对IPSec中AH和ESP协议的分析与建议

蓝集明,陈 林
(四川理工学院 计算机学院,四川 自贡 643000)

摘 要:IPSec是IETF提供的在Internet上进行安全通信的一系列规范。由于历史的原因,从开始设计IPSec的那一天起,IPSec的体系结构就逐渐走向了复杂,变得越来越庞大而不合理。为了简化IPSec的体系结构,提高IPSec的运行效率,在介绍了IPSec中的AH和ESP协议以及它们的工作模式的基础上,通过对AH和ESP异同点的分析和比较,提出了一条简化IPSec体系结构的思路,那就是不妨考虑通过取消AH协议来实现。这对IPSec的理论研究和实际应用都具有一定的参考价值。

关键词:IPSec;AH;ESP
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2009)11-0015-03

Analysis and Suggestion on the AH and ESP in IPSec

LAN Ji-ming, CHEN Lin
(School of Computer Science, Sichuan University of Science & Engineering, Zigong 643000, China)

Abstract: IPSec is a series of norms proposed by International Engineer Task Force(IETF), which can be used to communication security on Internet. IPSec has an over scaled architecture, and becomes more and more complicated due to history. In order to simplify IPSec architecture and improve the efficiency, introduces the AH, ESP and their working mode in IPSec in detail, compares the differences and similarities between the AH and ESP, suggests an idea of simplifying IPSec architecture by abolishing the AH. The research work should be valuable in the project application and the theory research of IPSec.

Key words: IPSec; AH; ESP

0 引 言

IPSec(Internet Protocol Security)协议是IETF提供的在Internet上进行安全通信的一系列规范,它为私有信息通过公用网提供了安全保障。IPSec包括安全协议和为这些安全协议协商安全参数的密钥管理协议,以及一些认证和加密算法。其中,安全协议包括封装安全载荷(Encapsulating Security Payload,ESP)和验证头(Authentication Header,AH),实现通信保护机制。这两种安全协议都提供数据源认证、完整性和抗重播攻击服务[1],但它们也存在一定的区别和联系。对此,文中进行了深入的分析和研究。

IPSec对于IPv4是可选的,对于IPv6则是强制性的,它是IPv6的一个组成部分。虽然IPv4也支持IPSec,但IPSec在IPv4中应用得并不成功,而且比较复杂。又因为IPv6正以蓬勃的速度向前发展,最终取代IPv4是历史的必然[2,3]。为此,文中探讨的环境默认是IPv6环境。

1 AH协议

AH协议为数据报提供身份验证、完整性和抗重播服务,并签署整个数据报,但不加密该数据报,因此不提供机密性服务。AH协议是IPSec安全协议之一,设计它的目的就是要用它来增强IP数据报的安全性。AH为IP数据流提供了高强度的密码认证,以确保被修改过的数据包可以被检查出来。

AH报头由5个固定长度域和一个变长的认证数据域组成[4]。AH的报头结构如图1所示。

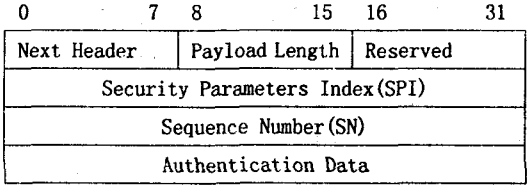

图1 AH的报头结构

说明:Next Header是一个8比特的域,指出AH

收稿日期:2009-03-02;修回日期:2009-05-24
基金项目:四川省教育基础应用研究基金(2008A140)
作者简介:蓝集明(1973-),男,四川富顺人,硕士,讲师,研究方向为计算机网络技术。

后的下一载荷的类型。Payload Length 也是一个 8 比特的域,它包含以 32 比特为单位的 AH 的长度减 2。Reserved 是一个 16 比特的保留域,供将来使用,现在应置为 0。SPI 是一个 32 比特的整数,是标识一个安全关联(SA)[5]的三要素之一。SN 是一个用作单调递增计数器的 32 位无符号整数,提供了抗重播的功能。Authentication Data 是一个变长域,存放了数据报的完整性校验值(Integrity Check Value,ICV)。ICV 是用消息验证码(MAC)生成的。MAC 是一种算法,它接收一个任意长度的消息和一个密钥,生成一个固定长度的输出,称作消息摘要或指纹。因为生成 IP 数据报的消息摘要需要密钥,所以 IPSec 的通信双方必须共享密钥才能在输入相同的数据时 MAC 算法计算出相同的消息摘要。生成 ICV 的算法是由 SA 指定的,这个算法因 IPSec 的不同实现而不同,但为了保证互操作性,AH 规定了两个强制身份验证器:HMAC - MD5 (Message Digest version 5)和 HMAC - SHA - 1(Secure Hash Algorithm version 1)。它们都使用 HMAC 算法,前者包含 MD5 哈希码,ICV 长度 128 位,后者包含 SAH - 1 哈希码,ICV 长度 160 位。对于 IPv6 数据报,这个 ICV 域的长度必须是 64 的整数倍,如果不是 64 的整数倍,必须添加填充比特使它达到所需要的长度。

这样,数据包在传输过程中有任何的变动,都会使得两次产生的 ICV 值不一致,从而保证了数据的完整性。由于完整性校验算法采用密码进行验证,只有发送方与接收方才知道密码,从而起到了不可抵赖的作用,保证了对数据源的身份认证。AH 中设有序列号域 SN,使目的主机可以辨别哪些是有效的数据报,拒收重复传播的数据报,从而起到了抗重播的功能。

2 ESP 协议

ESP 协议提供:包括消息内容的机密性和有限的通信量的机密性,作为可选的功能,ESP 也可以提供 AH 的验证服务。ESP 通过使用密码算法加密 IP 数据报的相关部分来实现保密服务,密码算法使用对称密码体制,如三重 DES,RC5,IDEA,CAST 等。

ESP 数据报由 4 个固定长度的域和 3 个变长域组成[6]。ESP 的报头结构如图 2 所示。

ESP 报头中多数字段的含义与 AH 相同,下面谈谈不同的部分。Payload Data 是一个变长域,但它以比特为单位且必须是 8 的整数倍。如果使用保密服务的话,这个域包含的是实际数据加密后的密文。如果采用的加密算法需要初始化向量(IV),它将在这个域中传输。相应的算法定义了 IV 的位置,以强制实施的算法(DES - CBC)来说,IV 是这个域中的第一个 8 位组,但需要注意的是,它仍是没有加密的。Padding 如果有的话,这个域包含填充比特,由加密算法使用或用于使 Pad Length 域和 4 字节中的第 3 个字节对齐。Pad Length 是一个 8 比特的域,表明 Padding 域中填充比特的长度。显然,它的取值范围是 0 到 255 的整数。Next Header 也是一个 8 比特的域,表明载荷中封装的数据类型。可能是一个 IPv6 扩展头或传输层协议。例如,值 6 表明载荷中封装的是 TCP 数据。Authentication data 域是可选的,仅当指定的 SA 要求 ESP 提供认证服务时才包含它。它与 AH 的 Authentication data 域类似,也是一个变长域,存放 ICV,只不过它是对 ESP 包(不含 Authentication data 域)进行计算后获得的。

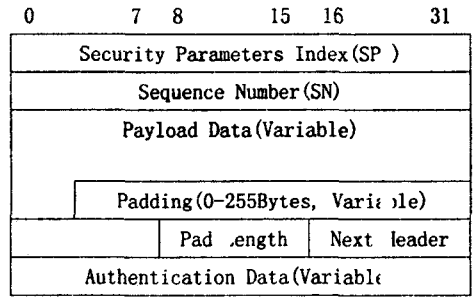

图 2 ESP 的报头结构

3 IPSec 的工作模式

IPSec 的 AH 和 ESP 在实际使用时都支持两种工作模式:传输模式和隧道模式[5,7]。前者在两个系统的通信中,数据报实际的 IP 头要暴露出来,以便在 Internet 上进行选路;后者则将需要传输的整个 IP 数据报进行封装。

3.1 传输模式

传输模式提供对上层协议(IP 的有效载荷)的保护,实现两个主机之间端到端的安全通信。当数据报从传输层传到网络层时,IPSec 会进行"拦截",在 IP 报头与上层协议头之间插入一个 IPSec 头。其中,AH 报头包含了整个 IP 数据报的鉴别信息,但那些在传送中要发生变化的 IP 头部信息(如 IPv4 中的 TTL、头部校验和、IPv6 中的 Hop - Limit),不能包含在鉴别算法计算的范围内。ESP 报头则分为两部分:一部分是由 SPI 和 SN 域组成 ESP 头部,另一部分是由 Padding、Pad Length 和 Next Header 域组成的 ESP 尾部。ESP 头部被插在 IP 头和所有的选项之后,但是在传输层协议之前,ESP 尾部和 ICV 存放在最后。图 3 表示了传输模式中 IPSec 的 AH 头和 ESP 头分别在 IPv6 数据报中的嵌入情况。

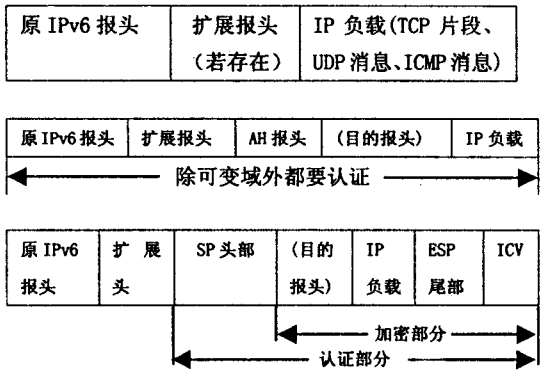

图 3　IPSec 头在传输模式中的嵌入情况

3.2　隧道模式

隧道模式的本质就是将一个 SA 应用于一条 IP 通道上。如果一个 SA 的某一端是一个安全网关,那么该 SA 就必须是隧道模式。所以,当一个 SA 位于两个安全网关之间或一个主机与一个安全网关之间时,它总是隧道模式。隧道模式提供对整个 IP 数据报的保护,它将整个 IP 数据报进行封装,然后添加一个外部 IP 头,并在外部 IP 头与内部 IP 头之间插入一个 IPSec 头。外部 IP 头用来指明 IPSec 处理的源/目的地即通道的源/目的地,内部 IP 头则指明数据报本身进行通信的源/目的地。IPSec 还支持嵌套隧道,对一个已经隧道化的数据报再进行一次隧道化处理。隧道模式中 IPSec 头在 IPv6 数据报中的嵌入情况如图 4 所示。

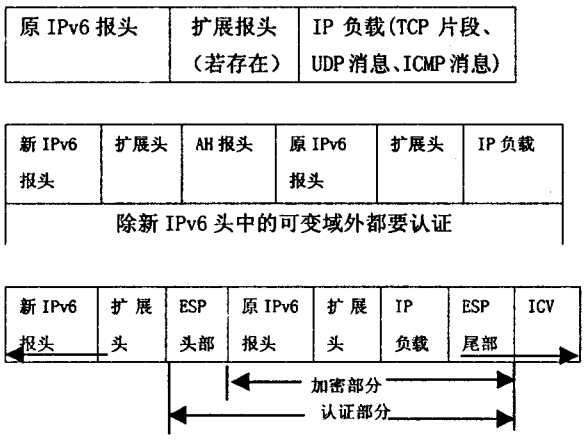

图 4　IPSec 头在隧道模式中的嵌入情况

4　对 IPSec 安全协议的分析与建议

AH 协议和 ESP 协议都是网络互联层的安全协议,但二者各有侧重。从认证服务方面来看,AH 协议和 ESP 协议都提供认证服务功能,但是 AH 是专门用来提供认证服务的,而 ESP 的认证服务是可选的[8]。另外,从图 3 和图 4 可知,ESP 提供的认证服务范围要小于 AH,在 ESP 头部以前的 IP 头是不会被认证保护的,而 AH 认证了几乎所有的 IP 报文。从保密服务方面来看,AH 协议不提供保密服务,而 ESP 则主要用于数据保密服务。当使用隧道模式时,在两个网关之间使用 ESP 保护的安全关联还可以提供一定的流量保密性。在 ESP 的隧道模式中由于内层的 IP 数据报被加密,所以它还隐藏了内层 IP 数据报真实的源地址和目的地址。另外,ESP 使用的填充字节也隐藏了报文的实际长度。从抗重播方面来看,AH 协议和 ESP 协议都有抗重播的功能。只要收方使能,AH 协议的抗重播功能就可以可靠地工作,而 ESP 协议则必须要有认证机制的配合,才能起作用。

IPSec 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,在实际的应用中这种区分是完全没有必要的。因为除了在认证范围上 ESP 要比 AH 小一点外,没有任何资料和应用证明 ESP 的认证安全性会比 AH 差,它们所使用的认证算法和认证步骤是完全相同的。恰恰相反,这样的区分会导致 IPSec 的实际操作变得更加的繁琐,效率也会更低。比如在 IKE 协商中就需要 SA 双方协商是使用 AH 还是 ESP,或者两者都使用,并分别为 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。实际上,IPSec 可以应用于端主机之间、网关之间、端主机与网关之间或远程主机与服务器之间。每种方式都可以应用一个或多个 SA,每个 SA 可以是传输模式 AH、传输模式 ESP、先传输模式 ESP 再传输模式 AH、或者前面的任意一种后再传输模式 AH 或 ESP 隧道模式等组合。这从表面上看好像可以根据不同的要求选用不同的组合,具有很强的灵活性,但实际上却带来了复杂和"过度保护"的问题。

另外,在 IPSec 的实际应用中,无论是单纯的认证服务还是单纯的加密服务,其安全保护都是很片面的。如果使用没有加密的认证,即在传输时使用明文,那么就有可能产生第三者截包和数据泄露的问题,对一些重要的单位和部门来说这无疑将产生一种灾难性的后果。如果使用没有认证的加密,由于加密和解密都要消耗大量的系统资源,对于数据包接收方来说,当收到来自第三方恶意修改后的大量的数据包时,不能辨别其真伪而一味地去进行解密,这势必会消耗网络系统的大量资源,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,仅使用认证或仅使用加密服务都存在很大的安全漏洞。所以,在 IPSec 安全体系中,如果要使用安全服务,加密和认证两项服务都应该同时强制使用,而且应该是先加密后认证,使接收方可以先验证数据报的完整性和真实性,再进行解密

(下转第 22 页)

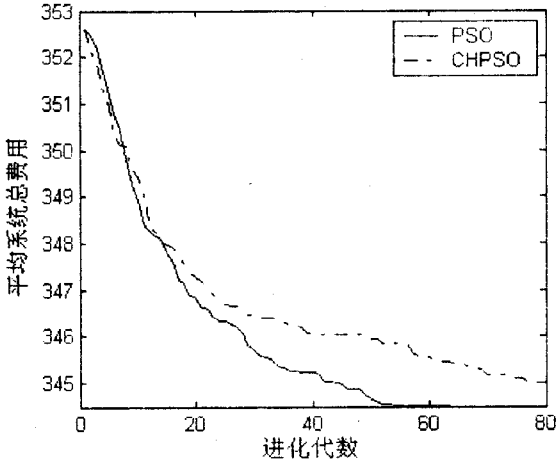

图 3 平均系统总费用与进化代数变化曲线

验证了该算法能够摆脱局部极值,得到全局最优。将 CHPSO 算法用于(N + M)系统费用模型求解,得到最优解。

新算法搜索效率、精度等方面均优于基本粒子群算法,同时具有较好的收敛稳定性。

参考文献:

[1] Kenedy J, Eberhart R C. Particle swarm optimization[C]// Proceedings of IEEE International Conference on Neural Networks. Piscataway, NJ: IEEE Press, 1995: 1942 - 1948.

[2] Eberhart R C, Kennedy J. A new optimizer using particle swarm theory[C]//Proceedings of the Sixth Internationals Symposium on Micro Machine and Human Science. Nagoya, Japan: IEEE Press, 1995: 39 - 43.

[3] Eberhart R C, Simpson P K, Dobbins R W. Computational intelligence PC tools[M]. Boston, MA: Academic Press Professional, 1996.

[4] 邹 毅,朱晓萍,霍 龙. 一种改进粒子群算法及其应用[J]. 沈阳工程学院学报,2006,3(2):283 - 286.

[5] 张雪东,赵传信,季一木. 一种混合粒子群算法及其在 Job Shop 问题中的应用[J]. 计算机技术与发展,2006,16(9):109 - 111.

[6] 曾万里,危韧勇,陈红玲. 基于改进 PSO 算法的 BP 神经网络的应用研究[J]. 计算机技术与发展,2008,18(4):49 - 51.

[7] 雷德明. 利用混沌搜索全局最优解的混合遗传算法[J]. 系统工程与电子技术,1999,21(12):81 - 83.

[8] 张春慨,王亚英. 混沌在实数编码遗传算法中的应用[J]. 上海交通大学学报,2000,12(12):1658 - 1660.

[9] Ye Luqing, Wang Shengtie. Control Maintenance Strategy for Fault Tolerant Mode and Reliability Analysis of Hydro Power Stations[J]. IEEE Transactions on Power Engineering, 2001, 16(3):340 - 345.

[10] Wang Shengtie, Ye Luqing, Malik O P. Intelligent Networked (N + M) Fault Tolerant Systems for Hydro Power Stations [J]. Electric Power Systems Research, 2001, 8(59):39 - 45.

(上接第 17 页)

操作,避免遭受 DoS 攻击。

根据以上的分析不难看出,ESP 所提供的功能涵盖了 AH 的功能,只需要对 ESP 的认证范围稍加修改,使它在原有安全服务的基础上提供对整个 IP 数据报的认证,就可以完全实现 AH 的功能,从而取代 AH 协议。为此,基于简化 IPSec 体系结构,提高安全协议运行效率的思想,笔者建议不妨考虑通过取消 AH 协议来实现对 IPSec 体系结构的简化。

5 结束语

AH 和 ESP 作为 IPSec 中的两个非常重要的安全协议,已经在 IPv4 和 IPv6 的网络中得到了重要的应用,但是从开始设计 IPSec 协议的那一天起,IPSec 体系结构就走向了日趋复杂的境地,变得越来越庞大而不合理[9]。目前,人们对 IPSec 的研究,不论是理论研究还是应用研究都还在不断地进行中,特别是在 IPv6 环境中的研究还有许多工作要做。简化、改进 IPSec 现有的体系结构,是 IPSec 研究的重点和难点,也是基础性的工作。文中仅对 AH 和 ESP 两者的区别和联系进行了分析,并提出了不妨取消 AH 协议的建议,这是一个值得进一步探讨的问题。

参考文献:

[1] 关 慧,刘 俊,曹连刚. 基于 IPv6 - IPSec 的网络安全访问的实现[J]. 微计算机信息,2008,24(2 - 3):95 - 96.

[2] IPv4 到 IPv6:互联网的发展趋势[EB/OL]. 2007 - 03 - 02. http://www.51cto.com/art/200703/41354.htm.

[3] 蓝集明,张海燕. 对 IPv4/IPv6 过渡技术的分析与研究[J]. 电脑知识与技术,2008,4(7):1885 - 1886.

[4] Kent S. RFC 4302: IP Authentication Header[S]. 2005.

[5] Kent S, Seo K. RFC 4301: Security Architecture for the Internet Protocol[S]. 2005.

[6] Kent S. RFC 4303: IP Encapsulating Security Payload (ESP) [S]. 2005.

[7] 李振强,赵晓宇,马 严. IPv6 技术揭秘[M]. 北京:人民邮电出版社,2006:225 - 280.

[8] 江 伟,苏本跃,周 健. IPSec 在基于 IPv6 的校园网安全中的应用研究[J]. 计算机技术与发展,2007,17(2):229 - 230.

[9] 黄 智,龚向阳,阙喜戎,等. IPSec 协议的研究和分析[J]. 计算机工程与应用,2002,39(11):160 - 162.