保密和认证的密钥及其机制.阶段 1 建立的安全联盟是双向的,因此,阶段 1 的发起者在阶段 2 中既可以是发起者,也可以是响应者.

IKE 协议有 4 种可提供不同服务的模式[2]:主模式、积极模式、快速模式和新组交换模式.主模式和积极模

* Supported by the National Natural Science Foundation of China under Grant No.60025205 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802 (国家重点基础研究发展规划(973))

第一作者简介: 范红(1969－),女,河北保定人,博士生,讲师,主要研究领域为计算机网络安全.

式在阶段 1 中使用,其区别在于主模式的消息交换是在一些初始认证完成之后进行的,而积极模式则没有这一层保护,而且交换的消息较少.根据使用的验证方法的不同,主模式和积极模式均可以用 4 种方式实施,但每一种方式都是使用 Diffie-Hellman 密钥分配协议来产生密钥因子的.快速模式在阶段 2 中使用,可提供 4 种选择:根据是否提供完美向前保密(perfect forward secure)而分别选用 Diffie-Hellman 密钥交换(DH 交换)机制和更为快速的传统的共享密钥生成机制;根据是否包含识别消息而分别选用两种不同的协议形式.新组交换模式用于协商新的 Diffie-Hellman(DH)组.因此,IKE 协议实际上是由 13 种不同的子协议组合而成的.IKE 协议涉及的相关术语[3]有:

HDR 是消息头,HDR*表示对头后的消息加密;

Sa*x* 表示由 *x* 提供的安全联盟;

KE*x* 是 *x* 的 Diffie-Hellman 密钥因子;

N*x* 表示由 *x* 生成的随机数;

ID*x* 是 *x* 的识别符号;

Ki*r* 表示由 KE*i* 和 KE*r* 产生的 Diffie-Hellman 密钥;

CKY-I 和 CKY-R 是分别由发起者 I 和响应者 R 产生的包含在消息头中的随机“Cookies”,是对一个秘密、对方的身份以及一个时间计数器值进行综合散列运算而创建的.

1.1 主模式

主模式通过 3 次交换的 6 条消息最终建立 IKE SA.3 次交换分别是用于模式协商的 1 次 DH 交换、1 次随机数交换以及 1 次双方身份相互验证交换.主模式有 4 种不同的身份验证方法:预共享密钥(PSKEY)、数字签名、标准公钥加密和修订公钥加密.基于预共享密钥验证方法的主模式为

(1) I→R: HDR,Sa*i*;

(2) R→I: HDR,Sa*r*;

(3) I→R: HDR,KE*i*,N*i*;

(4) R→I: HDR,KE*r*,N*r*;

(5) I→R: HDR*,ID*i*,HASH_I;

(6) R→I: HDR*,ID*r*,HASH_R.

在第 1 次交换中(消息 1,2),通信双方需要协商 IKE SA 的各项参数,拟定其余部分的交换规范,并互换双方的随机“Cookies”.在第 2 次交换中(消息 3,4),双方交换 DH 公共值(在第 1 次交换中协商好的组内交换)以及伪随机数.此后,通信双方生成 SKEYID,并进而衍生一组密钥,包括加密材料生成密钥 SKEYID-d、验证密钥 SKEYID-a 以及加密密钥 SKEYID-e.在最后一次交换中(消息 5,6),双方各自标定自己的身份,并互换验证散列摘要.交换的最后两条消息是用 SKEYID-e 加密的.

预共享密钥是最简单的身份验证方法,其中一个明显的局限是由于 SKEYID-e 的生成要用到预共享密钥的方法,因此在不能确知所使用的预共享密钥的情况下,通信双方都无法解密消息 5,6 中的 ID 载荷.因此预共享密钥只能基于对方的 IP 地址.但在远程访问中,由于协议发起者的 IP 地址无法预知,响应者仍无法获知预共享密钥.因此,在远程访问中可采用数字签名验证方法,或者如果预共享密钥验证方法是必须的,那么可采用积极模式.基于数字签名验证方法的主模式为

(1) I→R: HDR,Sa*i*;

(2) R→I: HDR,Sa*r*;

(3) I→R: HDR,KE*i*,N*i*;

(4) R→I: HDR,KE*r*,N*r*;

(5) I→R: HDR*,ID*i*,[CERT,] SIG_I;

(6) R→I: HDR*,ID*r*,[CERT,] SIG_R.

SIG_I 和 SIG_R 是散列的签名.上述两种验证方法的区别在于,后者增加了可选的载荷,所以可进行证书的

交换,而且验证的是散列的签名而不仅仅是散列.

标准公钥加密和修订公钥加密两种验证方法都是基于加密随机数的.后者的出现是由于标准公钥加密验证方法代价过高,而修订方案只进行一次的公钥加密,对其他载荷的加密是用对称加密算法来完成的.这两种方法存在的脆弱点是,即使会话消息和通信状态被完好保存,参与通信的任一方仍可事后抵赖.这是因为交换的随机数是用对方的公钥加密的,而且双方都知道对方交换消息的完整内容,所以整个过程可以轻易伪造.基于标准公钥加密验证方法的主模式为

(1) I→R: HDR,Sa*i*;

(2) R→I: HDR,Sa*r*;

(3) I→R: HDR,KE*i*,{ID*i*}pub_*r*,{N*i*}pub_*r*;

(4) R→I: HDR,KE*r*,{ID*r*}pub_*i*,{N*r*}pub_*I*;

(5) I→R: HDR*,HASH_I;

(6) R→I: HDR*,HASH_R.

在这种交换方式下,ID 载荷是在第 2 次交换中进行传递的.这是因为发起者必须向响应者指明自己的身份,以便响应者能够正确地定位公钥,从而对反馈给它的响应进行加密.

将 ID 载荷和随机数载荷分开加密是必须的,否则 ID 载荷的长度中就必须包括加密的随机数载荷的长度,而接收者将猜测 ID 载荷与随机数载荷的分界处,这是困难的.但两次公钥加密却不是必须的.修订方案通过使用对称密钥 ke_*ir* 对消息进行加密可减少一次公钥加密,如下所述:

(1) I→R: HDR,Sa*i*;

(2) R→I: HDR,Sa*r*;

(3) I→R: HDR,Ke*i*,{ID*i*}ke_*ir*,{Ni}pub_*r*;

(4) R→I: HDR,Ke*r*,{ID*r*}ke_*ir*,{N*r*}pub_*I*;

(5) I→R: HDR*,HASH_I;

(6) R→I: HDR*,HASH_R.

1.2 积极模式

积极模式的用途与主模式一样,所不同的是,积极模式只用了主模式一半的消息,而且不提供身份保护,因此其协商能力受到限制.所以积极模式最大的优点是速度快,其代价则是在某种程度上降低了协议的安全性.积极模式的协商过程为:发起者在第 1 条消息中提供一个保护套件列表、DH 公共值、随机数以及身份资料;响应者在第 2 条消息中回应一个选定的保护套件、DH 公共值、随机数、身份资料和一个验证载荷(对于预共享密钥和公钥加密验证来说是一个散列,对于数字签名验证来说则是一个签名的载荷);发起者在最后一条消息中发送它的验证载荷.响应者只有在收到第 3 条消息并正确识别发起者的身份之后才生成 DH 乘幂.因此,第 3 条消息是不加密的.根据所采用的验证方法的不同,积极模式也有 4 种不同的表示形式.

积极模式的功能非常有限但却十分有用.如在上述的远程访问中,如果双方都打算用预共享密钥的验证方法,那么积极模式是建立 IKE SA 惟一可行的交换方法.另外,如果发起者已知响应者的策略,或者对策略有着非常全面的理解,那么使用积极模式可更快地创建 IKE SA.

1.3 快速模式

快速模式是在 IKE SA 保护下在阶段 2 中进行的交换,而且在一个 IKE SA 的保护下可并发地进行多个快速模式交换.在一次快速模式交换中,通信双方需要协商 IPSec SA 的各项特征,并为其生成密钥.IKE SA 提供两项保护:一是使用 SKEYID_e 对消息进行加密以保证交换消息的机密性;二是使用 SKEYID_a 对整个消息进行验证以提供数据的完整性,并对数据源的身份进行验证.每个快速模式交换都有一个独一无二的消息 ID,所以当对 IKE 协议消息进行多路复用时能够据此判断消息从属于哪一次交换.

在默认的情况下,IPSec SA 使用的密钥是由 IKE 协议秘密状态衍生的,因此这些密钥均不具备完美向前保密的特性.为了提供 PFS,DH 公共值以及衍生出它们的那个组都要和随机数一起进行交换,同时还要交换具体

的 IPSec SA 协商参数.最后,利用所得到的秘密来生成 IPSec SA,以确保实现 PFS.

1.4 新组交换模式

新组交换是在阶段 1 之后必须进行的.IKE 协议共定义了 5 个 DH 组,通信双方均可使用.其中 3 个组使用了乘幂算法(在一个质数模的基础上),另两个组使用了椭圆曲线算法.新组交换模式允许各方协定自己的私有组,并定义了组标识符,以便在将来的交换中对组进行指定.由于交换的数据是极为敏感的,故这种交换必须受到 IKE SA 的保护.需要指出的是,响应者应当对发起者提出的组的强度进行测试.例如发起者提议在一个质数模的基础上乘幂运算,并给出了相应的质数和底数,响应者针对提供的模数,应检查它是否为质数.如果不是,则应拒绝提议.

2 IKE 协议的安全性分析

2.1 IKE协议阶段1的分析

对阶段 1 中基于数字签名验证方法的积极模式进行分析.首先给出协议描述:

(1) I→R: HDR,SAi,KEi,Ni,Idi;

(2) R→I: HDR,SAr,KEr,Nr,IDr,Kr^{-1}[prf(Kir,(KEr,KEi,CKY-R,CKY-I,IDr))];

(3) I→R: HDR,Ki^{-1}[prf(Kir,(KEi,KEr,CKY-I,CKY-R,IDi))].

协议的一个攻击描述如下(Z 表示攻击者):

(1) I→R: HDR,SAi,KEi,Ni,Idi.

攻击者 Z 截获此消息,用 IDz 替换 IDi 后将结果发给 R.

(1′) Z→R: HDR,SAi,KEi,Ni,Idz;

(2′) R→Z: HDR,SAr,KEr,Nr,IDr,Kr^{-1}[prf(Kir,(KEr,KEi,CKY-R,CKY-I,IDr))].

这条消息也被攻击者截获并伪装成 R 发向 I.

(2) Z(R)→I: HDR,SAr,Ker,Nr,IDr,Kr^{-1}[prf(Kir,(KEr,KEi,CKY-R,CKY-I,IDr))].

I 收到此消息认为是 R 对其初始消息的应答消息.但是 R 却认为是在与 Z 进行通信,所以当它收到一个 I 签名的消息时将会拒绝它.

2.2 对IKE协议阶段2的分析

在阶段 1 建立的 IKE SA 的保护下,通信的任何一方都可在阶段 2 中主动发起协议.因此,我们在下面的分析中用 A,B 取代 I,R 来表示通信双方的实体,以免产生歧义.阶段 2 的 IKE 协议快速模式采用随机或伪随机数字生成器生成一个惟一的以明文形式包含在每一个消息头中的消息标识 M_ID 来识别一次协议交换中的消息.协议具体描述如下:

(1) B→A: HDR,EK_{AB}[prf(AK_{AB},(M_ID,SA_B,N_B,KE_B)),SA_B,N_B,KE_B].

EK_{AB} 和 AK_{AB} 分别是阶段 1 建立的 A,B 间共享的加密密钥和认证密钥.prf 是伪随机函数.

(2) A→B: HDR,EK_{AB}[prf(AK_{AB},(M_ID,SA_A,N_A,N_B,KE_A)),SA_A,N_A,KE_A].

B 收到此消息后,用 N_A,N_B,KE_A 和 KE_B 生成共享密钥.

(3) B→A: HDR,EK_{AB}[prf(AK_{AB},(M_ID,N_B,N_A))].

A 收到此消息后亦生成共享密钥.

协议的一个攻击描述如下:

(1) B→A: HDR,EK_{AB}[prf(AK_{AB},(M_ID,SA_B,N_B,KE_B)),SA_B,N_B,KE_B].

B 向 A 发起建立共享密钥的请求,此消息被攻击者截获.

(1′) Z(A)→B: HDR,EK_{AB}[prf(AK_{AB},(M_ID,SA_B,N_B,KE_B)),SA_B,N_B,KE_B].

攻击者伪装成 A 向 B 发起建立共享密钥的请求.

(2′) B→A: HDR,EK_{AB}[prf(AK_{AB},(M_ID,N_B,SA'_B,N'_B,KE'_B)),SA'_B,N'_B,KE'_B].

B 响应 A(实际上是攻击者)的请求,此消息也被攻击者截获.

(2) Z(A)→B: HDR,EK_{AB}[prf(AK_{AB},(M_ID,N_B,SA'_B,N'_B,KE_B')),SA'_B,N'_B,KE'_B].

攻击者利用截获的消息伪装成 A 回应 B 建立共享密钥的请求.收到此消息后,B 生成密钥并视之为与 A(实际上是攻击者)进行通信的良好会话密钥.

(3) B→A: HDR,EK_{AB}[prf(AK_{AB},(M_ID,N_B,N_B'))].

攻击者截获此消息.

(3′) Z(A)→B: HDR,EK_{AB}[prf(AK_{AB},(M_ID,N_B,N_B'))].

攻击者利用截获的消息伪装成 A 回应 B,使 B 相信 A(实际上是攻击者)与之建立了良好的共享密钥.

协议完成时,B 认为它与 A 共享两个密钥,一次是 B 主动与 A 建立的,一次是 A 主动与 B 建立的.但实际上,A 根本没有参与任何实际的协议运行,因此 B 事实上拒绝了服务(与 A 建立共享密钥).

2.3 弱点分析

通过分析我们大致可以得到IKE协议遭受上述攻击的原因.IKE协议在一次交换中使用每一个消息的最后一个密文块作为下一个消息的初始向量以抵抗报文重放攻击,此技术可抵抗重放的消息插入正在进行的交换中的攻击,却对重放整个报文序列造成的重放攻击无能为力.上述报文序列重放攻击产生的一个重要原因是IKE协议消息格式上的类同,而且通信双方可扮演双重角色(发起者和响应者),所以接收者无法判断所接收的消息是一个初始消息,还是一个应答消息.因此在消息头中明确指出消息的初始/应答状态是非常重要的.一个主体判定所收到消息的初始/应答状态的方法有两种,一是解密消息并检验其内容,二是检查是否存在另一个正在进行的具有同样 ID 的消息交换.如果存在,则消息被视为一个应答消息,否则为一个初始消息.显然,第 2 种方法可以抵抗上述攻击.当 B 收到一个重放的消息时,通过检查消息 ID,B 认为这是一个应答消息.而当 B 进一步解密消息时,将会发现这是一个错误消息并丢弃它.此方法依赖于消息ID的随机性,因此在IKE协议说明中应明确标注消息的初始/应答状态,并且消息 ID 必须是随机产生的.

2.4 其他攻击

(1) 反射攻击

IKE 协议的 HASH_I 和 HASH_R 的计算公式是对称的,这隐含了一个反射攻击.例如,在基于预共享密钥验证方法的主模式中,一个不诚实的响应者可以声称为一个与发起者同样的实体并仍通过认证.具体作法是不诚实响应者用 CKY-I 取代 CKY-R,用 g^i 取代 g^r,并使用发起者的标识,此时 HASH_R 等于 HASH_I.由此,不诚实响应者可将发起者发送的 Hash 值“反射”回去(事实上,不诚实的响应者并不能解读由发起者发来的第 5 条消息,但由于不诚实的响应者欲发送的消息与加密的第 5 条消息具有同样的格式,第 5 条消息可被当作第 6 条消息加以返回).同样的攻击可发生在基于数字签名验证方法的主模式中,响应者可重放发起者的最后消息并通过验证.

(2) 选项攻击

Hash 的计算不包括响应者对 SA 的答复,这使得攻击者可对 SA 进行任意的操纵.假设发起者发送了一系列按优先等级排列的选项,攻击者在不影响其他交换正常进行的前提下,可通过修改响应者的 SA 来选择一个最弱的模式,并用这个比诚实响应者所期望的弱得多的安全选项进行通信.假设攻击者在阶段 1 的积极模式中实施了此攻击,并得到一个弱的 IKE SA.当发起者使用“协商”的弱密钥时,攻击者可对密钥进行穷举搜索.一旦破解了,攻击者可佯装成响应者而与发起者共同“协商”IPSec SA.

3 结束语

IKE 协议目前面临的最大的问题是过于复杂,这可能会导致二义性、矛盾、低效和漏洞等诸多安全问题.因此对其进行严格的安全性分析是十分必要的.但由于过于复杂,现有的安全协议分析工具很难直接应用到其中.因此必须通过减少 IKE 协议选项和提高模块化程度来降低其复杂性,同时对现有安全协议分析工具进行改进,以适应 IKE 协议安全性分析的需要[4].

致谢 中国科学院研究生院信息安全国家重点实验室的冯登国研究员对本文的工作给予了细心的指导,《软件学报》的编辑们对本文提出了很多有益的建议,在此一并表示感谢.

References:

[1] Meadows C. Analyzing formal methods to the analysis of a key management protocol. Journal of Computer Security-ESORICS 96, Springer-Verlag, 1996. 365~384.

[2] Borella MS, Grabelsky JLD, Montenegro G. Realm specific IP: framework. Internet Draft draft-ietf-nat-rsip-framework-03.txt, 1999.

[3] Harkins D, Carrel D. The Internet key exchange (IKE). Internet RFC 2409, 1998.

[4] Meadows C. Analysis of the Internet key exchange protocol using the NRL protocol analyzer. In: Proceedings of the 1999 Symposium on Security and Privacy. IEEE Computer Society Press, 1999. 287~305.