第 34 卷 第 8 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.8 Computer Engineering April 2008
·安全技术· 文章编号：1000—3428(2008)08—0147—03 文献标识码：A 中图分类号：TP393.08

基于预共享密钥认证的 IKE 协议分析与改进

武 涛，郑雪峰，姚宣霞，李明祥
(北京科技大学信息工程学院，北京 100083)

摘 要：对基于预共享密钥认证的主模式 IKE 协议进行研究，针对其安全漏洞以及不支持移动用户的缺陷，提出相应的改进建议。该方案能及时发现并阻止中间人攻击和拒绝服务攻击，同时保护双方的身份，没有固定 IP 地址的限制。性能分析表明，该方案是安全、高效的。
关键词：IKE 协议；预共享密钥认证；主模式交换；IPSec 协议

Analysis and Modification of Internet Key Exchange Protocol Based on Pre-shared Key Authentication

WU Tao, ZHENG Xue-feng, YAO Xuan-xia, LI Ming-xiang
(School of Information and Engineering, University of Science and Technology Beijing, Beijing 100083)

【Abstract】The paper elaborates on IKE protocol with pre-shared Key authentication in main mode and puts forward corresponding advises to the potential secure flaws and the disadvantage of not supporting road warrior users. The proposed scheme can detect the attack quickly by authenticating the messages at once and prevent the identity of senders and receivers from being got by others, with no limitation to fixed IP address. It is secure, efficient and feasible.
【Key words】Internet Key Exchange(IKE) protocol; pre-shared key authentication; main mode exchange; IPSec protocol

IPSec 作为目前唯一的一种能为任何形式的通信提供安全保障的协议，近年来得到了广泛的应用。与其他安全协议一样，该协议基于密码学技术，其安全性依赖于密钥的安全，所以提供一个安全可靠的密钥管理机制是保证 IPSec 应用安全的关键。IKE 作为 IPSec 默认的密钥交换协议，在主机之间建立密钥和相关的安全参数，保护数据的传输安全，是 IPSec 中最为重要的部分。

1 IKE协议简介[1-2]

用 IPSec 保护一个 IP 包前，必须先建立一个安全联盟 SA，SA 可以手工创建或动态建立，IKE 的作用就是在 IPSec 通信双方之间动态建立安全联盟 SA。它是一个建立在 3 种协议(ISAKMP, Oakley, SKEME)之上的混合协议，IKE 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密钥生成技术，协商共享策略，验证交换信息以及动态更新密钥的方法。

IKE 的协商分两个独立的阶段进行，第一阶段有 2 种模式(具有身份保护并能协商大量属性的“主模式”和不具有身份保护且只能协商较少属性的“野蛮模式”)，第二阶段则只有“快速模式”。

在第一阶段，通信各方彼此间建立了一个已通过身份验证和安全保护的通道，即建立 IKE SA。第二阶段在 IKE SA 的保护之下为另一个不同的协议(比如 IPSec)协商安全服务，它的安全性建立在第一阶段的安全性之上。

IKE 协议的交换机制建立在 Diffie-Hellman 密钥交换算法的基础上。由于 Diffie-Hellman 交换容易受到“中间人”的攻击，为了防止中间人攻击，必须对通信双方的身份进行认证。主要的认证方式有以下 3 种：

(1)预共享密钥认证。通信双方通过带外机制创建一个共享密钥，并基于该密钥进行双方的身份认证。

(2)数字签名认证。通信双方利用自己的私钥加密特定的信息，并由对方利用相应的公钥解密，从而向对方证实自己的身份。

(3)公钥加密认证。通信双方利用对方的公钥加密特定的信息，并利用对方返回的私钥解密结果来验证对方的身份。

本文主要针对预共享密钥认证方式进行详细分析。

2 交换与认证过程[2]

如图 1 所示，通信的发起方和接收方之间共交换 6 条消息。消息(1)和消息(2)用于协商策略，消息(3)和消息(4)用于 DH交换，在第(4)条消息结束后，通信双方会根据各自计算的密钥值k(DH交换得到)及其他交换的参数生成 4 种秘密：*SKEYID*, *SKEYID_d*, *SKEYID_ a* 和 *SKEYID_e*。其中，*SKEYID*=*prf*(预共享密钥，$N_I|N_R$。其他 3 种秘密都建立在*SKEYID*的基础上：

$$SKEYID\_d=prf(SKEYID, k|C_I|C_R|0)$$
$$SKEYID\_a=prf(SKEYID, SKEYID\_d|k|C_I|C_R|1)$$
$$SKEYID\_e=prf(SKEYID, SKEYID\_a|k|C_I|C_R|2)$$

其中，*prf* 是在消息(1)和消息(2)中协商的伪随机函数；*SKEYID* 提供了用于生成实际所用密钥的原始信息；*SKEYID_ d* 用于为 IPSec SA 衍生加密材料；*SKEYID_ a* 是用来为 IKE 消息保障数据的完整性和对数据源的身份进行认证的密钥；*SKEYID_ e* 用于对 IKE 消息进行加密。用这些不同的密钥产生新的密钥材料、进行认证、加密的目的是为了使攻击者的破译更加困难。

作者简介：武 涛(1974－)，女，博士研究生，主研方向：网络安全；郑雪峰，博士生导师；姚宣霞、李明祥，讲师
收稿日期：2007-04-25 **E-mail：**wswutao@sina.com

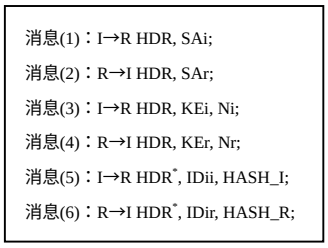

图 1　基于预共享密钥的主模式交换与认证过程

消息(5)和消息(6)负责对上述交换的认证，其中，

$HASH\_I=prf(SKEYID, X|Y|C_I|C_R|SA_I|, ID_I)$

$HASH\_R=prf(SKEYID, Y|X|C_R|C_I|SA_I|, ID_R)$

认证完成后，第 1 阶段交换结束，至此，已为第 2 阶段 IPSec SA 的协商建立了一个经过验证了的安全通道，即 IKE SA，同时也为 IPSec SA 提供了会话密钥材料。

3　协议的局限性及改进

3.1 局限性

协议的局限性主要包括以下 4 个方面：

(1)中间人攻击

由于 D-H 密钥交换容易遭受中间人的攻击，因此在最后一次交换过程中增加了对双方身份的认证来抵御中间人攻击。通信双方通过计算散列来认证对方的身份。但是，由于在散列的计算方法中存在的缺陷，仍不能避免针对 SA 的中间人攻击。

针对 SA 的中间人攻击分 2 种情况：

1)在第一次交换过程中，攻击者截获发送者发送给响应者的消息(1)，并且把 *SAi* 改为 *SAa*，然后让响应者从 *SAa* 中进行选择，一般来讲，*SAa* 的安全强度要比 *SAi* 低很多，这样就违背了响应者选择更高安全强度的初衷。因为没有立即对消息进行认证，这种最初的攻击直到最后集中认证时才能被发现。

2)在第一次交换过程中，攻击者截获响应者回应给发起者的消息(2)，并且把其中 *SAr* 改为 *SAb*。*SAb* 对 *SAr* 中所提供的保护套件进行修改，之后伪装为第 2 条消息发送给发起者，由于在最后一次交换进行验证计算散列摘要时，只用到了 *SAi* 进行验证，因此通信双方对于攻击者所做的修改可能完全不知情，并可顺利通过认证。当攻击者所提供的保护套件中的加密算法和散列算法与响应者的加密算法和散列算法不同的话，攻击可能不会成功，因为在计算 *HASH_I* 和 *HASH_R* 的时候会用到这些算法，但是如果攻击者只改变了 SA 的生存时间等在计算 *HASH_I* 和 *HASH_R* 时不会用到的安全属性时，那么上述的攻击可能会成功并且带来安全隐患，直到最后验证都不能发现。产生这种攻击的关键所在就是没有对 SAr 进行验证。

为了抵御中间人攻击并及时发现，文献[1]提出了在第 2 条消息中就对其进行认证并且要对 *SAi* 和 *SAr* 同时进行认证，同时对 *SAi* 和 *SAr* 进行验证虽然稍微增加了计算的工作量，但却提高了安全性。

(2)拒绝服务攻击

在 IKE 中，响应者要进行需要大量 CPU 时间的指数运算 *g^ab*，故可能会遭到 DoS 攻击。虽然，在设计之初，考虑到使用 cookie 来解决此问题，但 cookie 不能完全防止这类攻击，尤其是 DDoS 攻击。要从根本上防止 DoS 攻击，必须在进行指数运算之前先认证发送者的身份。

(3)不适用于没有固定 IP 的用户

从上面的讲述可以看出，*SKEYID_e* 必须在 ID 载荷交换之前使用，所以，对一个预共享的密钥来说，它只能建立在对方的 IP 地址的基础上，即只适用于具有固定 IP 地址的用户。这种要求给实际使用带来了很大的限制，那些不具有固定 IP 地址的用户都无法使用这种方式。

(4)双方的身份都不被保护

在这种认证方式中，预共享密钥的选取是基于双方的 IP 地址，这样，双方的身份都被泄露，简单的被动攻击都无法抵抗。

3.2　改进

针对以上缺点，本文对 IKE 协议进行了改进，图 2 为改进后的交换与认证过程。

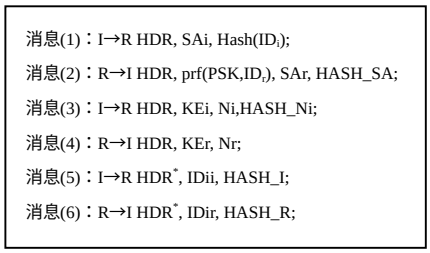

图 2　改进后基于预共享密钥的主模式交换与认证过程

改进的基本思想是[1]：(1)为了避免中间人攻击并及时发现，在消息(1)和消息(2)中及时对SA进行认证。(2)为了抵抗拒绝服务攻击，在进行计算量极大的指数运算之前，先进行简单的认证。(3)为了保护双方的身份，发送者首先需传送 $Hash(ID)$[3-4]向响应者表明自己的身份，响应者可根据发送者的身份($Hash(ID)$与ID的对应关系)选择相应的预共享密钥，计算$prf(PSK, ID_r)$[5]并回送，以便发送者识别响应方的身份，并能够选择同样的预共享密钥，计算出相同的*SKEYID*以及后续的一系列密钥。

改进以后的密钥材料及认证散列计算如下：

$SKEYID=prf(psk, C_I|C_R)$

$SKEYID\_d=prf(SKEYID, k|N_I|N_R|0)$

$SKEYID\_a=prf(SKEYID, SKEYID\_d|k|N_I|N_R|1)$

$SKEYID\_e=prf(SKEYID, SKEYID\_a|k|N_I|N_R|2)$

$HASH\_SA=prf(SKEYID, SAi\_b|SAr\_b)$

$HASH\_Ni=prf(SKEYID, Ni)$

$HASH\_I=prf(SKEYID, X|Y|IDii\_b)$

$HASH\_R=prf(SKEYID, Y|X|IDir\_b)$

其中，*prf* 是在消息(1)和消息(2)中协商的伪随机函数，采取密钥输入的 *Hash* 运算，通常是 HMAC-md5 或 HMAC-SHA。

具体协议描述如下：

消息(1)和消息(2)用于协商策略：消息(1)中发送*SAi*和$Hash(ID_i)$，响应者收到消息(1)后，首先根据$Hash(ID_i)$识别发送者的身份，然后根据发送者的身份选择相应的预共享的密钥，计算出$prf(PSK, ID_r)$, *SKEYID*, *HASH_SA*；消息(2)中发送$prf(PSK,ID_r)$, *SAr*, *HASH_SA*，发送者收到后，通过$prf(PSK,ID_r)$识别响应者的身份，然后选择对应的预共享密钥并计算出相应的*SKEYID*, *HASH_SA*，再与收到的*HASH_SA*相比较，如果不同，则表明发生了中间人攻击，中止操作。如果相同，通过验证，策略协商完成。

消息(3)和消息(4)用于交换 Diffie-Hellman 公开值(如*g*,*p*,*X*,*Y*)及用来防止“重放攻击”的与当前时间相关的随机数 Nonce：消息(3)发送 *KEi*, *Ni*, *HASH_Ni*，响应方收到后，通过

计算 *HASH_Ni* 对 *Ni* 进行验证，以防止拒绝服务攻击。验证通过后，再进行指数运算，发送 *KEr, Nr*。因为计算 *Hash* 的效率远远高于计算指数，所以，这样防止DDoS 攻击是有效可行的。

消息(5)和消息(6)负责对上述交换参数的认证以及身份的进一步确认。

实现中，可在安全策略数据库(SPD)中存放 2 个对应关系以提高效率。(1)*Hash*(*ID*)与 *ID* 的对应关系，*ID* 为自己的 *ID*，用于充当发送者时，首先表明自己的身份。(2)可根据协议所支持的 *prf* 算法的个数，对每个 *ID*(不同于本机的、可能与之通信的另外的 *ID*)，预先计算出一个或多个 *prf*(*PSK,ID*)，将之与 *ID*, *Hash*(*ID*)和 *PSK* 一起绑定并存放在安全策略数据库(SPD)中，即存放 *Hash*(*ID*), *ID*, *PSK*, *prf*(*PSK*, *ID*)的对应关系。用于在接收到 *Hash*(*ID*)或 *prf*(*PSK,ID*)时快速识别对方的身份。

改进后双方的身份可以不再必须为 IP 地址。取消了只适用于固定 IP 地址的限制。

4 改进方案的性能分析

(1)安全性。改进后的方案可以有效保护双方的身份不泄露。虽然$Hash(ID_i)$[4]在一定程度上会遭受到字典攻击，可以采取较长的*ID*来避免。$prf(PSK, ID_r)$[6]由于PSK的机密性以及*prf*的单向性，攻击者通过猜测*ID*并计算$prf(PSK, ID_r)$来验证是行不通的，也就有效避免了字典攻击的方式。

(2)性能。总体认证改为分步认证[1]，增加了$Hash(ID_i)$，*HASH_Ni*等的计算好像计算量增加，但是，从总体上来看，有效避免中间人攻击和拒绝服务攻击可以大大提高效率，及时发现攻击可以减少DH交换中计算量极大的指数运算，同时在消息(5)和消息(6)中的*HASH_I*和*HASH_R*的计算得以 简化。

从表 1 中可以看出，改进后的方案，既能适用于不具有固定 IP 地址的用户，保护了双方的身份；又能在攻击者发起进攻的初期有效遏制中间人攻击和拒绝服务攻击，大大提高了系统性能。

表 1 几种改进方案的对比

	文献[3]方案	文献[4]方案	文献[5]方案	文献[6]方案	本方案
改进方法	消息 3 中加入 *Hash*(*PSK*)	消息 3 中加入 *Hash*(*ID*)	更改 *SKEYID* 以及 *Hash* 生成方法，更改 *ID* 载荷	将集中认证改为分步认证，改变 *SKEYID* 的计算方法等	将集中认证改为分步认证，在消息(1)，消息(2)中加入识别身份的信息，并改变 *SKEYID* 的计算方法等
能否保护发送方身份	能	能	能	否	能
能否保护响应方身份	否	否	能	否	能
是否破坏协议对称性	是	是	否	是	是
攻击发现时间	晚	晚	晚	早	早

5 结束语

IKE协议由于其复杂性及存在的一些缺陷，使其应用受到了一定的限制，本文针对基于预共享密钥的认证方式进行了分析和改进，使得任何用户都可以采用基于预共享密钥认证的方式，而且能尽早避免中间人攻击和拒绝服务攻击[1]，保护了双方的身份，增加了协议的通用性及安全性。对于进一步的研究有一定的借鉴价值。

参考文献

[1] Maughham D, Schertler M. Internet Security Association and Key Management Protocol(ISAKMP)[S]. RFC 2408, 1998-11.

[2] Harkins D, Carrel D. The Internet Key Exchange(IKE)[S]. RFC2409, 1998-11.

[3] 韩秀玲. IPSec 的单播与多播密钥管理的研究[D]. 上海, 中国: 华东理工大学, 2003.

[4] Zhou Jianying. Further Analysis of the Internet Key Exchange Protocol[J]. Computer Communications, 2000, 23(17): 1606-1612.

[5] 卫剑钒, 唐礼勇, 陈 钟. IKE 协议两种身份保护缺陷的改进[J]. 计算机工程与应用, 2004, 40(26): 1997: 33-36.

[6] Liu Dongxi, Zhang Lianhua, Bai Yingcai. Two Modifications on IKE Protocol with Pre-shared Key Authentication[J]. 上海交通大学学报, 2003, E-8(2): 142-145.

(上接第 146 页)

从表 6 的统计结果可以看出，改进的字典法生成的隐密文本的各项常见指标都在自然文本的正常指标范围内，此外，隐密文本中高频次单词占文本单词总数的比例也在自然文本的正常范围内。这弥补了传统字典法的不足，能够抵抗一般的统计分析攻击，在很大程度上提高算法的安全性。

当然，改进后的算法在语法、语义上仍然与自然文本存在差异，从信息理解的层面来说仍然不够安全。这些有待以后更进一步的研究。但是，当用于隐蔽通信时，一般攻击者只是利用计算机来做分析，因而对简单的统计分析攻击而言，该方法是比较安全的。

5 结束语

本文在研究字典隐藏方法原理的基础上，通过对自然文本的建模分析，剖析了其隐密文本与普通自然文本的不同特征，证明了传统的字典法存在较大的脆弱性。文章根据这些脆弱性对用户字典加以改进，使得隐密文本与自然文本的常用统计特征并无明显差异，从而弥补了传统算法的缺陷，在统计特征上提高了算法的安全性。

参考文献

[1] Jensen C D. Fingerprinting Text in Logical Markup Languages[M]. Heidelberg, Berlin: Springer-Verlag, 2001: 433-445.

[2] EI-Kwae E A, Li Cheng. HIT: A New Approach for Hiding Multimedia Information in Text[C]//Proceedings of SPIE Security and Watermarking of Multimedia Contents IV. San Jose, CA: [s. n.], 2002.

[3] Chapman M, Davida G I. Hiding the Hidden: A Software System for Concealing Ciphertext as Innocuous Text[C]//Proc. of the 1st International Conference on Information and Communications Security. London, UK: Springer-Verlag. 1997: 335-343.

[4] Walker J. Stego Tool[EB/OL]. (2004-05-10). http://www.fourmilab.ch/.

[5] 周继军, 杨 著, 钮心忻. 文本信息隐藏检测算法研究[J]. 通信学报, 2004, 25(12): 97-101.

[6] Baeza-Yates R. 现代信息检索[M].. 北京: 机械工业出版社, 2005.

[7] 谢盛千. 概率论与数理统计[M]. 杭州: 浙江人民出版社, 2002.