第 17 卷第 3 期　　温 州 大 学 学 报　　2004 年 6 月
Vol 17, No 3　　Journal of Wenzhou University　　Jun, 2004

IKE 协议中存在的安全漏洞

肖　磊[1]，胡众义[2]

（1．温州大学现代教育技术中心；2．温州大学信息工程学院，浙江温州　325035）

摘　要：IKE (Internet key exchange)协议是 IPSec 协议中缺省的密钥管理协议，但是它的实现却相当复杂，所以可能出现安全漏洞．本文主要分析了 IKE 可能出现的一种安全漏洞．

关键词：网际密钥交换协议；密钥；数字签名

中图分类号：U491.13　　**文献标识码**：A　　**文章编号**：1008-309(2004)03-0036-10

IKE 协议是在 ISAKMP 定义的协议框架基础上建立的一种混合型密钥交换协议，是对安全服务进行协商的手段．它提供了 Oakley 和 SKEME 密钥交换技术，并且它还定义了自己的共享密钥交换技术[1]．IKE 是 IPSec 缺省的密钥管理协议，也是一个建立在 ISAKMP，Oakley 和 SKEME 三种协议上的一种混合协议，实质上是采用了 Diffle_Hellman 密钥交换算法，从而衍生出 IPSec 所需要的公共密钥．

一、Diffle_Hellman 密钥交换算法[2]

Diffle_Hellman 密钥交换算法的根本目的是为了允许两个主机产生和共享一个秘密密钥．该算法的工作过程如下：

(1) 首先，通信双方 A 和 B 协商一个大于 2 和“基准”的素数 p，一个小于 p 的整数 g；

(2) A 和 B 各自生成一个小于 p-1 的私有数据，分别为 xA 和 xB；

(3) 然后就可以得到公开密钥 yA 和 yB：

yA=g^xA mod p, yB=g^xB mod p

(4) 接着，A 和 B 相互交换公开密钥 yA 和 yB，然后将交换后的数转换为私有密钥 zA 和 zB：

zA=yA^xB mod p, zB=yB^xA mod p

这样，zA 和 zB 就可以作为 A 和 B 任意加密方法的秘密密钥，在 A 和 B 之间进行信息交换．

二、Diffle_Hellman 密钥交换算法存在的安全漏洞

Diffle_Hellman 密钥交换算法的安全性是基于有限范围内计算离散对数比计算指数更困难的理由设计的．但是 Diffle_Hellman 密钥交换算法却存在着一个最大的安全漏洞，就是无法抵挡中间人攻击（man_in_the_middle），由于参与密钥协议过程的通信双方没有办法来验证他们是否正与另一方进行通信．

中间人攻击的过程如下：

经过上图这样一个过程，发起方和接收方交换的信息都会被中间攻击人所截获并窃取，而发起方和接收方却对此可能并不知道．

收稿日期：2003 - 5 - 28

作者简介：肖磊(1977-)，男，浙江永嘉人，助教，学士，研究方向：计算机应用

发送方（I） 攻击人（A） 接收方（R）

p,g,g^x mod p -->

p,g,g^z mod p -->

<-- g^z mod p

<-- g^y mod p

三、IKE 协议中存在的安全漏洞

由于 IKE 协议中使用的是 Diffle_Hellman 密钥交换算法，所以也存在中间人的攻击．在 IKE 协议中，包括了两个阶段：第一个阶段，通信双方经过协商，建立经过认证和安全保护的安全联盟．该阶段包括两种工作模式，分别为主模式和野蛮模式；第二个阶段，就是在建立了的安全联盟的基础上，为 IPSec 协商具体的安全联盟．这个阶段使用快速模式[1].

IKE 协议的安全漏洞主要出现在第一阶段，虽然使用了数字签名，但依然可能会出现安全隐患．下面就以 IKE 中的预共享密钥认证方式的主模式密钥交换协议为例来说明这个安全漏洞．

预共享密钥认证方式的主模式 IKE 协议在第一阶段的工作过程如下：

发送方（I） 接收方（R）

（1）HDR, SA -->

<-- （2）HDR, SA

（3）HDR, KE, Ni -->

<-- （4）HDR, KE, Nr

（5）HDR*, IDii, [CERT,] SIG_I -->

<-- （6）HDR*, IDir, [CERT,] SIG_R

其中，HDR 表示 ISAKMP 消息头，HDR*表示 ISAKMP 消息中加密的载荷；SA 表示安全联盟载荷，其中可以包含多个提议载荷；KE 表示密钥交换载荷，包含在一次 Diffle_Hellman 交换中要交换的公开的参数；Ni 和 Nr 分别表示发送方和接收方 nonce 载荷；IDii 和 IDir 分别表示 ii 和 ir 的身份载荷；CERT 表示证书载荷；SIG_I 和 SIG_R 分别表示发送方和接收方的数字签名载荷．

在 IKE 协议上的中间人攻击使用了其他的方法一起使用，这个中间人攻击的过程如下：

(一) 首先，发送方发送消息（1），而中间攻击人截获该消息，这样他就知道了接收方的 IP 地址，然后他只是转发这个消息给接收方，并保留了这个消息的副本（攻击人每次都可以保留截获的消息副本）．接收方收到由攻击人转发来的消息（1）后，就发回一个带自己 SA 的消息（2），攻击人截获这个消息就知道了发送方的 IP 地址，此时，攻击人就假冒接收方发送一个消息把自己的 SA 发送给发送方．

(二) 然后，发送方发出消息（3），攻击人收到后就用发送方的 IP 地址假冒发送方将消息（3）发送给接收方，并在消息中使用自己的 Kei，接收方收到消息（3）后，发回消息（4）给攻击人，攻击人就用在消息（4）中用自己的 KEr 发给发送方，这样在发送方和攻击人，攻击人和接收人之间就建立了各自的秘密密钥和共享密钥，而发送方和接收方却以为是在他们之间建立的各自的秘密密钥和共享密钥，那么加密的信息也就可能被攻击人所解密而获取．

(三) 而后，发送方就发送带有数字签名 SIG_I 的消息（5）给攻击人，而此时攻击人保留这个消息的副本，并使用步骤（二）中和发送方协商好的密钥解密，用发送方公开的变换转换经签名的信息，就可以得到信息了．然后攻击人又将该信息（5）转发给接收人，接收人接着就发送带有数字签名 SIG_R 的消息（6）给攻击人，攻击人保留了副本后，用和接收方协商好的密钥解密信息，并用接收方公开的变换转换经签名的信息，这样信息也为攻击人所获取，然后攻击人把消息（6）转发给发送方．这个工作过程如下：

发送方（I） 攻击人（A） 接收方（R）

（1）HDR, SAi -->

（1’）HDR，SAi -->

（2）HDR, SAr

<-- （2’）HDR, SAr

（3）HDR, KEi, Ni -->

（3’）HDR, KEa, Ni -->

<-- （4）HDR, KEr, Nr

<-- （4’）HDR, KEa, Nr

（5）HDR*,IDii,[CERT,]SIG_I -->

（5’）HDR*, IDii,[CERT,]SIG_I -->

<--（6）HDR*,IDir,[CERT,]SIG_R

<--（6’）HDR*,IDir,[CERT,]SIG_R

序号带“’”的消息是攻击人发送的，或转发的.

在 IKE 协议中，虽然使用了数字签名来认证身份，但是在上述过程中攻击人只是相当于借用了发送方和接收方的数字签名，就像一个代理一样，而这些发送方和接收方却一无所知，即可以截获到通信双方的信息．即使攻击人对信息不做修改，这也是不安全的.

四、结束语

IKE 协议是 IPSec 协议中缺省的密钥管理协议，但是它的实现是比较复杂的，这也就带来了不安全的因素，上面分析了 IKE 协议中的一种可能的安全漏洞，所以要对 IKE 协议进行改进．目前，IETF 的安全专家推荐使用下一代 IKE 协议，称之为子 IKE 或 JFK（Just Fast Keying），作为 IKE 的替代品．总之，在 IKE 协议中，改进协议的密匙交换方法应该是进一步研究的重点问题之一，有待进一步的研究和改进.

参考文献

[1] Andrew S T. 计算机网络(第三版) [M]. 北京: 清华大学出版社, 2001

[2] [美] Marcus Goncalves (宋书民, 朱智强译). 防火墙技术指南[M]. 北京: 机械工业出版社, 2000

The Security Leak in the Internet Key Exchange (IKE)

XIAO Lei[1], HU Zhongyi[2]

(1. Modern Education And Technology Centre；2. College of Information Science and Engineering, Wenzhou University, Wenzhou, China 325035)

Abstract: The Internet key exchange (IKE) is the default ministration protocol of key in the IPSec. However, its implementation is very complicate. So it may be appear the security leak. This paper mainly assays a possible security leak in the IKE.

Key words: IKE; Key; DS (Digital Signature)