文章编号:1001 - 9081(2005)03 - 0563 - 02

IKEv2 协议安全性分析与改进

高 翔,李亚敏,郭玉东,马红途
(信息工程大学 信息工程学院,河南 郑州 450002)
(ariesstar3@sina.com)

摘 要:简单介绍了新一版密钥交换协议草案 IKEv2,对 IKEv2 密钥协商机制的安全性进行分析。通过分析,发现其 EAP 交换过程繁琐且身份信息不易隐藏;证书验证中可能受到假冒证书攻击;为避免安全隧道非授权访问而需要重新认证等几处安全问题。针对这几处安全问题提出了改进建议和解决方法。

关键词:IKEv2;EAP;认证
中图分类号: TP393.08 **文献标识码**:A

Security analysis and improvements of IKEv2 protocol

GAO Xiang, LI Ya-min, GUO Yu-dong, MA Hong-tu
(*College of Information Engineering, Information Engineering University, Zhengzhou Henan* 450002, *China*)

Abstract: IETF put forward a new version of IKE, IKEv2. Different from the old IKE, IKEv2 combines and redefines key exchange process. This paper introduced IKEv2, and analysed the security of key negotiation mechanism of IKEv2. Aiming at some security problems in EAP exchange, such as authentication with digital certificate and reauthentication to avoid accessing VPN tunnel with unauthorized identity, some improvement advice and solutions were given.

Key words: IKEv2; EAP; authentication

0 引言

IKE(Internet Key Exchange)协议利用认证和加密机制,以及特有的密钥材料生成与共享密钥协商技术,能够动态地为 IPSec 协商建立和维护 SA(Security Association)。随着密钥交换的日益重要,IKE 协议已经成为 VPN、端 - 端安全等 IPSec 实现中的首选密钥交换协议。但由于它是一个混合型的协议,其自身的复杂性不可避免地带来一些安全及性能上的缺陷。IETF(Internet Engineering Task Force)一直在对现有版本 IKE 的不合理部分积极地征集修改意见。其 IPSec 工作组于 2004 年 5 月推出了最新一版的 IKE 协议草案——IKEv2,版本号是 2-14[1]。IKEv2 在沿用原有协议的共享策略协商方法的基础上,对第 1 版协议进行了全面的优化和改进,从而使之具有更高的性能、更好的安全性以及更低的系统耗费。以 IKEv2 取代 IKE 作为新一代的密钥交换协议标准已逐渐成为业内人士的共识。

由于 IKEv2 代替 IPSec 进行密钥协商管理的特殊地位,很多重要信息的传递都要依赖于 IKEv2 所建立的经过认证的安全信道,例如,加密算法、密钥信息等,因此 IKEv2 中对网络攻击进行了充分考虑并始终将安全性放在协议实施过程的首位。本文首先对 IKEv2 协议简单介绍;然后基于 IKEv2,对其安全性进行分析并提出改进建议。

1 IKEv2 简介

1.1 协议规范

IKEv2 简化和统一了 IKE 的协议规范。它用一个独立单一的文档 Internet Key Exchange (IKEv2) Protocol 定义完整的 IKE 协议,代替了原有密钥交换协议中 RFC2407 (IPSec DOI),RFC2408(ISAKMP)和 RFC2409 (IKE) 的内容,从而使以前 IKE 相关的策略和安全属性的定义分散于各处,缺乏一致性的问题得到了改善。同时,它删除了原有协议中的 DOI、SIT 以及域名标识符、提交位这些功能不强且难以理解容易混淆的数据结构。

1.2 交换类型

IKEv2 中定义了三种交换类型,分别是初始交换(Initial Exchanges)、协商子 SA 交换(CREATE_CHILD_SA Exchanges)和信息交换(Informational Exchanges)。

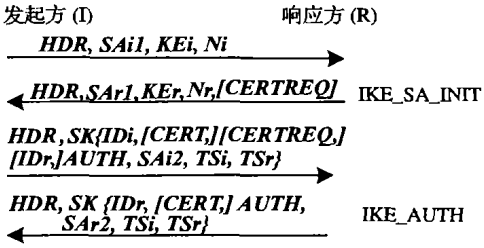


图 1 初始交换

1) 初始交换

初始交换实现了一版本中第一阶段和第二阶段所完成的功能,即建立 IKE SA 和 IPSec SA。它由四条消息组成,其中头两条消息被称作 IKE_SA_INIT 交换,主要进行密钥算法的协商、nonces 的交换以及一次 Diffie-Hellman 交换,从而生成用于加密和验证后续交换的密钥材料。后两条消息被称作 IKE_AUTH 交换,实现对前两条消息的验证,同时交换身份和

收稿日期:2004 - 08 - 23;修订日期:2004 - 10 - 29

作者简介:高翔(1975 -),女,河南郑州人,硕士研究生,主要研究方向:计算机网络安全; 李亚敏(1964 -),男,河南荥阳人,副教授,主要研究方向:计算机网络安全; 郭玉东(1964 -),男,河南太康人,教授,主要研究方向:计算机操作系统、网络安全; 马红途(1976 -),男,河北秦皇岛人,硕士研究生,主要研究方向:计算机并行编译.

证书信息,并建立第一个 IPSec SA,除消息头外,IKE_AUTH 交换中的消息都用前面生成的密钥材料进行了加密和完整性保护。初始交换的消息传递见图 1。

2) 协商子 SA 交换

这一过程可由通信中的任一方在初始交换完成之后发起,作为有额外的 IPSec SA 或完美向前保密(PFS)需求时的一种交换类型。该交换包含了两条消息。第一条消息发送 SA 提案,交换 nonce 和流量选择符 TSi 和 TSr;第二条消息对 SA 提案和流量选择符进行响应,交换 nonce。同时能根据 PFS 的需要可选地进行 Diffie-Hellman 交换。该过程的消息传递见图 2。

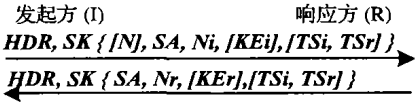


图 2 协商子 SA 交换

3) 信息交换

信息交换用于通信双方传递控制信息以及相互通告错误或特定事件时的一种辅助手段。信息交换应该在初始交换完成后进行,并用生成的密钥材料进行加密和完整性保护。信息交换可以根据发送信息的目的不同,在消息中包含零个或多个通知、删除或配置载荷。

1.3 密钥生成

同第 1 版本类似,IKEv2 需要从 IKE_SA_INIT 交换的 nonces 和建立的 Diffie-Hellman 共享秘密中计算出一个基秘密 SKEYSEED。SKEYSEED 被进一步用来计算其他的五个密钥材料:SK_d 用来提取用于子 SA 的密钥;SK_ai 和 SK_ar 被用作验证 IKE_SA_INIT 后续交换的完整性的密钥材料;SK_ei 和 SK_er 用来对后续交换进行加解密。与第 1 版本不同的是,通信的双方各自使用不同的密钥,即用 SK_ai 和 SK_ei 保护发起方的消息,而用 SK_ar 和 SK_er 保护响应方的消息。SKEYSEED 及其派生值的提取方法如下:

```
SKEYSEED = prf( Ni | Nr, g^ir)
{SK_d | SK_ai | SK_ar | SK_ei | SK_er} =
  prf+ (SKEYSEED, Ni | Nr | SPIi | SPIr )
```

其中 SK_d,SK_ai,SK_ar,SK_ei 和 SK_er 的值顺序地取自 prf+的生成比特值。g^ir 是一个取自 Diffie-Hellman 交换的共享秘密值。Ni 和 Nr 是交换的 nonces 值。Prf 是 IKE 协商的伪随机函数。各算法的密钥材料都取自伪随机函数的输出。当所需密钥材料的总长度大于 prf 算法的输出时,我们采用迭代的方法使用 prf。函数 prf+描述了利用 prf 的输出串联(concatenation)来产生伪随机流的方法:

```
prf+ (K,S) = T1 | T2 | T3 | T4 | ...
其中:
T1 = prf (K, S | 0x01)
T2 = prf (K, T1 | S | 0x02)
T3 = prf (K, T2 | S | 0x03)
T4 = prf (K, T3 | S | 0x04)
```

1.4 功能扩展

IKEv2 合并了 IETF 工作组后来对 IKE 协议所作的修改,包括通过 NAT 网关协商 SA 的能力、使用扩展认证协议(EAP)、对移动用户远程地址配置与密钥协商的支持等;并根据扩充功能实现的需要,在协议中添加了几种载荷类型,如通知载荷(N)、删除载荷(D)、配置载荷(CP)、流量选择符载荷(TS)、加密载荷(SK)、认证载荷(AUTH)等。这些修改使协议能够适用于更多场合中动态 SA 的创建与维护,功能更加强大。

2 分析与改进

2.1 EAP 协议的使用及建议

除了使用签名证书和共享密钥的认证方法外,IKEv2 还支持 EAP 协议的使用。EAP 认证方式可以是非对称的,通常用于主机向服务器的认证。在 IKEv2 中采用 EAP 认证的消息数可变,主机向服务器发起的一次最小化密钥协商的过程有以下几步:

1) 在第 3 条消息中,只包含身份载荷,没有 AUTH 载荷,这意味着发方提供了自己的身份信息但没有对其进行验证。通过这样的消息形式,发方即向收方表明自己期望使用 EAP 协议进行认证。

2) 如果收方的策略支持 EAP 认证,则在第 4 条消息中指示具体的 EAP 认证类型;如果策略不支持,则用通知载荷告知对方不支持 EAP 认证。

3) 根据收方指示的 EAP 认证类型,发方在第 5 条消息中给出该类型对应的数据信息。

4) 收方对提供的 EAP 数据信息进行验证,验证通过则向发方送出 EAP 认证成功的消息,双方继续 IKE_AUTH 交换,建立 IPSec SA;验证失败发送 EAP 认证失败消息,关闭连接,删除 IKE SA。

在 IKEv2(2-14)中,最小的 EAP 认证需进行 8 次消息传递,过程繁琐。由于该方式用于主机向服务器认证的特定情形,相对于发起者,响应者的 IP 地址甚至身份都较容易被别人得到,而发起者可能是 IP 地址每天都在变化的漫游主机。既然向主动攻击者同时隐藏双方的身份是不可能的,那么隐藏发起者的身份信息是更有价值的做法[2]。基于此,本文建议,将 ID 的传递放在第 5 条消息中,放在 EAP 载荷之前。同时,第 7,8 条消息分别合并在第 5、6 条消息中(见图 3)。这样改动的好处是,即使主动攻击者伪装成收方协商建立了 SKEYSEED 及其他派生密钥,也必须先向对方提供自己的身份验证材料,从而使发方的身份免于泄露,并且发方与收方身份对于被动攻击者也是隐藏的;EAP 认证时仍可以从第 5 条消息中提取出所需的发方的身份信息;缩减了协商的次数。在这里,包含 EAP 认证信息的所有消息都进行了加密和完整性保护。

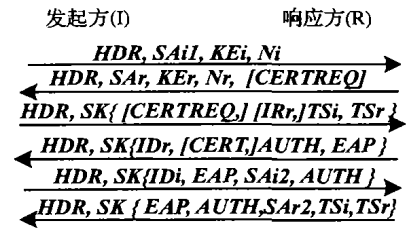


图 3 改进后的 EAP 认证交换

2.2 持有证书的伪装者的攻击

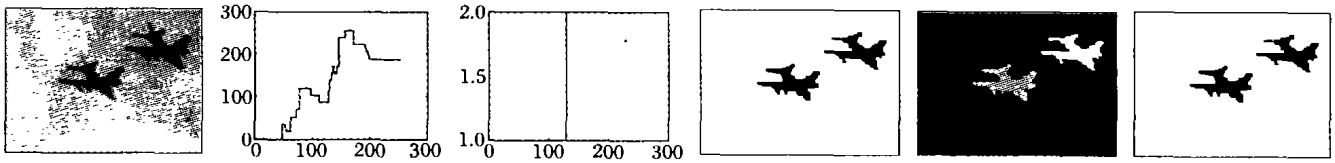
采用签名证书的验证方式可以确保通信者身份的真实可信,避免 Diffie-Hellman 交换受到中间人攻击。但这种验证方式对于持有证书的恶意的攻击者是无效的。因为攻击者可以伪装成所期待的响应方与发起者进行密钥协商,在进行证书交换时,以自己的身份信息及所持有的证书假冒响应方的身份信息与证书,顺利通过认证,从而建立 IPSec SA,阻断与真正响应方的正常协商。由此可见,如果想防止这种攻击,解决问题的关键在于如何分辨出正在与我们协商密钥的是我们真正想与之通信的一方,而不是持有证书的伪装者。

在此给出一种解决方法,通信的双方都维护一张对方的 CA 与证书序号的映射关系表,在接收到对方的证书后,将这两项与表中所期待的CA和证书序号进行对比,如果二者都

(下转第 572 页)

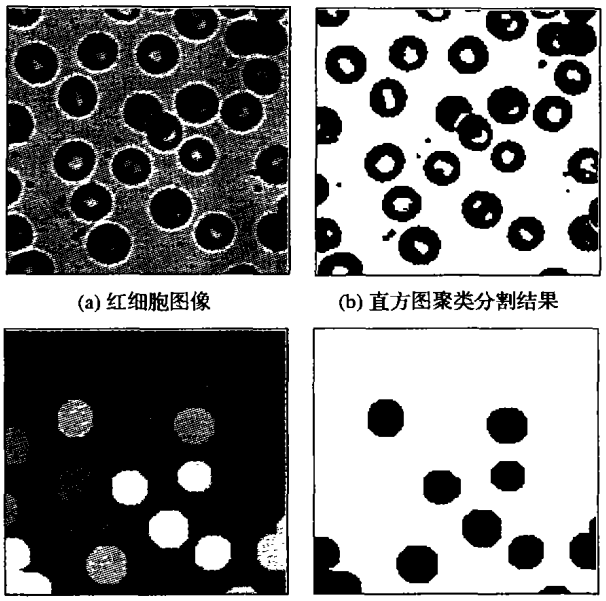
现,不同类型图像有其各自的最佳分割参数范围,具体为:红外图像,$\beta = 200 \sim 300$,$stop = 1e-4$;可见光图像,$\beta = 80 \sim 200$,$stop = 1e-3$;医学图像$\beta = 5 \sim 10$,$stop = 1e-3$。

图 4 为使用几种方法对可见光飞机图像(图像大小为 160×120)进行分割对比的实验。图 4(b)~(d)为使用直方图数据进行聚类划分分割的结果,实验条件为$\beta = 80$,$stop = 1e-3$,所得阈值为 129,计算相似度使用的是 4 连通图,运算时间为 0.08 秒。图 4(e)~(f)为使用图划分方法对原图像灰度数据直接进行聚类分割的结果,实验条件为$\beta = 30$,$stop = 1e-4$,计算相似度使用的是 4 连通图,运算时间为 6.95 秒。可以看到,在同样使用 4 连通图的情况下直接使用图像灰度数据聚类算法速度要慢很多。图 5 为相同条件下对不同尺寸图像进行分割的对比实验(图像尺寸为 160×155),使用直方图聚类分割与灰度数据聚类分割的运算时间分别为0.05 秒及 20.97 秒,可以看到,尽管图像尺寸仅有略微增大,直接使用图像灰度数据进行聚类分割的运算量却大为增加。



(a) 可见光飞机图像 (b) 势函数 (c) 势函数二值聚类 (d) 分割结果 (e) 对灰度数据划分的势函数 (f) 对灰度数据聚类的分割结果

图 4 可见光飞机图像的分割对比实验



(a) 红细胞图像 (b) 直方图聚类分割结果 (c) 灰度数据聚类势函数 (d) 灰度数据分割结果

图 5 医学图像分割对比实验

4 结语

基于图论的图像分割方法是近年来国际上图像分割领域一个新的研究热点。原有的方法都是对图像灰度数据进行聚类,算法运算速度较慢。本文将图论方法用于对直方图数据进行聚类,在保证分割质量基本不变的情况下使算法的运算速度大为提高。将图论方法用于直方图聚类,是一种阈值化分割算法,因此仅适于所有可用阈值化方法进行分割的图像。

参考文献:

[1] WU Z, LEAHY R. An optimal graph theoretic approach to data clustering: theory and its application to image segmentation[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1993, 15(11): 1101~1113.

[2] SHI J, Malik J. Normalized Cuts and Image Segmentation[A]. Proceedings of IEEE Conference on Computer Vision and Pattern Recognition[C], 1997. 731~737.

[3] WANG S, SISKUND JM. Image segmentation with ratio cut[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003, 25(6): 675~690.

[4] GRADY LJ. Space - Variant Computer Vision: A Graph - Theoretic Approach[D]. Boston University, 2004.

(上接第 564 页)

相符,则确定是真正的响应者,可以建立 IPSec SA;否则,判断为攻击者,中断协商流程,关闭连接。

2.3 重新认证的问题及解决方法

在某些密钥协商的场合,特别是远程访问时,通信的双方可能需要对彼此的身份周期性地进行重新验证。这样做的目的是尽可能避免非授权的第三方利用 SA 的某一端获得已建立的 VPN 安全隧道的使用和控制权(例如当真正的使用者暂时或长期地离开时),减少其对 IKE SA 的非授权使用时间。在 IKEv2 中,定义了通过发起一次协商子 SA 交换来重新生成 IKE SA 的方法,称为 Rekeying。但由于协商子 SA 过程中并不对双方的身份进行验证,因此 Rekeying 不适于解决重新认证的问题。

解决这个问题的一种方法是由任一方用通知载荷告知另一方验证的时限,在该时限之前,另一方必须重新发起 IKE 密钥协商和身份验证,重新建立 SA。否则,提出验证要求的一方将会删除 SA,关闭 VPN 安全隧道。重新验证过程见图 4,需要注意的是,在新的密钥协商的第三条消息中,通知载荷 N 包含了旧 SA 的 SPI,以表明是对于旧 SA 的重建。周期性地对通信方进行重新验证除了可以防止第三方非授权使用 VPN 隧道外,由于重新生成了 IKE SA,密钥也随之重新衍生,从而保证了消息中密钥的新鲜度,降低了会话密钥被攻击者破解的危险。

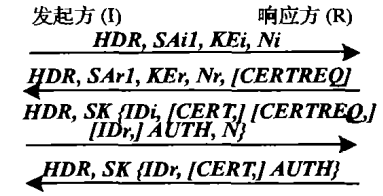


图 4 重新密钥协商及身份验证

参考文献:

[1] KAUFMAN C. Internet Key Exchange (IKEv2) Protocol[EB/OL]. http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-14.txt, 2004.

[2] RADIA P, KAUFMAN C. Analysis of the IPSec Key Exchange Standard [A]. Sixth International Workshop on Enterprise Security[C], 2001.

[3] KENT S, ATKINSON R. Security Architecture for the Internet Protocol [EB/OL]. http://www.ietf.org/rfc/rfc2401.txt, 1998.

[4] BLUNK L, VOLLBRECHT J. PPP Extensible Authentication Protocol (EAP)[EB/OL]. http://www.ietf.org/rfc/rfc2284.txt, 1998.