

文章编号:1001-9081(2005)02-0390-04

IPSec 的分析与改进

龙艳彬,王丽君

(鞍山科技大学 计算机科学与工程学院, 辽宁 鞍山 114044)

(longby2008@126.com)

摘 要:首先对 IPSec 协议体系进行了复杂性和安全性分析,然后在此基础上讨论了几个改进措施,包括传输模式和隧道模式的统一、AH 和 ESP 的简化、IKE 的改进等。通过改进,协议会更加安全和实用。

关键词:IPSec; AH; ESP; IKE; 传输模式; 隧道模式

中图分类号:TP393.18 **文献标识码:**A

Analysis and improvement of the IPSec

LONG Yan-bin, WANG Li-jun

(College of Computer Science and Engineering, AnShan Science and Technology University, Anshan Liaoning 114044, China)

Abstract: This paper analyzed the complexity and security of IPSec protocols, then some reformative features were discussed, including the unity of transport mode and tunnel mode, the simplification of AH and ESP, the reformation of IKE and so on. So the protocol can be more practical and securer by modification.

Key words: IPSec; AH; ESP; IKE; transport mode; tunnel mode

1 IPSec 的分析

IPSec 作为一个新兴的网络安全标准,其自身体系结构还不完善,不仅某些概念过于复杂,实际应用中还存在一些漏洞。本文将对其体系结构以及 IKE 协商的第一阶段作出改进,使其更加实用和完善。

1.1 IPSec 的安全协议与模式

IPSec 安全协议给出了封装安全载荷(ESP)和认证头(AH)两种通信保护机制。按照相应 RFC 的规定,AH 机制提供完整性保护、抗重放攻击和连接的访问控制;而 ESP 除提供 AH 提供的保护外,还提供机密性和一定程度的流量保护。由此可见,AH 对网络流量提供的安全保护是 ESP 提供的保护的子集。而这两种安全协议根据封装的载荷内容不同,有传输和隧道两种模式:。传输模式将上层协议部分封装到载荷中,即对上层数据提供保护;隧道模式是将整个 IP 分组封装到载荷中,即对整个数据包提供保护。也就是说,在应用中 IPSec 体系结构的发送端可以有以下四种选择:AH 传输模式、AH 隧道模式、ESP 传输模式和 ESP 隧道模式。这对于用户来说,似乎可以根据不同的情况做出不同的选择。然而,在实际应用中并不是都需要这四种组合。实际应用中这几种选择在认证功能上几乎没有什么差别,而且认证所花费的代价差别不大。允许多种选择只会使系统的概念更加复杂,在实际应用中也会增加协商的开销,违背了越简单越安全的原则,因此有必要作出改进。

1.1.1 模式的统一

IPSec 提供的传输模式适用于端主机,两个端主机经过 IKE 协商 SA,从而双方传输的 IP 分组将受到 ESP(或 AH)的

安全保护。其优势在于:

- 1) 即使内网中的其他用户,也不能理解传输与两个端主机之间的数据内容。
- 2) 分担了 IPSec 处理负荷,避免了 IPSec 处理的瓶颈问题。

传输模式具有如下缺点:

- 1) 由于希望实现安全保护的端主机必须安装 ESP(或 AH)协议,因此不能实现对端用户的透明服务,用户得到安全服务的代价是牺牲内存和处理时间。
- 2) 不能使用私有 IP 地址,必须使用公有地址资源。
- 3) 暴露了子网内部拓扑信息。

IPSec 提供的隧道模式主要用于网关之间或网关与主机之间,也适用于主机之间的通信。这种模式的优点是:

- 1) 保护子网中的所有用户都可以透明地享受由安全网关提供的安全服务。
- 2) 子网内部可以使用私有 IP 地址,无须使用公有 IP 地址资源。

子网内部的拓扑信息被保护。

隧道模式的缺点是:

- 1) 增大了网关的处理负荷,容易形成通信瓶颈。
- 2) 对内部的诸多安全问题无能为力。

RFC2401 规定,这两种模式的区别是:传输模式中仅对上层协议的报文提供安全服务,而 IP 报头是不受保护的;而隧道模式是对上层协议和 IP 报头都提供安全服务。也就是说,两种模式的实质区别是对数据包保护的范围不同。然而,在实际的应用中,是对上层数据还是对整个数据包进行保护,其操作方式、执行效率和开销差别甚微。很显然这种区分局限

收稿日期:2004-07-19;修订日期:2004-10-10

作者简介:龙艳彬(1975-),男,辽宁鞍山人,讲师,硕士,主要研究方向:网络安全与通信;王丽君(1961-),女,辽宁鞍山人,教授,主要研究方向:网络安全与通信。

于概念,并没有什么实际意义。再加上传输模式所能达到的保护目的,隧道模式也完全可以达到。虽然在使用隧道模式时因为要在数据包外层增加一个新 IP 头而比传输模式多消耗一定的带宽,但我们可以使用一种特殊的头部压缩技术(IPComp)来解决该问题。IPSec 在 VPN 的应用中,由于路由器(网关)的存在,几乎都是使用隧道模式来保护数据。

基于以上分析,我们可以将传输模式和隧道模式进行统一,并称之为隧道传输模式。这样一来,主机和路由器(网关)的概念在 IPSec 中得到了统一,为后面的 IKE 协商减少开销打下基础。

1.1.2 安全协议的统一

由于提供 IP 数据报完整性的认证机制非常初级,所以 IP 协议本身缺乏安全性。设计 AH 协议的目的是用来增加 IP 数据报的安全性。AH 协议提供无连接的完整性,数据源认证和抗重放保护服务,而不提供任何保密服务。其作用是为 IP 数据流提供高强度的密码认证,以确保被修改过的数据包可以被检查出来。它使用消息验证码(MAC)对 IP 进行认证,常用的 MAC 有 HMAC_MD5、HMAC_SHA_1、HMAC_RIPEMD_160,它的认证范围是数据包里除可变域外的所有域。而相对的 ESP 协议同样用来增强 IP 的安全性,它提供数据保密,数据源认证,无连接完整性,抗重放服务和有限的数据流。实际上 AH 提供的安全服务 ESP 都能提供。在 RFC2406 中规定用 AES 来代替原来的 DES 实现对数据包的高强度加密,用 HMAC_MD5、HMAC_SHA_1 和 NULL 算法来对数据包提供认证服务。与 AH 的唯一区别是 ESP 不认证 IP 头,即它的认证范围比 AH 的认证范围小。

在实施 IPSec 时,AH 和 ESP 可以单独使用,也可以结合使用。IPSec 协议的制定者之所以对 AH 和 ESP 进行区分,主要是为了功能分配清晰,体现一定的灵活性。然而,这种区分在现实情况中完全没有必要。因为 ESP 除了在认证范围上与 AH 有一点区别外,没有任何资料显示它的认证安全性比 AH 差,它们所使用的认证算法和认证步骤都完全一样。这种区分会使实际操作更加繁琐。比如在 IKE 协商中需要 SA 双方协商是使用 AH 还是使用 ESP,或者两者都使用,就必须分别为 AH 和 ESP 建立存储单元,记录对应的认证算法、使用的密钥和生存周期等等。

因此,我们取消 AH 的概念,对 ESP 作出一定修改,使它在原有安全服务的基础上提供对整个数据包的认证。为了实施修改后的 IP 安全体系和 ESP 安全协议,我们作如下规定。因为在 IPSec 协议中,无论认证还是加密,其安全保护都是片面的。如果使用没有加密的认证,或者在传输时使用明文,那么对于第三者的截包和数据的泄露将无能为力,这对于许多公司和企业来说无疑是灾难。如果使用没有认证的加密,由于加解密将消耗大量的资源,对于数据包接收方来说,当接收到来自第三方恶意修改后的数据包时,不能辨别其真伪而进行解密,将消耗大量的系统资源,使系统性能急剧下降,甚至导致网络系统崩溃而终止服务。由此可见,单方面使用认证或加密都存在安全漏洞。所以,在 IPSec 安全体系中,如果要使用安全服务,加密和认证必须强制使用,而且,应该是先加密后认证。此外,为了使接收方不遭受重放包的攻击,抗重放功能必须被强制使用,接收方必须使用滑动窗口机制启用抗重放服务。

1.2 IKE 的分析与改进

IKE(Internet Key Exchange)是 IPSec 中的自动密钥交换协议,用于动态地建立安全关联(SA),为通信双方协商 IPSec 通信所需的相关信息:如加密算法、密钥信息、通信方身份等。IKE 建立在 ISAKMP 定义的框架上,并实现了两种密钥管理协议——OAKLEY 和部分 SKEME,是建立在多个协议基础上的混合型协议。它使用了两个阶段的 ISAKMP:第一阶段建立 ISAKMP SA;第二阶段利用这个既定的 SA,为 IPSec 协商具体的 SA。

第一阶段中两个 ISAKMP 实体之间建立了一个安全的、验证无误的通信信道,被称为 ISAKMP SA。它可以由主模式和积极模式两种方式完成。不管是哪种模式,它们完成的任务是相同的:即建立 ISAKMP SA 和建立验证过的密钥,为双方的 IKE 通信提供机密性、消息完整性以及消息源验证服务。IKE 中定义的其他所有交换都要求以建立一个验证过的 ISAKMP SA 为首要条件。所以在进行其他任何交换之前必须完成一次第一阶段交换。第二阶段中完成了 IPSec SA 的协商,并且协商过程要受到第一阶段的 ISAKMP SA 的保护。ISAKMP SA 保护快速模式交换的方法是:对其进行加密,并对消息进行验证。

在 IKE 交换过程中之所以要分两个阶段交换是因为这样可以提高协商效率。因为第一阶段协商可以应用于多个第二阶段的协商,而第二阶段协商可以申请多个 SA。这种优化减少了完成每个 SA 的传输往返及 DH 幂运算,从而提高协商的效率。第一阶段中的主模式提供了身份保护。当身份保护不必要时,可以使用积极模式以进一步减少传输往返。本文主要对 IKE 协商第一阶段需要进行身份保护的主模式中存在的安全漏洞进行分析并作出改进。

1.2.1 IKE 的主模式消息交换过程

IKE 主模式需要六个消息来完成:头两个消息进行 Cookie 交换和协商策略,包括加密算法、散列算法及认证方法等;中间的两个消息交换 Diffie-Hellman 共享密钥和必要的辅助数据(如伪随机数 Nonce);最后的两个消息认证 Diffie-Hellman 交换和身份信息。主模式提供了四种不同的认证方法:公钥签名认证、两种公钥加密认证、预共享密钥认证。其消息交换过程如下:

1) 公钥签名认证方式(如图 1 所示)。其中,消息 5,6 用前面协商的密钥材料生成密钥加密,而且可以进行证书交换。

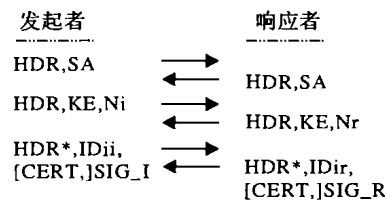


图 1 IKE 中签名认证的主模式

2) 第一种公钥加密认证方式。其中,消息 3,4 中的 Nonce 和 ID 用对方的公钥加密,消息 5,6 用前面协商的密钥材料产生密钥加密。

3) 第二种公钥加密认证方式。公钥加密认证方式的主要缺点是需要进行两次公钥加(解)密运算,而公钥加(解)密需要较高的计算代价。另外,公钥加密认证方式不允许证书的请求和交换,因为这样会失去身份保护的功能。第二种公

钥加密认证方式对其做了修改:Nonce 仍然用对方的公钥加密,而身份信息 ID 和 Diffie_Hellman 交换值 KE 用另外产生的对称密钥加密,而且可以选择证书交换,证书也用相同的对称密钥加密。这样的修改在保证安全性的前提下,降低了计算代价,而且提供了证书交换的功能。

4) 预共享密钥认证方式。其中,消息 5,6 用前面协商的密钥材料产生密钥加密。

1.2.2 IKE 安全隐患及改进

下面将针对 IKE 交换中的几种攻击方式和安全隐患分别进行分析改进:

1) 针对拒绝服务攻击的改进

众所周知,拒绝服务攻击(Denial of Service Attack)是通过大量消耗系统资源(存储资源、CPU 计算资源等)的方法,致使系统无法响应正常的处理请求,甚至陷入瘫痪。在 IKE 的协商过程中,需要通过 Diffie_Hellman 交换进行密钥协商,其中的模幂运算会占用较大的计算资源。因此,一个拒绝服务攻击者会通过 IP 欺骗(IP Spoofing)的方法发起大量虚假交换请求,如果系统不能分辨出这些伪造的请求包,则不得不对伪造的请求进行大量模幂运算,从而降低处理效率,甚至引起拒绝服务。为了抵御针对 Diffie2Hellman 交换的拒绝服务攻击,主模式交换采用了 Cookie 的方式,即在密钥交换前先进行 Cookie 交换,以确认请求方可以收到回应,再进行密钥交换,从而防止通过 IP 欺骗进行的拒绝服务攻击。其运行方式如下:

a) 发起者首先向响应者发出一个 Cookie_Request 信息,同时启动一个重传计时器,如果在一定时间内,发起者没有收到一个 Cookie_Response 信息,它将继续发送 Cookie_Request 信息。

b) 当响应者收到一个信息 Cookie_Request 时,它首先会检测是否有足够的资源来进行一次密钥交换。当有过多的 SA,并且进行请求的发起者所对应的 SPI 值已经启用时,或者相关的一些资源已经耗尽时,响应者就会返回错误信息。否则,响应者就会生成一个 Cookie,填充在 Cookie_Response 信息相应的 Cookie 域中,发出 Cookie_Response 信息(发起者的 Cookie 域也要被填充作为 Cookie_Response 信息的一部分)。

c) 发起者收到 Cookie_Response 信息后,首先验证它的有效性,这时通过根据响应者的 IP 重构 Cookie,与 Cookie_Response 信息发起者的 Cookie 域值比较,如果相同就可以进行其他交换,否则,就把信息丢掉。这样就会使通信双方在进行消耗资源很大的 DH 交换之前,先进行一次 Cookies 交换,用来防范拒绝服务攻击。

在 IKE 中, Cookies 除了可以用来防范拒绝攻击外,另外一个作用就是放在 ISAKMP 头中,用作标志 ISAKMP SA。对于 Cookie 的计算,本文建议的方法是: $\text{Cookie} = \text{PRF}(\text{对方的 IP 地址}, \text{对方的 Cookie}, \text{自己所拥有的一个秘密})$ 。并且这个秘密应该阶段性地进行改变,这样做的目的是防止攻击者在一段时间内,用大量的 IP 地址来获得大量的 Cookie 值,然后一次性地重传这些信息来攻击通信一方。

2) 针对重放攻击的分析及改进

重放攻击(Replay Attack)是指攻击者在通信线路中窃听、截获通信双方的消息,然后重新向通信的一方发送截获的消息。重放攻击会迫使系统被迫处理大量不必要的操作,严

重时可导致拒绝服务。然而 IKE 协议没有提供明确的防范重放攻击的机制,为了抵御重放攻击,我们对 IKE 协议的消息格式进行了修改,为整个 IKE 交换提供了统一的抗重放攻击的保护。

即将 IKE 消息包头中的消息 ID 字段用作抗重放计数器,同时加入滑动窗口机制,使 IKE 交换能够有效地抵御重放攻击的威胁。IKE 交换的消息具有统一的格式,包括包头和载荷两部分。其中,包头中的消息 ID(Message ID) 字段,长度为 4 字节,它由快速模式交换的发起者随机生成,用作第二阶段的消息标志符,判断该消息属于哪一个快速模式。而在第一阶段交换中,消息 ID 字段被闲置,恒为 0。现在修改消息 ID 字段的作用,将其用作抗重放计数器,可以防范整个 IKE 交换中(包括两个阶段)的重放攻击。修改方法为: IKE 第一阶段的发起者发送第一个消息时,将消息 ID 设为 1,以后的每次消息交换依次加 1;同样,响应者的消息 ID 也从 1 开始计起,只是最高位恒为 1,以确保与发起者的消息 ID 不同。同时,交换双方各需要一个滑动窗口进行消息的判断接收,其运行机制与 ESP 中的滑动窗口类似。对于当前收到的消息,若消息的 ID 小于滑动窗口的左端的消息 ID,则为重放消息予以丢弃;若消息的 ID 在窗口内,则可以根据是否已接收来验证是否为重放消息;若消息的 ID 在窗口右端外,则为新消息,经验证通过后,接收此消息并将窗口的右端右移。这样通过在 IKE 协议中引入了抗重放计数器和滑动窗口的机制,可以为 IKE 交换中的消息提供统一的抗重放攻击的保护。

3) 针对身份保护的缺陷及改进

在 IKE 的主模式阶段提供了对通信端点身份的隐藏,协商过程中用生成的密钥对 IDI 和 IDR 进行了加密。虽然对于被动攻击者,能够做到对于双方身份的保密,但是却很难设计一种协议来防范已知道某一方身份的主动攻击者。

在不能完全保证向主动攻击者隐藏通信另一方身份的情况下,最好保护发起者身份,而不是响应者的身份。因为在实际情况下,VPN 用户的发起者,一般为单个用户,流动性很强,它的 IP 地址往往是不固定的,可能每一天都在变化;而响应者一般是一个机构,往往都是用一个固定的 IP,这个 IP 地址是很容易就能被别人得到的。所以,保护发起者的身份比保护响应者的身份更有实际意义。

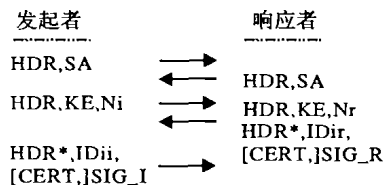


图2 改进后的签名认证的主模式

在通过签名验证的主模式中,响应者的身份不仅对被动攻击者,而且对主动攻击者也是隐藏的。但对于知道响应者的地址主动攻击者而言,发起者的身份就是暴露的。因为,主动攻击者可以通过伪造响应者的 IP 地址来和发起者进行 Diffie_Hellman 密钥协商,顺利地进行上述 5 步的操作,并且可以在第 5 步得到发起者的身份。然而,它是无法通过第 6 步操作的,因为它不知道响应者的签名。但是,目前针对发起者的攻击更是层出不穷。因此本文作如下改进如图 2 所示。这样,主动攻击者在第 4 步就无法通过,从而就不能获知发起者的身份,同时整个协议仅仅需要 5 步就可以完成。这样修

改后的协议不但可以对被动攻击者隐藏通信双方的身份,而且对于知道响应者身份的主动攻击者也无法获得发起者的身份。这在实际应用中会更有价值。

2 改进后的 IPSec 体系模型

通过以上的分析,可以看出对 IPSec 体系改进的必要性,为此我们构造了 IPSec v2 协议模型,其安全体系模型结构如图 3 所示。

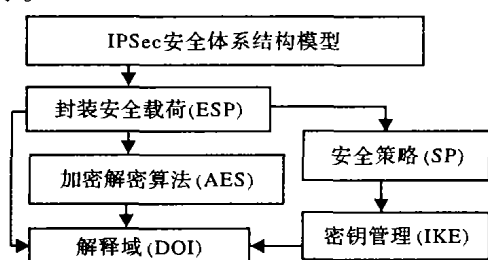


图3 改进的IPSec体系模型

由于我们对 ESP 作出了改进,它包含了原安全协议中 AH 协议和 ESP 协议的功能。新 ESP 的特性:缺省提供认证功能;加密功能则是可选;认证范围是除可选域外的整个数据包;强制提供抗重放服务。因此在 IPSec v2 中只提供封装安全载荷协议,而密钥管理也将使用改进后的 IKE,其他组成部分和原协议相同。

2.1 隧道传输模式的数据包格式

在 IPSec v2 模型中,我们使用改进后的隧道传输模式。其数据包格式如图 4 所示。

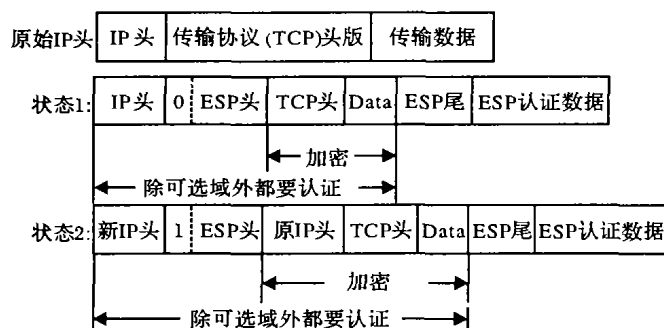


图4 隧道传输模式数据包格式

在新 ESP 头中增加了一个标志位用来判断对数据包的处理。若标志位为 0 表示内外 IP 相同,数据包省去内部 IP 头以节省带宽,这种情况类似原模型中的传输模式;若为 1 表示内外 IP 头不同,此时类似原模型的隧道模式。实际应用时,可用 ESP 协议的“下一协议”域来作标志位以判断数据包格式。如果下一字段为 TCP 或 UDP 等,则标志位为 0,是状态 1 下的数据包;如果下一字段为 IP,则标志位为 1,是状态 2 下的数据包。

2.2 数据处理流程

数据外出处理流程如下:

1) 当 IPSec 模块接收到一个外出数据包时,它使用选择符(目的 IP 地址和端口、传输协议等)查找安全策略库 SPD,决定其是否需要安全处理,如不需要,直接转到 8)。

2) 如果需要安全处理并且 SA 或 SA 束已建立,则与选择符匹配的 SPD 项将指向安全关联库 SAD 中相应 SA;如没建立则调用 IKE 协商一个 SA 并将其链接到 SPD 项。

3) 生成或增加序列号并对每个数据包构造隧道传输模式的外层 IP 头。

4) 比较内外层的 IP 源地址,如果不同,置标志位为 1,转到 7)。

5) 如果相同,置标志位为 0,压缩数据包并删除内层 IP 头。

6) 对内层数据进行加密并对数据包进行认证,转到 8)。

7) 对整个数据包除可选域外进行数据认证并对内层数据实施加密。

8) 结束对数据包的处理,返回 TCP/IP 协议栈的其他协议。

数据进入处理流程如下:

1) IPSec 主机或安全网关接收到数据包时,使用 IP 头中的目的 IP 地址和 IPSec 协议以及 ESP 头中的 SPI 进入 SAD 查找进入包的 SA。如果失败,则转到 8)。

2) 使用 1) 中查找到的 SA 对 ESP 包进行处理,使用包中的选择符进入 SPD 查找一条与其匹配的策略,如果没有,则转到 8);否则启用抗重放窗口检测是否是重放包,如是则丢弃。

3) 查看数据包 ESP 头中的标志位,如为 1,转到 7)。

4) 对数据包进行认证并对内层数据进行解密。

5) 根据外层 IP 头构造内层 IP 头并插入到上层数据之前。

6) 删除外层 IP 头并转到 8)。

7) 对数据包进行认证并对内层数据进行解密,然后删除外层 IP 头。

8) 结束对数据包的处理,然后返回 TCP/IP 协议栈的其他协议。

3 结语

本文对原 IPSec 安全体系进行分析和探讨后,对模式的概念作出了简化,对安全协议作出了统一并对 IKE 协商的阶段一的签名认证主模式作出了改进,使该安全体系模型更加实用。当然要使改进的安全体系更好地应用,还必须解决它与原 IPSec 的兼容问题以及与一些网络边界设备如网络地址转换 NAT 的兼容问题,还有使用安全服务后带宽的增加,性能的下降及相对独立性等问题,我们将在以后的研究中致力解决这些问题。

参考文献:

- [1] FERGUSON N, SCHNEIER B. A Cryptographic Evaluation of IPSec, Counterpane Internet Security, Inc, 3031 Tisch Way, Suite 100PE, San Jose, CA 95128[EB/OL]. <http://www.counterpane.com> 1-28, 2004.
- [2] RADIA P, KAUFMAN C. Analysis of the IPSec Key Exchange Standard[R]. Call for Paper Sixth International Workshop on Enterprise Security, 2001-06.
- [3] DAVIS CR. IPSec VPN 的安全实施[M]. 周永彬,等译. 北京:清华大学出版社, 2002.
- [4] IPSec Working Group[S]. The Internet Key Exchange (IKE). Protocol Internet-draft draft-ietf-ipsec-ikev2-00.txt, RFC 2406, 2001-11.
- [5] 于佳,李大新. IKE 的分析与改进[J]. 山东大学学报, 2003, (5): 159-160.
- [6] MADSON C, GLENN R. The use of HMAC-SHA-1-96 within ESP and AH[S]. RFC 2404, 1998.
- [7] 朱丽芬. IP 安全模型的分析与改进[J]. 南京大学学报, 2004, (3): 45-47.
- [8] 戴宗坤,唐三平. VPN 与网络安全[M]. 西安:电子工业出版社, 2002.