第33卷 第17期 计 算 机 工 程 2007年9月
Vol.33 No.17 Computer Engineering September 2007
·安全技术· 文章编号：1000—3428(2007)17—0153—03 文献标识码：A 中图分类号：TP393

IKE协议的研究与改进

袁志勇[1,2]，熊惠林[1]，陈绵云[2]
(1. 武汉大学计算机学院，武汉 430079；2. 华中科技大学控制科学与工程系，武汉 430074)

摘 要：分析并指出了因特网密钥交换协议的安全漏洞和设计缺陷，提出了一种安全高效的密钥交换协议。对比现有的几种密钥交换协议，改进的协议具有更好的安全性、抗DoS攻击能力、较少的密钥交换时间和消息数。
关键词：因特网密钥交换；安全联盟；拒绝服务攻击；阶段；模式

Research and Improvement of Internet Key Exchange Protocol

YUAN Zhi-yong[1,2], XIONG Hui-lin[1], CHEN Mian-yun[2]
(1. School of Computer, Wuhan University, Wuhan 430079;
2. Dept. of Control Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074)

【Abstract】 This paper gives an analysis of Internet key exchange (IKE) protocol and identifies its security holes and design weaknesses and proposes an efficient and improved secure key exchange protocol. Compared with existing key exchange protocol, the proposed protocol is more secure, robust to DoS attacks and has less key exchange time and messages.
【Key words】 Internet key exchange (IKE); security association(SA); denial of service attack; phase; mode

因特网密钥交换协议是由IETF因特网工程任务组提出的为因特网协议安全(IPSec)服务的因特网密钥交换协议[1]，是在Oakley[2]协议和SKEME[3]协议的基础上发展而来的。密钥交换的重要性日益突出，但现有的版本仍然存在不足和安全漏洞，因而IKE协议只是作为RFC文档形式而提出，在业界并未形成标准。虽然很多研究者对IKE协议进行了研究分析[4]，并提出了一些代替IKE协议的改进方案，包括IKEv2[5]、JFK[6]等。但是这些改进方案同样存在诸多缺陷，如IKEv2协议由于其消息交换数不固定，增加了复杂性，易受DoS攻击；JFK协议则由于重复使用DH_{pp}(Diffie-Hellman公私密钥对)，破坏了其完美前向保密(PFS)属性。

1 IKE协议的分析

在Photuris[7]协议中，为了应对DoS攻击，cookie被首次提出来并被使用，其主体思想是在发起者证明其能够通过其声称的IP地址接收到信息之前，应答者不保存连接的状态，从而大大减少攻击者使用虚假的IP地址发起耗尽应答者CPU资源和内存资源的DoS攻击的机会。但是IKE协议没有很好地使用cookie，并不能阻止IP泛滥的DoS攻击，因为在IKE协议中，应答者在接收到消息1后立即保存了连接状态，所以一个非法的发起者能够使用虚假的IP地址发送SA请求来耗尽应答者的内存资源从而实现DoS攻击。同样，IKE协议易遭受到耗尽CPU资源DoS攻击，当发起者在消息3中发起大量的SA，而不发送对自己身份认证的消息5，那么应答者由于频繁计算DH值而耗尽CPU资源。

IKE协议的野蛮模式由3个消息组成，抗DoS攻击能力很脆弱。使用数字签名(DS)认证的野蛮模式将身份信息在交换消息的过程中以明文的形式传送，文献[5]中提出了将发起者和应答者的身份在消息2和消息3中用DH共享值g^xy mod p进行加密传送，以免将身份泄露给偷听者。另外，如果消息3在网络上丢失，那么发起者就会使用没有协商完成的SA持续一段时间向应答者发送数据。在公共密钥加密(PKE)认证模式下，必须假定发起者已经拥有应答者的公钥值，但是这在规模巨大的实际网络环境下是不可能的。

IKE协议认为在预共享密钥(PSK)模式下，通信双方的身份对于主动攻击者是保密的，但是在文献[5]中指出通信双方的身份实际被暴露给了偷听者。因为，当应答者接收到消息5后，无法知道发起者的身份和将要使用哪一个共享密钥。IKE协议通过将通信双方的身份与相应的IP地址绑定的方法来解决这个问题，这样，双方的身份就可以被偷听者截获。IKE协议在快速模式下很容易受到反射攻击，由于在通信的2个方向上都使用相同的加密密钥，因此攻击者只需要将消息中的IP地址改动后再发送回去。反射攻击导致发起者认为已经与应答者共享了2个SA，实际上没有共享SA。

IKE协议的设计存在着协议过于复杂和交换的消息数过多的缺陷。一个SA提议要么完全被接受要么完全被拒绝，发起者必须为每一个可能的加密或者认证算法组合生成1个SA，这就导致了大量的SA提议，另外，IKE协议通信双方要进行协商的参数数量也众多。IKE协议在阶段1的协商中可以分为8种不同的方式，包括：DS认证方式，PKE认证方式，修改后的PKE认证方式和PSK认证方式，每一种方式都分为主模式和野蛮模式[1]。这些都增加了协议的复杂性和消息交换数。IKE协议在cookie使用设计上也存在缺陷，在文献[5]中指出，2个不同的SA可能会拥有相同的cookie，这种情况下当使用cookie来认证SA时就会产生冲突。在隧道模式下可

基金项目：国防科技预研基金资助项目
作者简介：袁志勇(1963－)，男，副教授，主研方向：图像处理与模式识别，信息安全；熊惠林，硕士；陈绵云，教授、博士生导师
收稿日期：2006-09-26 **E-mail：**yzypcc@163.com

能会有多个发起者在使用同 1 个IP地址，当用户身份被隐藏时，应答者就无法知道发起者想要与哪个应答者进行通信。

2 改进的 IKE 协议

本文在 JFK 协议和 IKEv2 协议的基础上提出了一种改进的 IKE 协议。JFK 协议认为 IKE 协议规定的用 2 个阶段进行密钥协商是没有必要的，JFK 协议使用 1 个阶段进行密钥协商。在阶段 1 生成 SA 后，协商的加密和认证算法可以用来生成多个阶段 2 的 SA，而且更容易对现有 SA 重新生成密钥和传送控制/错误消息，从整体上提高了密钥交换的效率。因此，本文提出的改进 IKE 协议保留了 IKE 协议的 2 个阶段的密钥协商模式。

IKEv2 协议规定在每 1 个提议中，多于 1 个算法被提出对应于每 1 个使用目的，例如 3 个加密算法和 2 个认证算法的组合，这样应答者就可以从每一种应用类型中选用 1 个算法，从而避免了过多的提议组合。但这引起了另外一个问题，一个应用类型所使用的算法不能使用于另一个应用类型。改进的 IKE 协议提议算法为套件的形式，并且套件的组合都具有相同的安全级别，在协议中不出现具体的算法，只是使用指针指向事先设置好的算法套件(算法套件可以公开获得)，这就大大简化了 SA 载荷并减小了载荷的长度。

PFS使得协议具有更好的安全性，它是通过不同时期所使用的密钥保持彼此之间不相关来达到的，这样在IKE协议中就要求 1 个新的SA被协商后就需要进行 1 次DH值交换或者旧的SA中的密钥进行重新生成。但是重新生成DH值需要大量的计算资源，并且当需要进行大量的SA协商和重新计算密钥时很容易出现问题，例如遭受到DoS攻击或多个新连接请求同时到达。改进的IKE协议使用DH_{pp}堆栈在不破坏PFS的情况下很好地解决了这个问题，每当处理器空闲时使，就计算DH_{pp}值存放在堆栈中。当 1 个SA请求到达时，就从堆栈中取出 1 对DH_{pp}，如果这个SA协商成功，那么就从堆栈中删除刚刚使用的DH_{pp}，并重新计算 1 对DH_{pp}值并压入堆栈。如果SA协商失败，这个DH_{pp}值就可以不删除重新使用。这样新协议就避免了花费大量时间进行计算非法的连接请求和没有协商成功的SA的DH_{pp}值，从而提高了新协议密钥交换的效率和抗DoS攻击能力。

3 改进的 IKE 协议的消息交换

改进的 IKE 协议消息交换都是以包含有 cookie 的 ISAKMP(Internet security association key management protocol)头开始，如果交换的消息经过加密，则 HDR 中加密位置位。如果是在 DS 认证方式和 PSK 认证方式下，则发起者需要选择认证算法并猜测双方都支持的 DH 群。如果阶段 1 的 SA 协商好后，只需要 2 个消息就可以协商好阶段 2 的 SA。

3.1 DS 认证方式下

IKE协议交换由 6 个消息组成，应答者在消息 1 到达后就保存连接状态。新协议只由 4 个消息组成，应答者在接收到消息 3 时保存连接的状态，这相当于旧协议的消息 5(如图 1 所示，图中符号#表示为应答者保存连接状态)。 本文符号意义见文献[1]，其中，CRQ是证书请求；KErid是堆栈索引值。消息 1 中包括阶段 1 的SA提议，发起者的DH公钥值和现在时间 (nonce)。消息 2 包括应答者选择过的SA提议，应答者从预先计算好的DH_{pp}堆栈中取得的DH公钥值，DH_{pp}堆栈索引值KErid，nonce和一个高强度的cookie(如式(1)所示意)，其中，高强度的cookie被用来发送消息 2 后清除连接状态，并由应答者在接收到消息 3 后重新生成以进行确认。在式(1)中，本地密码S隔一段时间进行 1 次变换。KErid的使用减小了消息的长度，发起者不需要将整个DH公钥值发回，只需要发回 1 个索引值即可，另外，通过在cookie中加入新元素更好地阻止了重放攻击。在应答者接好到消息 2 后，就可以删除所有的连接状态。接收到 1 个重复的消息 1 相当于接收到 1 个新的消息 1。

$$CKY\text{-}R=prf(S,IP_i|IP_r|CKY\text{-}I|SAi1|SAr1|g^xi|g^xr|KErid|Ni\_b|Nr\_b) \quad (1)$$

其中，S 为本地密码；IP 为 IP 地址。

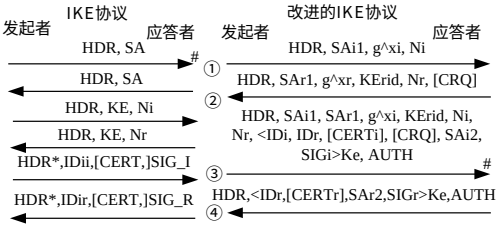

图 1 DS 认证下方式新旧协议对比

发起者在消息 3 中将把从应答者接收到的除DH公钥值以外的所有内容未加密地包括在其中，而其他内容都经过加密，包括：发起者的身份，应答者身份，发起者的证书，发起者对应答者的证书请求，阶段 2 SA提议和发起者的DS。整个消息通过AUTH进行认证。当应答者接收到消息 3 后，首先检查KErid是否正在被使用，如果未被使用过，那么就丢弃消息 3。如果使用过，那么就从DH_{pp}堆栈中取出相应的DH公钥值，并重新计算cookie值进行验证。如果cookie验证成功，应答者就继续计算DH共享密钥和所有其它需要的密钥信息。然后验证认证信息的合法性，并对加密的部分进行解密，验证发起者的DS。如果DS是合法的，应答者就发送经过加密的消息 4，包括：应答者的身份，证书，对阶段 2 提议进行选择后的SA和DS。消息 4 也用AUTH进行认证。以下公式是阶段 1 发起者计算出的密钥材料，应答者的密钥材料需要交换Ni_b和Nr_b、CKY-I和CKY-R的位置，其它应答者情况也同样处理。其中，SKEYID_x可以是SKEYID_a和SKEYID_e，取决于想要得到哪种密钥值。从K_{mat}中前面符合Ka和Ke长度的比特值中取出相应的比特值依次作为Ka和Ke。

$$SKEYID=prf(Ni\_b|Nr\_b,g^xy)$$

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

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

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

$$HASH=prf(SKEYID,g^xi|g^xr|Ni\_b|Nr\_b|CKY\text{-}I|CKY\text{-}R|SAi1|SAr1)$$

$$K_{mat}=K_1|K_2|K_3\ldots,K_1=prf(SKEYID\_x,0),K_2=prf(SKEYID\_x,K_1)\ldots$$

$$AUTH=prf(SKEYID\_a,message),SIG=Sig(HASH)$$

3.2 PSK 认证方式下

IKE 协议在 PSK 认证方式下在消息 5 才进行加密(图 2)，改进的 IKE 协议在消息 1 就用式(3)(应答者情况下将 CKY-R 替换为 CKY-I)生成的密钥 Ki 进行加密(其中，Kid 除外)。消息 1 中的加密部分包括：阶段 1 的提议 SA，发起者的 DH 公钥值和 nonce。Kid(式(2))用来标识正在使用的预共享密钥，每次协商新的 SA 就使用不同的 Kid 值。因为只有合法的发起者能够计算正确的 Kid 值，所以在 PSK 模式下无法发起 DoS 攻击。为了防止通信双方同时发送 SA 提议产生相同的 Kid，规定通信双方分别使用奇数和偶数作为 Kid 避免冲突。

$$Kid=prf(pre\text{-}shared\text{-}key,1),Kid=prf(pre\text{-}shared\text{-}key,2),\ldots \quad (2)$$

K_i=prf(pre-shared-key,IP_i|IP_r|CKY-R) (3)

SKEYID=prf(pre-shared-key,Ni_b|Nr_b|g^xy) (4)

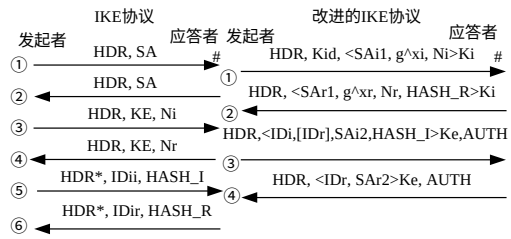

图 2　PSK 认证方式下新旧协议的对比

应答者接收到消息 1 后，变换Kid，保存连接状态并发出由Ki进行加密的消息 2，内容包括：经过应答者选择后的SA，DH_{pp}，nonce，对应答者进行认证并能够对SAi1 和SAr1 提供完整性保护的HASH_R，完整性保护可以避免应答者被欺骗而选择最弱的提议。发起者收到消息 2 后验证HASH_R并发出消息 3，消息 3 由DH共享密钥值所计算出来的密钥进行加密和认证，内容包括：发起者身份，应答者身份，阶段 2 的提议SA和对发起者进行认证的HASH_I。应答者接收到消息 3 后，对HASH_I和认证进行验证。消息 4 同样进行加密和认证，对应答者的身份和选择后的SA进行加密，SKEYID由式(4)进行计算，其他的密钥材料由式(1)进行　　计算。

3.3　PKE 认证方式下

在PKE模式下(图 3)，消息 1 包括阶段 1 的提议SA和DH群选项，应答者接收到消息 1 后选择 1 个提议和DH群，然后发送 1 个高强度的cookie(式(5))和应答者IP地址证书PK_g给发起者。应答者的IP地址是固定的，所以IP地址不保密。消息 3 包括提议SA和选择后的SA，用PK_g进行加密的发起者nonce，消息 3 的余下部分用对称密钥K_n进行加密，K_n是由发起者nonce计算而来(式(7)，对应答者Nr和CKY-R替换为Ni和CKY-I)。余下部分包括发起者的身份，DH公钥值，发起者的证书(可选项)，应答者身份，用应答者的公钥进行加密的第 2 个nonce(为可选项，当应答者的公钥是可以获得的而且发起者想要与直接协商密钥时)。消息 3 用密钥A_n进行认证(式(8)，对应答者Nr替换为Ni)。

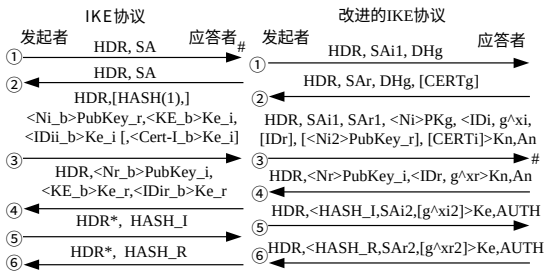

图 3　PKE 认证方式下新旧协议的对比

应答者接收到消息 3 后变换其cookie，保存连接状态并发送消息 4，消息 4 包括由PubKey_i进行加密的nonce。余下的消息是用对称密钥K_n进行加密，内容包括应答者身份和DH公钥值。消息 5 是由DH共享密钥值计算出来的密钥进行加密的，内容包括用于认证发起者的HASH_I，阶段 2 的提议SA和当阶段 2 SA需要PFS特性时包括的可选的DH公钥值。在DS和PSK模式下由于消息长度太大这个可选项并不存在。消息 6 与消息 5 类似，不同点在于消息 6 包括了选择后的SA。SKEYID根据式(6)计算出来，余下的密钥材料计算与 3.1 节的公式相同。

CKY-R=prf(S,IP_i|IP_r|CKY-I|SAi1|SAr1|Ni_b|Nr_b) (5)

SKEYID= prf(Ni_b|Nr_b,CKY-I|CKY-R|g^xy) (6)

Kn=prf(Nr,CKY-R) (7)

An=prf(Nr,message) (8)

4　改进的 IKE 协议的安全性分析

改进的IKE协议在DS和PKE模式下使用高强度的cookie来应对IP泛滥攻击。在PSK模式下，每 1 个接收到的消息 1 都必须有 1 个合法的Kid，所以IP泛滥攻击在这种模式下是无效的。新协议同样能够抵抗中间人DoS攻击，因为在发起者没有认证自己之前不需要应答者进行高强度地计算。IKE协议控制路由器的攻击者很容易就可以发起耗尽CPU资源攻击，攻击者发送消息 1，接收到应答后发送消息 3 让应答者计算DH共享密钥和所有的密钥材料只是为了验证发起者的合法性。攻击者使用不同的IP地址重复这种攻击使得应答者最后拒绝服务。改进的IKE协议可以抵抗这种攻击，因为应答者只有在从DH_{pp}堆栈中取出的DH_{pp}能够成功地协商SA时才重新计算DH_{pp}。由于每 1 次成功协商SA都是用的新的DH_{pp}，因此PFS没有受到损害。而JFK协议通过重复使用DH_{pp}值来应对这种攻击，所以PFS受到破坏。

改进的 IKE 协议中所有的 SA 都是单向的，因而可以应对反射攻击。另外，它使用消息计数器来区分应答者的请求，在协商过程中使用序列数区分不同的 SA。重放攻击可以使用高强度的 cookie 来解决，高强度 cookie 同样可以防止其他 3 种攻击：

(1)提供了消息 1 和消息 2 中最大域(包括 SAi1)的完整性保护，以避免受到欺骗应答者选择最弱的 SA 提议的攻击。

(2)通过频繁变换本地密码可以应对 cookie 冲突攻击。

(3)所有需要应答者重新计算 cookie 的域出现在消息 3 的前面，如果消息 3 被分段了，应答者可以首先从第 1 个分段中计算出 cookie，以确定是否需要等待消息 3 的余下分段。

改进的IKE协议在PSK模式下有很好的效率和安全性，发起者的消息 1 中使用Kid提供了低级别的认证，每当 1 个合法的Kid到达，应答者认为这很可能是 1 个合法的发起者，这样就充分利用了PSK认证的能力。在消息 1 和消息 2 中加密SA和g^xi提供了额外的安全性。新协议在不损害协议的安全性的情况下使用了最少的消息数，当应答者接收到消息 1 后，通过立即从DH_{pp}堆栈中取出DH_{pp}回复消息 2，具有更少的消息交换时间。而DH_{pp}堆栈是在处理器空闲时填充的。同时使用KErid和协议套件指针大大地减小了消息的长度。

5　结论

IKE 协议已经被广泛应用在 IPSec 中，在其他需要生成密钥的地方，也被用来进行密钥协商。本文对 IKE 协议进行了安全性分析，提出了较为全面的改进方案，使 IKE 协议更加安全、简单和高效。但是如何使 IKE 协议的安全性和复杂性达到最大的协调优化，还需要进一步研究。

参考文献

1 Harkins D, Carrel D. The Internet Key Exchange Protocol(IKE)[S]. RFC 2409, 1998.

(下转第 189 页)