Internet 密钥交换协议的安全缺陷分析*

张 勇[1], 冯东雷[1], 陈涵生[2], 白英彩[1]

[1](上海交通大学 计算机科学与工程系,上海 200030);
[2](华东计算技术研究所,上海 201800)
E-mail: yzhang818@yahoo.com
http://www.sjtu.edu.cn

摘要: IKE(Internet key exchange,RFC2409)提供了一组 Internet 密钥交换协议,目的是在 IPSec(IP security)通信双方之间建立安全联盟和经过认证的密钥材料.随后有学者发现 IKE 协议存在一个安全缺陷,并给出相应的修改建议.指出了修改后的 IKE 协议仍然存在类似的安全缺陷,并描述了一个成功的攻击.在给出修改建议的同时,成功地利用 BAN 逻辑分析了导致这两个安全缺陷的原因.

关 键 词: Internet 密钥交换协议;安全联盟;认证;主模式;认证者
中图法分类号: TP393 文献标识码: A

IPSec(IP security)是一种协议套件,可以"无缝"地为 IP 引入安全特性,并为数据源提供身份验证、数据完整性检查以及数据机密性保护机制,可以防范数据受到来历不明的攻击.同时,IPSec 也是目前适用于所有 Internet 通信的惟一一种安全技术.

IPSec 提供的安全服务需要用到共享密钥,它是提供认证和机密性的基础.为了动态验证 IPSec 参与各方的身份,协商安全服务以及生成共享密钥等,IETF(Internet engineering task force)的 IPSec 工作组制定了 Internet 密钥交换协议[1].IKE(Internet key exchange)协议的目的是在 IPSec 通信双方之间建立安全联盟以及经过认证的密钥材料.

IKE 协议已被广泛地研究和应用.目前有多家公司推出了基于 IKE 的产品.但是,文献[2]指出了 IKE 协议存在的一个安全缺陷,并对 IKE 协议进行了修改.本文将指出,文献[2]的作者对 IKE 协议的修改并不完善,将会引起另一个类似的安全缺陷.两个安全缺陷都是由认证过程中使用的认证者的不完整性所造成的.

1 IKE 协议简介

IKE 利用 ISAKMP[3]语言描述了一种混合型协议,它建立在 ISAKMP 定义的框架上,提供了 Oakley[4]和 SKEME[5]密钥管理协议的一部分,同时还定义了自己的两种密钥交换技术.

IKE 协议分为两个阶段.第 1 阶段,通信双方建立经过认证和安全保护的通道,即协商 ISAKMP 安全联盟.该阶段有两种工作模式,包括主模式和野蛮模式.第 2 阶段,利用该 ISAKMP 安全联盟为 IPSec 安全协议协商具体的安全联盟,称为 IPSec SA.此阶段采用快速模式.

在通信双方之间建立安全通信的一个非常重要的步骤是认证对方的身份,未经过认证的 SA 和会话密钥不算是安全的.在 IKE 协议中,通信双方建立共享秘密的惟一方式是采用 Diffie-Hellman 交换.

Diffie-Hellman 密钥交换协议最大的缺陷是无法抵御中间人攻击(man-in-the-middle),其原因是参与密钥协

* 收稿日期: 2000-08-15; 修改日期: 2001-03-01

作者简介: 张勇(1971－),男,河南郑州人,博士生,主要研究领域为计算机网络安全,密码协议,网络管理;冯东雷(1972－),男,海南人,博士生,主要研究领域为分布式系统,协议工程;陈涵生(1938－),男,上海人,研究员,博士生导师,主要研究领域为软件工程,分布式系统,语言编译;白英彩(1936－),上海人,教授,博士生导师,主要研究领域为计算机网络及其应用.

商过程的通信双方没有办法来验证他们正与另一方进行会话.为了弥补 Diffie-Hellman 密钥交换协议的不足,在 IKE 协议中增加了对交换的共享秘密进行认证的步骤,同时对所建立的 ISAKMP SA 本身也进行认证.在 IKE 协议的第 1 个阶段中定义了 3 种认证方法:预共享密钥认证、数字签名认证和公钥加密 Nonce 认证.

2 IKE 协议安全缺陷分析

安全缺陷存在于 IKE 协议的第 1 阶段,包括主模式和野蛮模式,以及每种模式的 3 种认证方法.这里,我们选取采用预共享密钥认证方法的主模式协议来说明该安全缺陷.

主模式包括 3 个过程,双方交换 6 条消息.在第 1 个过程中的两条消息交换用于双方协商 ISAKMP SA;随后的两条消息交换 Diffie-Hellman 公开数字;最后两条消息认证 ISAKMP SA 和 Diffie-Hellman 交换.

I 表示发起方,R 表示响应方;HDR 表示 ISAKMP 头,HDR^*表示对载荷加密;SA_r 和 SA_i 表示安全联盟载荷;N_i 和 N_r 表示 Nonce 载荷;ID_{ii} 和 ID_{ir} 表示身份载荷; g^{x_r} 和 g^{x_i} 表示 Diffie-Hellman 公开数字.

假定 SA_i 包含发起方提供的两个提案 T#1 和 T#2,SA_r 包含响应方选择一个提案 T#1.假定 A 是攻击者,可以生成包含另一个提案 T#2 的 SA_a 攻击过程描述如下:

1. $I \to R: HDR_1, SA_i$,
2. $R \to A: HDR_2, SA_r$,

2′. $A \to I: HDR'_2, SA_a$,

3. $I \to R: HDR_3, KE_i, N_i$,
4. $R \to I: HDR_4, KE_r, N_r$,
5. $I \to R: HDR^*_5, ID_{ii}, HASH\_I$,
6. $R \to I: HDR^*_6, ID_{ir}, HASH\_R$.

攻击者截获响应方发送的第 2 条消息中的 SA_r,然后将自己生成的 SA_a 发送给发起方.在协议正常完成后,发起方相信已经和响应方建立了包含提案 T#2 的 ISAKMP SA,而响应方相信也已经和发起方建立了包含提案 T#1 的 ISAKMP SA.这个安全缺陷是由认证者 $HASH\_I$ 和 $HASH\_R$ 的错误定义引起的.

在文献[2]中,作者建议在 $HASH\_I$ 和 $HASH\_R$ 的生成方法中简单地用 SA_{r_b} 取代 SA_{i_b}:

$$HASH\_I = PRF(SKEYID, g^{x_i} | g^{x_r} | CKY\_I | CKY\_R | SA_{r\_b} | ID_{ii\_b}),$$
$$HASH\_R = PRF(SKEYID, g^{x_r} | g^{x_i} | CKY\_R | CKY\_I | SA_{r\_b} | ID_{ir\_b}).$$

这样,通信双方就可以明确地认证响应方选择作为 SA 的提案.

下面,我们将针对修改后的 IKE 协议给出一个新的攻击.假定 A 是攻击者,可以生成 SA_a,其中包含两个提案中的任意一个.不失一般性,这里假定是 T#2.新的攻击过程描述如下:

1. $I \to A: HDR_1, SA_i$,

1′. $A \to R: HDR'_1, SA_a$,

2. $R \to I: HDR_2, SA_r$,
3. $I \to R: HDR_3, KE_i, N_i$,
4. $R \to I: HDR_4, KE_r, N_r$,
5. $I \to R: HDR^*_5, ID_{ii}, HASH\_I$,
6. $R \to I: HDR^*_6, ID_{ir}, HASH\_R$.

在第 1 条消息中,攻击者截获发起方发送的 SA_i,然后将自己生成的 SA_a 发送给响应方.在协议正常完成后,通信双方都相信已经建立了包含提案 T#2 的 ISAKMP SA.无论发起方还是响应方都不会意识到攻击行为的存在.该攻击方法之所以成功,是因为在文献[2]中,作者简单地用 SA_{r_b} 取代 SA_{i_b},仅考虑了攻击者假冒响应方的情况,而没有考虑到攻击者同样可能假冒发起方.在我们新的攻击方法中,攻击者正是成功地假冒了发起方,使得响应方和发起方都不能发觉.

该攻击的危害性是很严重的.如果通信双方都打算利用 Triple-DES 作为加密算法,而不愿意为 DES 进行设置,那么攻击者就可以将一个“Triple-DES 或者 DES”请求修改为“单纯使用 DES”请求.作为响应方,尽管不愿意,

也别无选择.这样,在协议完成后,通信双方都不会意识到它们正以一种双方都不愿意而且安全强度低的方式进行通信,同时该方式将会被用作对阶段 2 的保护.

为了避免这种攻击,我们新的修改建议是对 *HASH_I* 和 *HASH_R* 进行更正:

$$HASH\_I = PRF(SKEYID, g^{x_i} \mid g^{x_r} \mid CKY\_I \mid CKY\_R \mid SA_{i\_b} \mid ID_{ii\_b}),$$

$$HASH\_R = PRF(SKEYID, g^{x_r} \mid g^{x_i} \mid CKY\_R \mid CKY\_I \mid SA_{r\_b} \mid ID_{ir\_b}).$$

既对发起方提出的待选择提案进行认证,也对响应方选择的提案进行认证.

3 IKE 协议的逻辑分析

目前,最著名的协议分析工具是基于广义模态逻辑中信任(belief)概念的 BAN 逻辑.BAN 逻辑中存在不完善之处,研究人员相继提出了一些对 BAN 逻辑的修改和扩展,但其缺点是没有原来的 BAN 逻辑简单、实用.下面,我们将利用 BAN 逻辑[6]对 IKE 协议和修改后的 IKE 协议进行形式化分析.

IKE 协议第 1 阶段的目的是在通信双方之间通过 Diffie-Hellman 交换建立共享秘密以及协商 ISAKMP SA.因此,利用 BAN 逻辑来分析协议的目标.

1. 协商 Diffie-Hellman 参数:

(g1.1) $I \mid\equiv I \xleftrightarrow{K} R$,

(g1.2) $R \mid\equiv I \xleftrightarrow{K} R$,

(g1.3) $I \mid\equiv R \mid\equiv I \xleftrightarrow{K} R$,

(g1.4) $R \mid\equiv I \mid\equiv I \xleftrightarrow{K} R$.

这是在协议中通信双方分别对所协商的会话密钥的两级信任关系.

2. 协商 SA:

(g2.1) $I \mid\equiv SA_r$,

(g2.2) $I \mid\equiv R \mid\equiv SA_r$,

(g2.3) $R \mid\equiv SA_i$,

(g2.4) $R \mid\equiv I \mid\equiv SA_i$.

类似地,对于所协商的安全联盟,通信双方也应有两级信任关系.

下面,利用主模式中的预共享密钥认证方式,对目标 2 进行逻辑推理,证明 IKE 协议和修改后的 IKE 协议存在安全缺陷,并论证我们提出的修改方案:

假定:

(1) $I \mid\equiv I \xleftrightarrow{K_{ir}} R$,

(2) $R \mid\equiv R \xleftrightarrow{K_{ir}} I$,

(3) $I \mid\equiv \#(K_i, N_i, SA_i)$,

(4) $R \mid\equiv \#(K_r, N_r, SA_r)$,

(5) $R \mid\equiv I \mid\Rightarrow SA_i$,

(6) $I \mid\equiv R \mid\Rightarrow SA_r$.

K_{ir} 是通信双方预共享密钥;K_i 和 K_r 是双方的 Diffie-Hellman 秘密参数;SA_i 和 SA_r 是双方协商的安全联盟;N_i 和 N_r 是双方生成的 Nonce.

逻辑推理:

由消息 6: $I \triangleleft \{ID_{ir}, HASH\_R\}_{K_{ir}}$.

又因为有 $I \mid\equiv I \xleftrightarrow{K_{ir}} R$,

所以,根据 Nonce 验证规则,可得:

$$I \mid\equiv R \mid\sim \{ID_{ir}, HASH\_R\}.$$

又根据传递规则,有

$$I \mid\equiv R \mid\sim HASH\_R, \quad ①$$

令 $HASH\_R = h(K,Y)$,K 表示 $SKEYID$,K 表示 $(g^{x_r} \mid g^{x_i} \mid CKY\_R \mid CKY\_I \mid SA_{r\_b} \mid ID_{ir\_b})$.

由假定(3)和新鲜性规则,有

$$I \mid\equiv \#(K), \quad I \mid\equiv \#h(K,Y). \quad ②$$

由①和②,根据 Nonce 验证规则,有

$$I \mid\equiv R \mid\equiv h(K,Y).$$

根据信任规则,有

$$I \mid\equiv R \mid\equiv SA_i.$$

由消息 5,同理可证:

$$R \mid\equiv I \mid\equiv SA_i.$$

由假定(5),根据权限规则,有

$$R \mid\equiv SA_i.$$

从逻辑推理得到的主体各自信任关系可以看出,在 IKE 协议中,主体 R 相信自己同通信对方协商的 SA_i(g2.3 和 g2.4);而不能得到主体 I 对所协商安全联盟 SA_r 的信任关系(g2.1 和 g2.2).这说明了 IKE 协议存在漏洞,通过逻辑分析可以看到攻击者有可能假冒响应方 R,和发起方 I 协商安全联盟.

在修改后的 IKE 协议中,由消息 5,可得

$$R \mid\equiv I \mid\equiv SA_r.$$

由消息 6,可得

$$I \mid\equiv R \mid\equiv SA_r.$$

由假定(6),根据权限规则,有

$$I \mid\equiv SA_r.$$

同样,仅仅可以得到主体 I 对所协商安全联盟 SA_r 的信任关系(g2.1 和 g2.2),而不能得到主体 R 对所协商安全联盟 SA_i 的信任关系(g2.3 和 g2.4).攻击者有可能假冒发起方 I 和响应方 R 协商安全联盟.

在我们提出的修改方案中,由消息 5,可得

$$R \mid\equiv I \mid\equiv SA_i \text{和} R \mid\equiv SA_i.$$

$I \mid\equiv R \mid\equiv SA_r$和$I \mid\equiv SA_r$ 由消息 6,可得

$$I \mid\equiv R \mid\equiv SA_r \text{和} I \mid\equiv SA_r.$$

满足 IKE 协议所要求的目标 2,防止了在协商安全联盟时,攻击者对双方的假冒.

4 结 论

通过对 IKE 协议和修改后的 IKE 协议的分析,我们发现了两个协议中都存在类似的安全缺陷,该缺陷存在于第 1 阶段的所有模式和认证方法中:

(1) 在原来的 IKE 协议中,无法防止假冒响应方的攻击者对安全联盟协商过程的攻击.因为在认证元素 $HASH\_I$ 和 $HASH\_R$ 中仅仅包含了发起方的 SA_{i_b}.

(2) 在修改的 IKE 协议中,无法防止假冒发起方的攻击者对安全联盟协商过程的攻击.因为在认证元素 $HASH\_I$ 和 $HASH\_R$ 中仅仅包含了响应方的 SA_{r_b}.

在 IKE 协议中,采用的认证方式是密钥交换过程结束之后的认证.因此,在认证过程之前的所有阶段以及协商好的参数应当都经过双方的有效认证.

通过分析 IKE 协议以及修改后的 IKE 协议,我们发现,对密码协议的任何微小改动都有可能导致协议出现新的安全漏洞.因此,通过严格的形式化方法来验证密码协议的安全性,以及透彻理解密码协议中安全机制运作原理非常重要.

References:

[1] Harkings, D., Carrel, D. The Internet key exchange (IKE). RFC 2409, 1998.

[2] Zhou, Jian-ying. Fixing of security flaw in IKE protocols. Electronics Letters, 1999,35(13):1072~1073.

[3] Maughan, D., Schertler, M., Schneider, M., *et al*. Internet Security Association and key management protocol (ISAKMP). RFC 2408, 1998.

[4] Orman, H. The Oakley key determination protocols. RFC2412, 1998.

[5] Krawczyk, H. SKEME: a versatile secure key exchange mechanism for Internet. In: IEEE ed. Proceedings of the 1996 Symposium on Network and Distributed System Security (SNDSS'96). 1996.

[6] Burrows, M., Abadi, M., Needham, R. A logic of authentication. ACM Transactions on Computer Systems, 1990,8(1):18~36.

Analyzing the Security Flaws of Internet Key Exchange Protocols*

ZHANG Yong[1], FENG Dong-lei[1], CHEN Han-sheng[2], BAI Ying-cai[1]

[1](*Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai* 200030, *China*);

[2](*East-China Research Institute of Computer Technology, Shanghai* 201800, *China*)

E-mail: yzhang818@yahoo.com

http://www.sjtu.edu.cn

Abstract: IKE (Internet key exchange, RFC2409) describes a suite of Internet key exchange protocols for establishing security associations and obtaining authenticated keying material. A security flaw in these IKE protocols is observed and a simple modification is proposed. In this paper, it is pointed out that there is a neglected security flaw in the amended IKE protocols. And a successful attack on the amended IKE protocols is also provided. A new amendment to IKE protocols is proposed, and the reasons which cause the two security flaws are analyzed by using BAN logic successfully.

Key words: Internet key exchange protocols; security association; authenticate; main mode; authenticators

* Received August 15, 2000; accepted March 1, 2001