激进模式下对IKEv1的中间人攻击分析

周 梦，白建荣

(北京航空航天大学教育部信息、计算与行为重点实验室 北京 海淀区 100083)

【摘要】分析了对IKEv1的一种中间人攻击方法，该方法基于IKEv1密钥交换在预共享密钥认证机制下的激进模式。实施中间人攻击的步骤是首先利用IKEv1的离线口令穷举获取预共享密钥，获得预共享密钥后，把Diffie-Hellman(DH)中间人攻击原理应用于IKEv1的激进模式，实现对IKEv1的中间人攻击。通过分析该模式的中间人攻击原理，得出了对IKEv1的激进模式进行中间人攻击的条件、实施方法并评估了其对IPsec的危害性。由于该模式存在用户名枚举漏洞，攻击者可以离线穷尽预共享密钥，在现实中IKE中间人攻击的威胁是存在的，建议在使用IPsec VPN时不使用激进模式的密钥协商，并加强中间路由器的安全防护。

关 键 词 密码体制； IKEv1协议； 中间人攻击； 信息安全

中图分类号 TP393.08 **文献标识码** A doi:10.3969/j.issn.1001-0548.2010.01.022

Analysis to Man-in-the-Middle Attack for IKEv1 on the Aggressive Mode

ZHOU Meng and BAI Jian-rong

(Laboratory in Mathematics, Information and Behaviour of the Ministry of Education,
Beijing University of Aeronautics and Astronautics Haidian Beijing 100083)

Abstract In the paper a method of man-in-the middle attack to IKEv1 is discussed and analyzed is based on the aggressive mode of IKEv1 key exchange with pre-share-key authentication. The conditions and implementing methods of the attack are obtained by analyzing the principle of the attack to IKEv1 on the mode. For implementing man-in-the middle attack, the pre-share-key is first achieved by exhaustion method with offline password of IKEv1. The theory of Diffie-Hellman (DH) man-in-the middle attack to applied to the aggressive mode of IKEv1. Because there are some offline password leaks in the mode for obtaining pre-share-key, the conclusion is that the attack would jeopardize IPsec VPN in practice.

Key words cryptography; IKEv1 protocol; man-in-the-middle attack; security of data

IPsec是IPv6的必备协议，从问世以来其安全性就引起了学术界的关注，而IKE作为IPsec的密钥协商协议，其安全性更备受关注[1]。IKE协议在1998年发布了第一版[2](RFC 2409，简称IKEv1)，2005年发布了第二版(RFC 4307)。到目前为止，对IKEv1的研究已经发现了诸多问题[3-7]，如用户名枚举漏洞、离线预共享密钥穷举等。IKEv1易受到中间人攻击也是学术界公认的，在RFC 2409的“安全考虑”中对该问题有简要描述。近年来对各种中间人攻击方法的研究不断出现[8-11]。但是，一直以来，IKEv1的中间人攻击需要哪些条件，如何实施，对IPsec的安全威胁性有多大，这些问题并不明确。本文针对这些问题，分析对IKEv1预共享密钥认证下激进模式的中间人攻击原理，得出对IKEv1的这种模式进行中间人攻击的条件、实施方法，并评估对IPsec的危害性。

1 IKEv1

1.1 简介

IKEv1安全协商主要分为两个阶段。第一阶段是协商相关的安全参数(包括使用的加密算法、Hash算法、密钥长度、密钥等)，建立一个共享的密钥(用于建立保护第二阶段协商的数据加密密钥)，认证对等方的身份；第二阶段是协商建立数据加密所需的安全参数。

IKE协议安全协商模式主要有四种：主模式、激进模式、快速模式和新组模式。其中主模式和激进

收稿日期：2008－08－08； 修回日期：2008－12－05
基金项目：国家自然科学基金(10871017)；北京市自然科学基金(102026)
作者简介：周 梦(1958－)，男，博士，教授，主要从事网络信息安全等方面的研究.

模式用于第一阶段的安全参数协商，快速模式用于第二阶段，新组模式用在第一阶段协商之后，它协助建立的新组可以用于将来的安全协商。主模式和激进模式都支持三种基本的认证机制，分别为签名认证、公钥加密认证和预共享密钥认证。

本文假定协商都使用预共享密钥认证，第一阶段使用激进模式，第二阶段使用快速模式，攻击方已知被攻击方的ID信息。文中的术语可参考RFC 2409[2]术语说明，载荷类型及含义可参考RFC 2408[1]。

1.2 安全参数协商过程

下面介绍IKEv1在假定条件下进行安全参数协商的过程。

IKEv1第一阶段过程如图1所示。

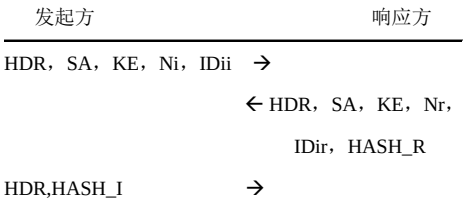

图1 激进模式协商过程

根据IKE协议，在预共享密钥认证的方式下，信息串SKEYID值计算方法为：

$$\mathrm{SKEYID}=\mathrm{prf}(\mathrm{psk},\mathrm{Ni\_b}\,|\,\mathrm{Nr\_b}) \tag{1}$$

式中 psk表示预共享密钥。

密钥材料计算方法为：

$$\mathrm{SKEYID\_d}=\mathrm{prf}(\mathrm{SKEYID},g^{xy}\,|\,\mathrm{CKY}-I\,|\,\mathrm{CKY}-R\,|\,0) \tag{2}$$

$$\mathrm{SKEYID\_a}=\mathrm{prf}(\mathrm{SKEYID},\mathrm{SKEYID\_d}\,|\,g^{xy}\,|\,\mathrm{CKY}-I\,|\,\mathrm{CKY}-R\,|\,1) \tag{3}$$

$$\mathrm{SKEYID\_e}=\mathrm{prf}(\mathrm{SKEYID},\mathrm{SKEYID\_a}\,|\,g^{xy}\mathrm{CKY}-I\,|\,\mathrm{CKY}-R\,|\,2) \tag{4}$$

在安全协商中，为了认证密钥交换信息，发起方产生HASH_I，响应方产生HASH_R，这两个值的计算方法为：

$$\mathrm{HASH\_I}=\mathrm{prf}(\mathrm{SKEYID},g^{xi}\,|\,g^{xr}\,|\,\mathrm{CKY}-I\,|\,\mathrm{CKY}-R\,|\,\mathrm{SAi\_b}\,|\,\mathrm{IDii\_b}) \tag{5}$$

$$\mathrm{HASH\_R}=\mathrm{prf}(\mathrm{SKEYID},g^{xr}\,|\,g^{xi}\,|\,\mathrm{CKY}-R\,|\,\mathrm{CKY}-I\,|\,\mathrm{SAi\_b}\,|\,\mathrm{IDir\_b}) \tag{6}$$

完成第一阶段协商后，通信双方获得了保护第二阶段密钥交换的ISAKMP SA参数(包括加密算法、hash函数等参数)，通过计算获得g^{xy}，进而根据式(2)～式(4)获得密钥材料SKEYID_d、SKEYID_a、SKEYID_e。第二阶段密钥协商在第一阶段协商获得的SKEYID_e及相关的SA保护下使用快速模式，快速模式交换过程如图2所示。

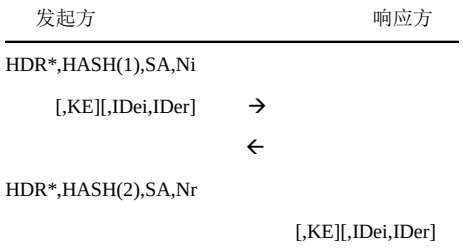

图2 快速模式协商过程

图中：

$$\mathrm{HASH(1)}=\mathrm{prf}(\mathrm{SKEYID\_a},M-\mathrm{ID}\,|\,\mathrm{SA}\,|\,\mathrm{Ni}[\,|\,\mathrm{KE}][\,|\,\mathrm{IDci}\,|\,\mathrm{IDcr}]) \tag{7}$$

$$\mathrm{HASH(2)}=\mathrm{prf}(\mathrm{SKEYID\_a},M-\mathrm{ID}\,|\,\mathrm{Ni\_b}\,|\,\mathrm{SA}\,|\,\mathrm{Nr}[\,|\,\mathrm{KE}][\,|\,\mathrm{IDci}\,|\,\mathrm{IDcr}]) \tag{8}$$

$$\mathrm{HASH(3)}=\mathrm{prf}(\mathrm{SKEYID\_a},0\,|\,M-\mathrm{ID}\,|\,\mathrm{Ni\_b}\,|\,\mathrm{Nr\_b}) \tag{9}$$

如果不需要PFS，且KE有效负载没有交换，则新的密钥材料定义为：

$$\mathrm{KEYMAT}=\mathrm{prf}(\mathrm{SKEYID\_d},\mathrm{protocol}\,|\,\mathrm{SPI}\,|\,\mathrm{Ni\_b}\,|\,\mathrm{Nr\_b}) \tag{10}$$

如果需要PFS，且KE有效负载已交换，则新的密钥材料定义为：

$$\mathrm{KEYMAT}=\mathrm{prf}(\mathrm{SKEYID\_d},g(\mathrm{qm})^{xy}\,|\,\mathrm{protocol}|\mathrm{SPI}|\mathrm{Ni\_b}|\mathrm{Nr\_b}) \tag{11}$$

式中 $g(\mathrm{qm})^{xy}$是共享秘密，来自于该快速模式的临时DH交换；“protocol”和“SPI”都取自ISAKMP[1]建议有效负载。

完成第二阶段密钥协商后，获得了SA参数，根据式(10)或式(11)就可以计算出数据加密使用的密钥材料KEYMAT。

2 IKE中间人攻击原理

IKE安全协商主要使用Diffie-Hellman密钥交换体制，因而对IKE的中间人攻击，主要是对Diffie-Hellman密钥交换体制进行中间人攻击。而IKE协议本身存在的漏洞或缺陷为实现DH的中间人攻击提供了一些基本条件。

2.1 DH中间人攻击

DH密钥交换体制很容易受到中间人攻击，因为通信双方Alice和Bob发出的消息中不存在消息的完整性确认信息，所以接收方无法确认消息是否被篡改，因而通信第三方Mallory就可以冒充合法通信方Alice或Bob。如果Mallory可以截取Alice和Bob之间的通信消息，Mallory就可以以中间人的方式同时与Alice和Bob进行通信。具体操作过程如图3所示。

Alice		Mallory		Bob
(g,x)	→	(g,x',y',g^{x})	→	$(g,y,g^{x'})$
$(g,x,g^{y'})$	←	(g,x',y',g^{x},g^{y})	←	$(g,y,g^{x'})$

图3　DH中间人攻击

(1) Alice发送g^x给Bob，但中途被Mallory截获，Mallory篡改g^x，用$g^{x'}$代替g^x转发给Bob；(2) Bob收到$g^{x'}$后，认定消息源于Alice；(3) Bob用g^y回应Alice，g^y发送过程中，又被Mallory截获，Mallory用$g^{y'}$代替g^y发送给Alice；(4) Alice收到$g^{y'}$后，认定消息源于Bob。

至此，DH密钥交换过程完成，Alice生成密钥$g^{xy'}$，Bob生成密钥$g^{x'y}$，而Mallory生成密钥$g^{xy'}$和$g^{x'y}$。

总结上述过程，实现DH中间人攻击必须具有两个先决条件：(1) 通信消息无完整性验证，第三方可以篡改截取的消息，冒充通信中的某一方，而不被被攻击对象发现。(2) 攻击者必须位于正常通信双方的信息通过的中间节点，能够进行信息存储转发。

2.2　IKE预共享密钥攻击

根据假定，攻击方已知通信中的ID内容，因而他可以进行预共享密钥的攻击，过程如图4所示。

发起方(Mallory)		响应方(Bob)
HDR,SA,KE,Ni,IDii	→	
	←	HDR,SA,KE,Nr, IDir,HASH_R

图4　激进模式预共享密钥攻击过程

Mallory冒充合法用户发起激进模式的安全协商，他发送的消息内容包括：CKY-I、SAi_b、g^{xi}、Ni_b、IDii_b；Bob接收到消息后，响应的消息内容包括：CKY-R、SAi_b、g^{xr}、Nr_b、IDir_b与HASH_R。Mallory接收到Bob的响应消息后，因为Mallory没有Bob的预共享密钥，他只能终止通信。由于假定攻击者已知被攻击方的IDii和IDir。根据式(1)和式(6)，可推出：

$$\text{HASH\_R}=\frac{\text{prf(prf(psk,Ni\_b|Nr\_b)},g^{xr}\mid g^{xi}}{\mid\text{CKY-R|CKY-I|SAi\_b|IDir\_b)}} \quad (12)$$

到此，Mallory知道了式(12)中除psk的所有其他参数，因而可以离线穷尽获取Bob的psk。

总结上述过程，可以得到以下结论：

(1) 对预共享密钥的离线穷尽是针对激进模式的密钥交换。(2) 离线穷尽预共享密钥，必须要知道被攻击方要求的身份识别信息。(3) 在预共享密钥体制下，通信双方具有相同的预共享密钥才能完成完整的通信协商。

2.3　IKE中间人攻击

在实施IKE中间人攻击之前，做如下假设：攻击者位于通信双方的中间路由节点；通信双方不对消息做完整性检测。

IKE中间人攻击过程如下：(1) 使用预共享密钥攻击获取psk。(2) 对第一阶段激进模式安全协商进行中间人攻击，获取保护第二阶段的密钥材料。过程如图5所示。

安全协商第一阶段

发起方(Alice)		中间方(Mallory)		响应方(Bob)
HDR,SA, KE(g^x),Ni,IDii	→			
		HDR,SA, KE($g^{x'}$),Ni,IDii	→	
			←	HDR,SA,KE(g^y), Nr,IDir，HASH_R
	←	HDR,SA,KE($g^{y'}$), Nr,IDir，HASH_R′		
HDR,HASH_I	→			
		HDR,HASH_I’	→	

图5　对激进模式中间人攻击

图中，KE(g^t)表示包含g^t的密钥交换载荷，t属于$\{x,x',y,y'\}$。

通过这一阶段，攻击方Mallory获得Alice和Bob的DH值g^x与g^y，并用$g^{x'}$和$g^{y'}$冒充g^x与g^y发送给Bob和Alice，进而生成与Alice的DH共享秘密$g^{xy'}$，与Bob的共享秘密$g^{x'y}$。

在这一过程中，根据式(1)可以获得SKEYID，根据式(5)和式(6)，HASH_I′与HASH_R′的计算公式如下：

$$\text{HASH\_I}'=\frac{\text{prf}(\text{SKEYID},g^{x}\mid g^{y'}\mid\text{CKY}-I}{\mid\text{CKY}-R\mid\text{SAi\_b}\mid\text{IDii\_b})}$$

$$\text{HASH\_R}'=\frac{\text{prf(SKEYID},g^{y}\mid g^{x'}\mid\text{CK}Y-R}{\mid\text{CKY}-I\mid\text{SAi\_b|IDir\_b})}$$

根据式(2)～式(4)，可以计算出安全协商第一阶段Alice与Mallory的密钥材料为：

$$\text{SKEYID\_d}=\text{prf}(\text{SKEYID},g^{xy'}\mid\text{CKY}-I\mid\text{CKY}-R\mid 0)$$

$$\text{SKEYID\_a}=\text{prf}(\text{SKEYID},\text{SKEYID\_d}\mid g^{xy'}\mid\text{CKY}-I\mid\text{CKY}-R\mid 1)$$

$$\text{SKEYID\_e}=\text{prf}(\text{SKEYID},\text{SKEYID\_a}\mid g^{xy'}\mid\text{CKY}-I\mid\text{CKY}-R\mid 2)$$

Mallory与Bob的密钥材料为：

$$\text{SKEYID\_d}' = \text{prf}(\text{SKEYID}, g^{xy'} | \text{CKY}-I | \text{CKY}-R | 0)$$

$$\text{SKEYID\_a}' = \text{prf}(\text{SKEYID}, \text{SKEYID\_d} | g^{xy'} | \text{CKY}-I | \text{CKY}-R | 1)$$

$$\text{SKEYID\_e}' = \text{prf}(\text{SKEYID}, \text{SKEYID\_a} | g^{xy'} | \text{CKY}-I | \text{CKY}-R | 2)$$

(3) 对第二阶段快速模式安全协商实施中间人攻击。在此协商过程中数据是被密钥材料SKEYID_e和SKEYID_e′加密保护的，SKEYID_e保护Alice和Mallory之间的通信，SKEYID_e′保护Mallory和Bob之间的通信。Mallory作为中间方对接收到甲方(Alice或Bob)的数据先解密，解密之后对数据做修改，然后用与乙方(Bob或Alice)通信的密钥加密数据发送乙方，攻击过程如图6所示。

安全协商第二阶段

发起方(Alice)	中间方(Mallory)	响应方(Bob)
HDR*,HASH(1), SA,Ni[,KE(g^u)] [,IDei,IDer] →		
	HDR*,HASH(1'), SA,Ni[,KE($g^{u'}$)] [,IDei,IDer] →	
		← HDR*,HASH(2), SA,Nr[,KE(g^v)] [,IDei,IDer]
	← HDR*,HASH(2'), SA,Nr[,KE($g^{v'}$)] [,IDei,IDer]	
HDR*,HASH(3) →		
	HDR*,HASH(3') →	

图6 对快速模式中间人攻击

图中，KE(g^t)表示传输g^t的密钥交换载荷，t属于$\{u,u',v,v'\}$。

通过协商，如果需要PFS，则Mallory可获得与Alice和Bob的第二阶段DH共享秘密信息$g^{uv'}$和$g^{u'v}$，进而利用式(10)或式(11)可以生成与Alice的密钥材料KEYMAT，与Bob的密钥材料KEYMAT′。

至此，完成对IPsec预共享密钥的激进模式安全协商的中间人攻击。

3 结 论

IKE预共享密钥认证机制下的激进模式安全协商易受到中间人攻击。对IKEv1的这种模式进行中间人攻击的条件为：(1) 通信中的消息无完整性验证。(2) 存在并能够控制通信中具有存储转发功能的IKE协商中间节点。(3) 可以获取ID信息和预共享密钥。在实施方法上，由于标准IKE预共享密钥的激进模式安全协商存在用户名枚举漏洞和离线穷尽预共享密钥的问题，并且不对消息做完整性验证，而且通信过程一旦被第三方截取，由于数据明发，ID信息也可以很容易被获得，因而进行中间人攻击的关键在于发现和控制具有存储转发功能的IKE协商中间节点。该方法在理论上是可以实现的。

中间人攻击方法在现实中对IPsec的安全性的威胁在于：一些VPN厂商仍旧支持IKE预共享密钥的激进模式安全协商，而且不对协商的消息进行完整性检测。这些VPN存在用户名枚举漏洞，攻击者可以离线穷尽预共享密钥。一旦攻击者获取了用户名和预共享密钥，就为IKE的中间人攻击提供了前提条件。攻击者使用Arp欺骗或占据中间路由器的方式就可以实施IKE中间人攻击。本文的评估结论是：IKE中间人攻击的威胁是现实存在的，建议在使用IPsec VPN时不使用激进模式的密钥协商，并且在通信过程中加强中间路由器的安全防护，对通信消息进行防篡改设计。

参 考 文 献

[1] RFC 2408. Internet security association and key management protocol (ISAKMP)[S]. 1998.
[2] RFC 2409. The internet key exchange (IKE)[S]. 1998.
[3] HILLS R. Common VPN security flaws[J/OL]. [2008-05-16]. http://www.nta-monitor.com/.
[4] DIAB W B, TOHME S, BASSIL C. Critical VPN security analysis and new approach for securing voip communications over vpn networks[C]//The Third ACM International Workshop on Wireless Multimedia Networking and Performance Modeling (WmuNeP'07). Greece: ACM Press, 2007: 73-78.
[5] LIU Dong-xi, ZHANG Long, BAI Ying-cai. Two modifications on IKE protocol with pre-shared key authentication[J]. Journal of Shanghai Jiaotong University, 2003, E-8(2): 142-145.
[6] PATERSON K G. A cryptographic tour of the IPsec standards[J]. Information Security Technical Report, Elsevier, 2006, 11(2): 72-81.
[7] 张卫乐, 余 洋, 汤 隽, 等. IKE协议安全隐患分析与验证[J]. 计算机工程与设计, 2007, 28(12): 11-14.
ZHANG Wei-le, YU Yang, TANG Jun, et al. Analyses of security flaws of IKE and test[J]. Computer Engineering and Design, 2007, 28(12): 11-14.

(下转第151页)

的前提下，得到了圆形量子点直径为20 nm、量子点间距为10 nm和方形量子点边长为20 nm、间距为20 nm的情况下量子磁盘的表面磁场分布。从分布图中可以看到明显的周期信号，由于记录点的量子化使读信号明显增大，并且轨道之间信号的间隔也明显增加，最重要的是，由于记录点尺寸减小，记录密度大大增加。通过本文对磁场分布的计算，为量子磁盘的可行性研究提供了强有力的理论依据。

本文研究工作得到电子科技大学青年基金(10810301030JX05017)的资助，在此表示感谢。

参 考 文 献

[1] SATO K, MAEKAWA Y, MIZOGUCHI T, et al. In-plane orientation of hcp-Co nanograins on grooved substrate in hard disk media[J]. Journal of Applied Physics, 2008, 104(3): 033914.

[2] GUO Zi-zheng, XUAN Zhi-guo, ZHANG Yuan-sheng, et al. Research on the temperature stability of triangular ferromagnetic nanowire arrays using the damage spreading method[J].Acta Physica Sinica, 2008, 57 (10): 6571-6576.

[3] SCHILLAK P, CZAJKOWSKI G. Optical anisotropy of quantum disks in the external static magnetic field[J]. Acta Physica Polonica A, 2008, 114(5): 1349-1354.

[4] WU Kuo-ming, HORNG L, WANG Jia-feng, et al. Influence of asymmetry on vortex nucleation and annihilation in submicroscaled permalloy disk array[J]. Applied Physics Letters, 2008, 92: 262507.

[5] VAVASSORI P, BONANNI V, BUSATO A, et al. Static and dynamical properties of circular NiFe/Cu/Co nanodisks[J]. Journal of Applied Physics, 2008, 103(7): 07C512-07C512-3.

[6] BARTICEVIC Z, PACHECO M, DUQUE C, et al. Energy spectra of exciton states in disk-shaped GaAs-$Ga_{1-x}Al_xAs$ quantum dots under growth-direction magnetic fields[J]. European Physical Journal B, 2007, 56(4): 303-309.

[7] KRAUSS P R, CHOU S Y. Fabrication of planar quantum magnetic disk structure using electron beam lithography, reactive ion etching, and chemical mechanical polishing[J]. Journal of Vacuum Science & Technolgy B, 1995, 13(6): 2850-2852.

[8] SBIAA R, TAN E L, AUNG K O, et al. Material and layer design to overcome writing challenges in bit-patterned media[J]. IEEE Transactions on Magnetics, 2009, 45 (2): 828- 832.

[9] YANG Xiao-min, XU Yuan, LEE K, et al. Advanced lithography for bit patterned media[J]. IEEE Transactions on Magnetics, 2009, 45(2): 833-838.

编　辑　张　俊

(上接第100页)

[8] 于　泠, 陈　波, 肖军模, 等. 一种网络攻击路径重构方案[J]. 电子科技大学学报, 2006, 35(3): 392-395.
YU Ling, CHEN Bo, XIAO Jun-mo, et al. A scheme of reconstructing network attack path[J]. Journal of University of Electronic Science and Technology of China, 2006, 35(3): 392-395.

[9] 吴　劲, 张凤荔, 何兴高, 等. SIP安全机制研究[J]. 电子科技大学学报, 2007, 36(6): 1211-1214.
WU Jin, ZHANG Feng-li, HE Xing-gao, et al. Research on SIP security mechanism[J]. Journal of University of Electronic Science and Technology of China, 2007, 36(6): 1211-1214.

[10] PERLMAN R, KAUFMAN C. Key exchange in IPsec: Analysis of IKE[J]. IEEE Internet Computing, 2000, 4(6): 50-56.

[11] CRAMPTON J, LIM H W, PATERSON K G. What can identity-based cryptography offer to web services?[C]// Proceedings of the 5th ACM Workshop on SWS. Virginia, USA: ACM Press, 2007: 26-36.

编　辑　漆　蓉