第 32 卷 第 19 期 计 算 机 工 程 2006 年 10 月
Vol.32 № 19 Computer Engineering October 2006
·安全技术· 文章编号：1000—3428(2006)19—0154—03 文献标识码：A 中图分类号：TP309

一种增加型的 IKE 协议签名认证

刘旭东，李占才，王 沁
(北京科技大学信息工程学院，北京 100083)

摘 要：由于 IKE 协议中签名认证方式易受中间人攻击，因此 IKE 协议存在用户 ID 泄漏的安全隐患。针对该问题，文章提出了一种隐藏用户 ID 的解决方案。此方案既保持了 ISAKMP 的框架结构又可以有效地抵御中间人攻击和暴力破解手段，而且付出的系统代价很小。此方案已被一款 IPSec 协处理器的设计所采纳。

关键词：Internet 密钥交换；中间人攻击；IPSec；信息安全

An Enhanced Internet Key Exchange Authentication with Signatures

LIU Xudong, LI Zhancai, WANG Qin
(School of Information Engineering, Beijing University of Science and Technology, Beijing 100083)

【Abstract】 Because Internet key exchange authentication with signatures is vulnerable to the man-in-the-middle attack, the user ID may expose to the outside in the IKE protocol. Aimeing at this issue, this paper proposes a solution to hide the user ID. This solution not only maintains the framework of ISAKMP but also resists the man-in-the-middle attack and brutal force attack effectively, with cheap system cost. This solution has already adopted by the design of an IPSec coprocessor.

【Key words】 Internet key exchange (IKE); Man-in-the-middle attack; IP security (IPSec); Information security

IPSec 协议是用来保护 Internet 信息安全的一组协议族。IKE 协议为通信双方动态协商 IPSec 加密保护所使用的算法和密钥素材。它需要完成两阶段工作：第 1 阶段用来协商保护 IKE 本身通信所使用的算法和密钥；第 2 阶段用来协商 AH(认证头)协议和 ESP(封装安全载荷)协议进行 IPSec 处理所使用的算法和密钥。

IKE协议是一个正在不断发展、完善的协议。IKEv1 与 IKEv2 版本分别于 1998 年和 2004 年正式发布。基于IKEv2 版本设计的IPSec协处理器应兼容已广泛存在的IKEv1 版本。然而，IKEv1 版本在密钥交换协商过程中会把用户ID泄漏出来，产生在IKEv1 第 1 阶段的主模式下签名认证方式中招致中间人攻击的安全问题。针对该问题有以下两类解决方案：一是将IKE第 1 阶段的响应方最后两条消息合并发送[4]，这样 IKE第 1 阶段只传递 5 条消息，破坏了ISAKMP(Internet安全关联与密钥管理协议)定义的框架结构，使消息传递失去对称性；二是将IKE第 1 阶段的最后两条消息中的ID载荷更改为 HASH(ID)[5]，但此方法又容易受到采用暴力猜测方式的“字典”攻击。为此，本文就IPSec协处理器实现IKEv1 版本之用户ID保护方法作一探讨。

针对上述改进方法的局限性，本文提出了一种既可以保持 ISAKMP 框架结构又可以抵抗字典攻击的签名认证方式的改进方案。

1 IKE 协议第 1 阶段简介

IKE协议[1]第 1 阶段协商ISAMKP SA(安全关联)，分为主模式和野蛮模式。其中主模式存在 6 次消息交换。IKE协议主模式下签名认证方式的工作原理如图 1。

在图 1 的消息 1 中，HDR 是 ISAKMP 头载荷，SAi 是 SA 协商载荷，其中包含着发起方支持的各种算法组合的建议。在消息 2 中的 SAr 中响应方表明了接受何种 SAi 中建议

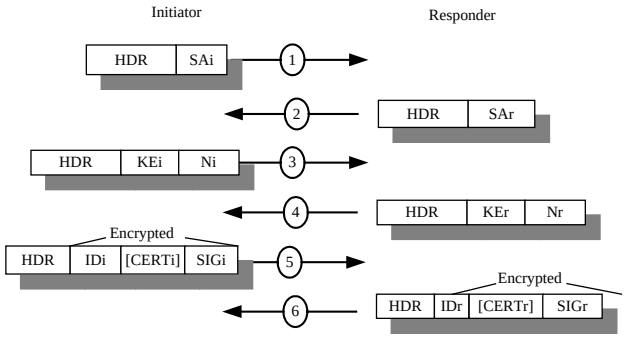

图 1 IKE 协议主模式下数字签名认证方式

的算法组合。通过消息 1、2，通信双方协商出第 1 阶段所使用的对称算法、认证算法等信息。消息 3、4 中的 KEi/KEr 载荷是双方交换的 Diffie-Hellman(D-H)共享密钥，Ni/Nr 是当前时间载荷。消息 5、6 中的 IDi/IDr 是用户 ID 载荷，SIGi/SIGr 是签名载荷；CERTi/CERTr 是证书载荷，在此认证方式下为可选项。消息 5、6 的作用是对 Diffie-Hellman 共享密钥双方进行身份认证。为了保护用户 ID 信息，消息 5、6 中除了 HDR 载荷外，其余载荷都使用在消息 1、2 中协商出的算法进行加密保护，密钥 SKEYID_e 由消息 3、4 交换的 Diffie-Hellman 密钥和 Ni/Nr 计算衍生得到。它的计算公式为

$$SKEYID\_sig = prf(Ni \mid Nr, g\hat{}xy) \quad (1)$$

$$SKEYID\_d = prf(SKEYID\_sig, g\hat{}xy \mid CKYi \mid CKYr \mid 0) \quad (2)$$

$$SKEYID\_a = prf(SKEYID\_sig, SKEYID\_d \mid g\hat{}xy \mid CKYi \mid CKYr \mid 1) \quad (3)$$

$$SKEYID\_e = prf(SKEYID\_sig, SKEYID\_a \mid g\hat{}xy \mid CKYi \mid CKYr \mid 2) \quad (4)$$

基金项目：国家科技部“863”计划立项及滚动基金资助项目(2003AA1Z1440，2005AA1Z1150)

作者简介：刘旭东(1981－)，男，硕士生，主研方向：信息安全和集成电路设计；李占才，博士、副教授；王 沁，教授、博导

收稿日期：2005-12-11 **E-mail：**liuxudongsm@163.com

其中：*prf(key,msg)*:伪随机函数，通常是一个带密钥的 HASH 函数。“|”：信息的串连，*“x^y ”*: x 的 y 次幂。*CKYi/CKYr*：ISAKMP 报头中 Cookie 域的内容。

IKE 第 1 阶段野蛮模式与主模式的不同在于，一共只有 3 次信息交换，基本不提供身份保护，即消息都是以明文的形式传输。图 2 表示了 IKE 第 1 阶段野蛮模式预共享密钥方式的工作情况。

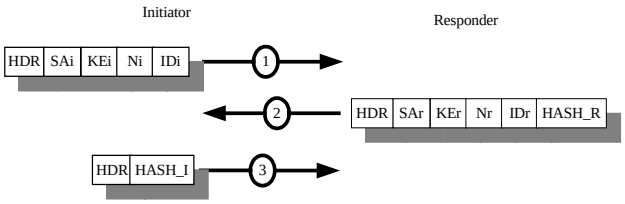

图 2　IKE 协议第 1 阶段野蛮模式的预共享密钥方式

$$HASH\_I = prf(SKEYID\_psk, g^{\wedge}x \mid g^{\wedge}y \mid CKYi \mid CKYr \mid SAi \mid IDi) \quad (5)$$

$$HASH\_R = prf(SKEYID\_psk, g^{\wedge}y \mid g^{\wedge}x \mid CKYr \mid CKYx \mid SAi \mid IDr) \quad (6)$$

$$SKEYID\ \_\ psk\ =\ prf\ (PSK\ ,Ni\ \mid Nr) \quad (7)$$

其中：*PSK*:预共享密钥。

由上面的描述可知，IKE 第 1 阶段主模式经历了协商算法、交换密钥和认证身份 3 个阶段，为后面第 2 阶段的协商提供了加密的算法和密钥素材。而野蛮模式使用较小的通信开销，完成了 IKE 第 1 阶段的功能，但所有的消息都是以明文形式传输，存在一定的风险。

2 IKE 协议主模式签名认证方式的漏洞分析

上文提到，IKE 第 1 阶段的消息 5 和 6 中的用户 ID 是以 SKEYID_e 为密钥，使用 SA 协商好的加密算法进行加密保护的，这样可以抵抗窃听等被动攻击。但是对于中间人攻击这种主动攻击方式就无能为力了。攻击者可以通过监听双方协商的 SA，更改 Diffie-Hellman 密钥的方式，窃取通信发起方的用户 ID 信息。进而攻击者利用窃取到的用户 ID，伪装成发起方，与响应方建立 IKE 第 1 阶段的野蛮方式通信，通过暴力破解的手段获得系统的预共享密钥，攻破整个系统。图 3 说明了中间人攻击的过程。

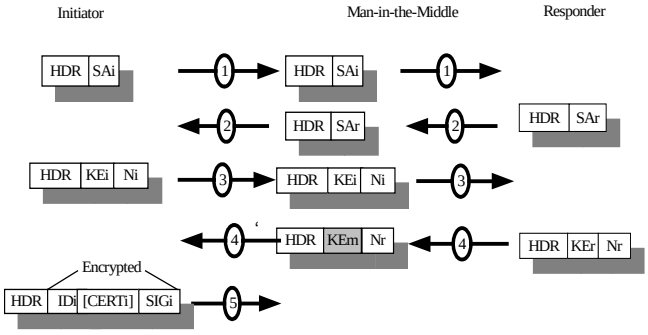

图 3　中间人攻击过程

假设攻击者对于通信双方的体系都有非常深入的了解，可以任意发起和阻断与通信双方的消息传递。攻击者通过在消息 4 传送过程中，阻断发起方和响应方的通信，篡改原 Diffie-Hellman 密钥交换信息，将其中的 KEr 换成自己计算出的 KEm，这样攻击者与发起方建立了 Diffie-Hellman 密钥对。因此根据式(1)~(4)，发起方所计算出的 SKEYID，以及由它衍生出的 SKEYID_d、SKEYID_a、SKEYID_e，攻击者也同样可以计算得到。当攻击者接收到消息 5，利用与发起方建立的密钥 SKEYID_e，解密获得 IDi。可见遭受这样的中间人攻击会导致发起方的用户 ID 泄漏。

在目前实现的VPN(虚拟专用网)网关中，发起方往往是VPN的用户，而响应方则是VPN服务器。攻击者通过上面的方式，得到了发起方的ID后，冒充发起方与响应方进行IKE第 1 阶段的野蛮模式预共享密钥方式的通信。由图 2 及式(6)、(7)可知，中间人可以获得由响应方回传的HASH_R，而HASH_R中又包含PSK信息，因此攻击者可以采用暴力破解的方式对PSK进行攻击，在有限的时间内可以获得VPN网关分配给原发起方(用户)的预共享密钥，从而成功进入VPN网络内部，使得整个系统完全暴露[2]。

目前可以统计到一些破解PSK工具的执行速度。表 1 表明了在AMD Athlon XP 2800+ 单CPU系统下不同复杂程度的密钥组合的暴力破解速度[2]。

表 1 单 CPU 系统下不同复杂程度的密钥组合的暴力破解速度

密码复杂度		可能的组合数	暴力破解时间
密码长度	符号范围		
6	a-z	309 000 000	16min
6	a-z,A-Z,0-9	57 000 000 000	2 天
8	a-z	209 000 000 000	8 天
8	a-z,A-Z,0-9	218 000 000 000 000	22 年

可见在应用 IKE 协议的 VPN 网关中，如果系统所采用的预共享密钥没有足够强壮的话，那么攻击者通过上述的中间人攻击，利用用户 ID 冒充发起方哄骗服务器获得包含 PSK 信息的 HASH_R，暴力破解获得 PSK 的方式，就可以成功突破 VPN 网关，使得系统内部机密完全暴露。所以这种攻击方式是有效而又极具威胁性的，因此对于用户 ID 的隐藏保护是非常必要的。

3 IKE 协议主模式签名认证方式的改进

为封堵安全漏洞，本文采用了对用户ID进行加密的方法。在SPD(安全策略数据库)中强制使用PSK域，使之变为SPD的必选项。PSK与目的IP地址、源IP地址相对应。对第 1 阶段消息 5、6 中的ID载荷，使用通信双方SA协商的对称加密算法进行加密，密钥由PSK衍生而成，衍生规则建议使用文献[1]附录B中的衍生算法。改进后的ID载荷记为$<ID>_{psk_k}$。

例如，假设通信双方协商的对称算法为 3DES 算法，使用的 prf 函数基于 MD5 算法。在消息 4 顺利传送后，通信双方都互相得知了 Diffie-Hellman 共享密钥，各自根据式(1)~(4)进行 SKEYID 密钥系统的计算。然后发起方在进行消息 5 组包的过程中，将 ID 载荷先进行一次 3DES 算法加密，使用的密钥由 PSK 衍生得到。因为 3DES 算法需要 3 个 64 位密钥，则根据下面的式(8)~(10)进行衍生。

$$psk\_k = k1 \mid k2 \quad (8)$$

$$k1 = prf\ (psk\ ,0) \quad (9)$$

$$k2 = prf\ (psk\ ,k1) \quad (10)$$

k1、k2 均为 128 位，psk_k为 256 位。截取psk_k的前 3 个 64 位作为 3DES算法的密钥进行加密运算。然后发起方再使用SKEYID_e对$<ID>_{psk_k}$和SIGi进行 3DES加密，组成消息 5 后传送给响应方。响应方则先使用SKEYID_e进行 3DES解密，再使用psk_k对IDi进行 3DES解密，使用得到的ID值计算SIGi，对IDi进行认证。若认证通过，则按照上述方法发送包含使用 3DES加密的IDr载荷的消息 6。发起方收到后，做同

样的双重 3DES解密处理。

在应用此改进方案的 IPSec 协处理器中，系统 SPD 库中还需增加一个标志位，用来表明是否使用此种改进方案。在执行IKE 协议读取SPD 库相应的安全策略时，检查此标志位。若为 1，则此次通信的 IKE 协议第 1 阶段采用上面描述的改进方案来完成 ISAKMP SA 的协商；若为 0，则此次通信就按照 IKEv1 标准协议的执行方式完成 IKE 第 1 阶段的协商。

4 改进方法的性能评价

若使用上述解决方案，可以弥补由于用户 ID 泄漏所引发的安全问题，保护正常的 IPSec 通信安全。下面从安全性、系统代价和通用性等方面就此改进方法作一评述。

(1)安全性方面

解决了用户 ID 泄漏问题。为量化分析，作如下准备：

1) 所有密码算法的安全性都取决于密钥的安全性，而不是基于算法细节的安全性[3]。

2) IKE协议中身份载荷有 11 种身份类型[1]，使用的字符和长度具有很强的随机性。

分析：当攻击者使用与发起方建立的密钥系统解密了消息 5 后，并不能直接得到IDi，而是得到$<IDi>_{PSK_K}$。根据 1)，$<IDi>_{PSK_K}$的安全性取决于PSK密钥的安全性。由于PSK对于中间人来说是私密信息，因此攻击者需要按照上文所描述的暴力破解的方法进行解密运算，所以攻击者同时猜测IDi和密钥PSK两个参数。根据 2)，假设IDi为 6 位字符，PSK为 4 位字符。表 3 说明了两种隐藏ID方法抵抗暴力破解的 能力。

表 2 两种改进方案暴力破解时间的比较

文献[5]方案			本文方案		
密码长度	符号范围	暴力破解时间	密码长度	符号范围	暴力破解时间
6	a-z	16min	10	a-z	14 年
6	a-z,A-Z,0-9	2 天	10	a-z,A-Z,0-9	82 707 年

结论：此种改进方案较之文献[5]大大增加了暴力破解的难度，有效地解决了用户 ID 泄漏的安全问题。

(2)系统代价方面

只需增加很少的系统资源。在 IPSec 协处理器的实现上应该尽可能完全支持 IKEv1 主模式的 4 种认证方式，因此 SPD 库中存在 PSK 域。使用 PSK 衍生出的密钥完成对 ID 信息的加密，是利用标准 IKE 实现中 SPD 的资源。为了硬件实现此改进方案，增加了一个标志位，只是为 SPD 库的每个策略项增加了 1bit。而按照文献[5]采用的方法，在 SPD 库中增加与 ID 对应的 HASH(ID)域，若采用 MD5 算法至少需要为 SPD 库每个策略项增加 128bit 的资源代价。相比之下，此方案资源代价很小。

由于改进后在IKE第 1 阶段最后一次消息交换时需要增加一次对称算法加解密运算，因此给系统运行增加了负担。在硬件实现上，RSA(D-H)大概比DES慢 1 000 倍[3]。粗略估算，设DES、HASH算法及AES算法执行时间为 1 个单位时间，则RSA签名和认证为 1 500 个单位时间，D-H算法为 1 000 个单位时间。整个系统修改前需完成一次IKE，第 1 阶段交换需要两次D-H运算，一次RSA签名和认证，一次密钥系统生成，一次对称算法加解密；本方案增加了一次对称算法的加解密和一次PSK密钥衍生过程。可以计算出改进后系统增加的额外时间占原来系统总时间的百分比：$(3510-3506)\div 3506\approx 0.11\%$，可见本方案带来系统延时负担完全可以忽略。

(3) 通用性方面

本文的改进方案在不破坏 ISAKMP 协议框架的条件下，通过在 SPD 库增加一个标志位，使系统可以支持标准 IKE 协议和改进 IKE 协议两种需求；加之对于体系完成过程中只需将最后两次消息传递做些调整，即可实现改进方案，因此具有很好的通用性(参见表 3)。

表 3 本文改进方案与其它集中改进方案的比较

方案 / 评价指标	文献[4]	文献[5]	本文
	将响应方最后两条消息合并发送	将 ID 改为 HASH(ID)	将ID改为$<IDi>_{PSK_K}$
安全性	保护发起方，泄漏响应方身份	易受到字典攻击	大大增加了字典攻击的难度
系统代价	无	依照系统支持的 HASH 算法预先计算若干 HASH(ID)，存储在 SPD 库中。	在 SPD 库中增加 1bit 的标志位；增加一次加解密和密钥衍生时间，占总时间的 0.11%
通用性	破坏 ISAKMP 框架结构，破坏消息传递的对称性	要求发起方身份长度较长	保持了 ISAKMP 框架结构和 IKE 协议的使用范围，不对发起方身份做特别的要求

5 结语

本文首先对 IKE 协议第 1 阶段的原理进行了描述。然后分析了攻击者如何使用中间人攻击，进而冒充发起方欺骗响应方，再通过暴力破解的手段获得系统的预共享密钥，最终攻破系统的整个过程。据此分析提出了一种通过加密的方法来隐藏用户 ID 的改进方案。此方案具有封堵了用户 ID 泄漏的安全漏洞，抵抗暴力破解攻击，只增加了极少的系统资源，几乎没有延误系统完成 IKE 协议的时间，具有非常好的通用性等优点。因此它可以在使用 IPSec 和 IKE 协议的系统中得到应用。目前它已在一款 IPSec 协处理器的设计中被采纳。

参考文献

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

2 Hills R. Common VPN Security Flaw[R]. NTA Monitor Ltd., 2005.

3 Schneier B. 应用密码学——协议、算法与 C 源程序[M]. 北京: 机械工业出版社, 2000.

4 Perlman R, Kaufman C. Analysis of the IPSec Key Exchange Standard[C]. Proceedings of the 10th IEEE International Workshops on WEI ICE, 2001: 150–156.

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): 33-36.