

IPSec 在基于 IPv6 的校园网安全中的应用研究

江 伟¹ 苏本跃¹ 周 健²

(1. 安庆师范学院 计算机与信息学院 安徽 安庆 246011 ;

2. 合肥工业大学 网络信息中心 安徽 合肥 230009)

摘 要 当前 IPv4 的地址空间不足是制约互联网发展的主要矛盾 ,采用 IPv6 已是大家的共识并将首先在校园网进行实验和广泛使用。文中主要探讨基于 IPv6 的校园网安全建设 ,通过对 IPv6 的安全机制和 IPSec 的分析 ,探讨了它在校网安全建设中的应用方法。

关键词 :IPv6 ;IPSec ;校园网 ;网络安全

中图分类号 :TP393.08

文献标识码 :A

文章编号 :1673-629X(2007)02-0229-04

Research on Application of IPSec at Campus Network of IPv6

JIANG Wei¹ ,SU Ben-yue¹ ,ZHOU Jian²

(1. School of Computer & Information ,Anqing Teachers College ,Anqing 246011 ,China ;

2. Network & Information Center ,Hefei University of Technology ,Hefei 230009 ,China)

Abstract Now the insufficience of IPv4 's address is a primary contradiction restricting the development of Internet. It 's been the consistent understanding that have to use IPv6. IPv6 will first be experimented and widely used at the campus network. The paper primarily studies the safety construction of the campus network based on IPv6. According to the analysis of the safety mechanism of IPv6 and IPSec ,the paper discusses its application methods of the safety construction at the campus network.

Key words :IPv6 ;IPSec ;campus network ;network safety

1 IPv6 及其发展历史

20 世纪后期 Internet 的大发展及在中国等发展中国家的广泛应用 ,带来用户数的迅速增加 ,并导致传统的 IPv4 网络地址严重不足。众所周知 ,由于历史的原因 ,1973 年提出的 IPv4 协议使用的是 32bit 地址域 (因为当时的 ARPANET 网络只需支持 250 个站点和 750 个计算机的互联 ,32 位即 2^{32} 个 IP 地址 ,可分配超过 40 亿台主机 ,对于当时来说 ,已经是个天文数字了)。时过境迁 ,当时提出 IPv4 的人肯定无法想到 ,这样庞大的地址体系 ,地址如今正面临枯竭 ,发展陷入困境。据 Internet 网络地址分配的管理机构 INTERNIC 预测 ,IPv4 协议地址空间将在 2010 年左右使用殆尽。

在此基础上 ,研究人员考虑从本质上来改进甚至替换 IP 协议以解决这一迫在眉睫的问题。1990 年后 ,IETF 开始了一项长期的工作 ,即研究和制定下一

代网络协议 (IPng) 选择接替现行的 IPv4 协议。此后 ,人们开展了许多工作 ,以解决 IPv4 地址的局限性 ,同时提供额外的功能。1994 年 9 月 IETF 提出了 the Recommendation for the IP Next Generation Protocol 草案 ,并在 1995 年底确定了 IPng 协议规范 ,称为 IP 版本 6 (即 IPv6)。1996 年 IPv6 的基本协议规范发表 ,1998 年发表了 IPv6 修订版。

IPv6 提出的最初目的是为了获得更多的 IP 地址 ,但随着 IPv4 的大量应用而产生了新技术 ,IPv6 在标准逐渐形成和完善的过程中 ,就吸收这些技术 ,使之成为自己的基本配置 ,丰富了自己的功能。概括地说 ,IPv6 具有以下特点 :

(1) 地址容量大大扩展 ,由原来的 32 位扩充到 128 位 ,彻底解决了 IPv4 地址不足的问题。IPv4 是在 32 位处理器普遍使用的基础上得到最大应用的 ,因此 ,从某种意义上来说 ,当 128 位处理器得到应用时 ,就意味着 IPv6 的到来。

(2) 提供更灵活的分层地址结构组织方式 ,从而更易于寻址 ,同时提供新的地址分配方案 ,减少了路由表大小 ,加快了路由器和交换机的数据处理速度 ,扩展支

收稿日期 :2006-04-30

基金项目 :安徽省高校青年教师科研资助计划项目 (2006jq1209) ;安徽省教育厅自然科学基金项目 (2006KJ252B)

作者简介 :江 伟 (1976-) ,男 ,安徽安庆人 ,讲师 ,硕士 ,研究方向为下一代互联网技术、网络安全。

持组播和任播地址,使得数据包可以发送给任何一个或一组节点。

(3)提供 Internet 和 Intranet 统一的地址方案;大容量的地址空间可以实现无状态地址自动配置,使基于 IPv6 的终端能够快速连接到网络上而无需人工配置,实现了真正的即插即用。

(4)报头格式大大简化,从而有效减少路由器或交换机对报头的处理开销,这对设计硬件报头处理的路由器或交换机十分有利。

(5)加强了对扩展报头和选项部分的支持,这除了让转发更为有效外,还对将来网络加载新的应用提供了充分的支持。

(6)流标签的使用,使得为数据包所属类型提供个性化网络服务成为可能,并有效保证了相关业务的服务质量。

(7)把 IPSec 作为必备协议,保证了网络层端到端通信的完整性和机密性,提供了认证与私密性。

(8)在移动网络和实时通信方面有很多改进,特别是强大的自动配置能力,可简化移动主机和局域网系统的管理。这一点是 IPv4 不能比拟的^[1]。

从 IPv4 向 IPv6 的转变也是国内校园网建设的趋势。2004 年 12 月 25 日,是我国互联网发展历史上值得铭记的一天。这一天,国家发改委、教育部等 8 部委联合宣布,中国第一个下一代互联网暨中国下一代互联网(CNGI)示范工程核心网(CERNET2)正式开通,这是世界上规模最大的纯 IPv6 互联网,标志着我国下一代互联网建设全面拉开序幕,并在世界下一代互联网发展上取得先机。第二代中国教育和科研计算机网(CERNET2)是“中国下一代互联网示范工程”中最大的核心网和唯一的学术网,它以每秒 10G 的传输速率(相当于每秒传送 15 个 VCD 光盘存储的信息)连接全国 20 个主要城市的核心节点,为全国几百所高校和科研单位提供高速 IPv6 网络接入服务,并高速连接国内外下一代互联网。与此同时,针对 IPv6 开展科学研究的高校实验室纷纷成立,如清华大学 IPv6 网络实验室、北航 IPv6 网络实验室、西安交大 IPv6 网络实验室、兰州大学 IPv6 网络实验室、兰州理工大学 IPv6 网络实验室等。可以预见,IPv6 在国内各高校普及的日期已经为时不远了。然而与此同时,网络发展所带来的安全性问题就象现在的 Internet 一样应该成为人们不得不提前考虑和研究的问题^[2]。

2 IPv6 的安全机制和 IPSec 的功能研究

在 Internet 网络上,网络安全性已经成为一个敏感而又重要的问题。但是过去人们认为安全性议题在

网络协议层的底层并不重要,安全性的责任应该在应用层,因此,IPv4 在网络安全性方面只具备最少的安全性选项,并不能提供有效的安全服务。特别是随着 EDI(电子数据交换)的兴起和应用的不断增加,要使得 Internet 网络仍能成为信息高速公路的重要组成部分,能够支持不同的应用系统的话,数据安全性问题是必须解决的。尤其对于像 EDI 这样的应用系统,数据出错可能会导致一个企业的破产,安全性的要求更加迫切。从 1995 年开始, IETF 着手研究制定了一套用于保护 IP 通信的 IP 安全(IPSECURITY, IPsec)协议, IPv6 的实现即遵循 IPsec 体系结构。

IPsec 使用 IP 身份验证头 AH(Authentication Header)和 IP 封装安全性净荷 ESP(Encapsulating Security Payload),并且提供了认证和加密两种机制。在 IPv4 中,它是一个可选扩展协议,但在 IPv6 中,却是一个重要组成部分,IPv6 是通过两个专用的扩展标题将其列入的。AH 用来确认 IP 信息包的可靠性和完整性,保护网络不受固定字段的非法修改和信息包电子欺骗的威胁,它定义了认证的应用方法;而 ESP 则提供数据加密封装,确保只有目的接口才可阅读由 IP 信息包发送的有效数据,它定义了加密和可选认证的应用方法。由此可看出, AH 和 ESP 都提供了认证服务,不过 AH 提供的认证服务要强于 ESP。它们既可以分别单独使用,也可以一起使用,提供更高的保密强度。一方面, IPv6 数据包的接收者可以要求发送者首先利用 AH 进行“登录”,确认数据发送方的真实身份以及数据在传输过程中是否被改动,然后才决定是否接收数据包,并且这种接收是算法独立的,可以有效地防止网络“黑客”的攻击。另一方面,利用 ESP 加密数据包,这种加密也是算法独立的,这意味着可以安全地在 Internet 上传递敏感数据,不用担心被第三方截取^[3-4]。

在一个特定的 IP 通信中使用 AH 或 ESP 时,协议将与一组安全信息和服务发生关联,称为安全关联(SA, Security Association)。SA 可以包含认证算法、加密算法、用于认证和加密的密钥。IPsec 使用一种密钥分配和交换协议如 Internet 安全关联和密钥管理协议(ISAKMP, Internet Security Association and Key Management Protocol)来创建和维护 SA。SA 是一个单向的逻辑连接,也就是说,两个主机之间的认证通信将使用两个 SA,分别用于通信方和接收方^[5]。

作为 IPv6 的一个重要组成部分, IPsec 是一个网络层协议。它只负责其下层的网络安全,并不负责其上层应用的安全,如 Web、电子邮件和文件传输等。也就是说,要验证一个 Web 会话,依然需要使用 SSL 协

议。不过 ,TCP/IPv6 协议簇中的协议可以从 IPSec 中受益 ,例如 ,用于 IPv6 的 OSPF 路由协议就去掉了用于 IPv4 的 OSPF 中的认证机制。总而言之 ,AH 和 ESP 使得 IPv6 的 Internet 具有潜在的端到端的安全性。

3 IPSec 的工作方式

IPSec 有两种工作方式 :传输模式(Transport Mode)和隧道模式(Tunnel Mode) ,AH 和 ESP 均可应用于这两种方式。传输模式通常应用于主机之间端对端通信 ,该方式要求主机支持 IPSec ,也就是说在它需要重构机器的通信协议栈之上 ,在原 IP 栈之上加载 IPSec 或者重构 IP 协议使其支持 IPSec。隧道模式应用于网关模式中 ,即在主机的网关(防火墙、路由器)上加载 IPSec ,这个网关就同时升级为安全网关(Security Gateway ,SG)。

(1)传输模式。

传输模式主要为上层协议提供保护 ,AH 和(或)ESP 包头插入在 IP 包头和传输层协议包头之间。其包结构如图 1 所示 ,显然传输模式下 ESP 并没有对 IP 包头加密处理 ,源、目的 IP 地址内容是可见的。传输模式用于两台主机之间 ,实现端到端的安全。它所保护的数据包的终点也是 IPSec 的终点。当数据包从传输层传递给网络层时 ,AH 和 ESP 会进行拦截 ,在 IP 头上与上层协议头之间插入一个 IPSec 头(AH 头或 ESP 头)。当同时应用 AH 和 ESP 传输模式时 ,应首先应用 ESP ,再用 AH ,这样数据完整性可应用到 ESP 载荷。

原 IP 包 :

原始 IP 头	传输层包头	数据
---------	-------	----

传输模式应用 AH 后 :

原始 IP 头	AH	传输层包头	数据
---------	----	-------	----

传输模式应用 ESP 后 :

原始 IP 头	ESP 头	传输层包头	数据	ESP 尾	ESP 认证
---------	-------	-------	----	-------	--------

图 1 传输模式包结构图

(2)隧道模式。

在隧道模式下 ,整个 IP 包都封装在一个新的 IP 包中 ,并在新的 IP 包头和原来的 IP 包头之间插入 IPSec 头(AH/ESP)。其结构如图 2 所示。

隧道模式应用 AH 后 :

新 IP 头	AH	原始 IP 头	传输层包头	数据
--------	----	---------	-------	----

隧道模式应用 ESP 后 :

新 IP 头	ESP 头	原始 IP 头	传输层包头	数据	ESP 尾	ESP 认证
--------	-------	---------	-------	----	-------	--------

图 2 隧道模式包结构图

从图 2 可以看出 ,在隧道模式下 ,如果应用了

ESP ,原始 IP 包头是加密的 ,真正的源、目的 IP 地址是隐藏的 ,新 IP 头中指定的源、目的 IP 地址一般是源、目的安全网关的地址。隧道模式对整个原始数据报提供了所需的服务 ,用于主机与路由器或两台路由器之间。该模式的通信终点由受保护的内部 IP 头指定 ,而 IPSec 终点则由外部 IP 头指定。如果 IPSec 终点为安全网关 ,则该网关会还原出内部 IP 包 ,并将其转发至最终目的地。IPSec 还支持隧道的嵌套 ,即对已隧道化的数据再进行隧道化处理^[6]。

4 IPSec 在校园网安全中的应用

基于 IPv6 的校园网安全机制中 ,IPSec 在 IP 层上对数据包进行高强度的安全处理 ,使用 AH 报头和 ESP 报头来保护 IP 通信安全 ,其安全机制在校园网络的各种不同层次中都得到应用。

(1)应用程序级的安全应用 :网络应用程序运行在 IPv6 的顶层 ,应用程序选择通信通道进行数据传输 ,在传输层指定通道的安全特性 ,数据在通道中传输 ,AH 和 ESP 对数据加以保护 ,保证原始的身份验证和数据完整性 ,接收主机从安全通道接收到数据后 ,再结合其他的安全机制完成数据的可靠传输。如图 3 所示 ,主机 A、B 分别位于两个不同的路由器(网关)C、D 内 ,C、D 通过校园网相连 ,主机 A、B 均配置了 IPSec。路由器(网关)C、D 都未应用 IPSec ,主机 A、B 可以单独使用 AH 和 ESP ,也可以将两者结合使用 ,使用的模

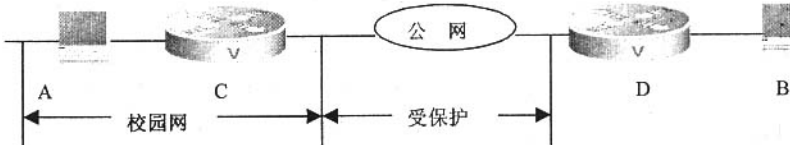


图 3 应用程序级的安全保护

式既可以是传输模式也可以是隧道模式。

(2)路由安全应用 :在 IPv6 中 IP 地址大多进行动态自动配置 ,通过 AH 和 ESP 报头 ,合适的组合应用到路由交换的信息上 ,如路由宣告信息、邻居宣告信息、Internet 控制报文协议等 ,防止伪造消息伪造路由器 ,保证不受错误 ICMP 的侵害 ,从而有效防止对网络逻辑结构的攻击破坏 ,这种通用的方案比特定为某种路由协议设计的身份验证机制显然具有优势^[7]。

如图 4 所示 ,与路由器(网关)相连的内部网一端 ,是一个受保护的校园网络 ,另一端则是不安全的公用或专用网络 ,例如 Internet。两个这样的路由器(网关)建立起一个安全通道 ,通信就可以通过这个通道从一个本地受保护子网发送到另一个远程保护子网 ,这样就形成了一个 VPN。路由器(网关)C、D 上运行隧道模式 ESP ,保护两个网内的主机通信 ,所有主机可不必

配置 IPSec。当主机 A 要向主机 B 发送数据包时,路由器(网关)C 要对数据包进行封装,封装后的包通过隧道穿越公用网络后到达路由器(网关)D,由 D 对该数据包解封,再转发给主机 B。反之亦然。

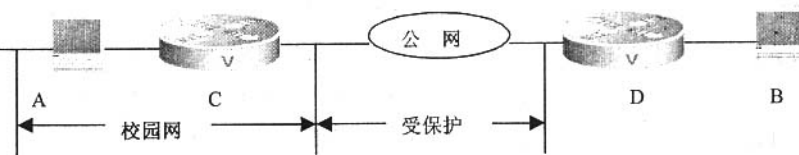


图 4 路由级的安全保护

除此之外,还可以通过隧道嵌套的方式实现网络安全。当配置了 IPSec 的主机通过隧道接入到配置了 IPSec 网关的路由器,并且该路由器作为外部隧道的终结点将外部隧道封装剥除时,嵌套的内部安全隧道就构成了对内部网络的安全隔离。

5 结束语

由于 IPSec 提供了两种工作模式:传输模式和隧道模式。再结合 AH 和 ESP 提供的不同的安全服务,在 IPSec 的实际应用中就有了多种选择。总的说来,ESP 隧道模式认证和加密服务所提供的安全性要强于传输模式,但由于隧道模式将比传输模式服务占用更多带宽,所以如果在带宽利用率非常重要的情况下,传输模式可能是更合适的选择。另外,尽管理论上 ESP 隧道模式认证提供的安全服务不如 AH 传输模式的安全性高,但由于包含 IP 数据包源地址的内部 IP 头被

加密了,因此,它可以提供一定的数据流保密服务,而这是 AH 所不具备的。

未来几年里,基于 IPv6 的校园网建设将是大势所趋,而校园网安全机制研究也是重中之重。IPv6 作为新一代的网络互连协议是一个建立可靠的、可管理的、安全和高效的 IP 网络的长期解决方案,其先进性和灵活性正在得到越来越多人的认可。从技术上看,并不是使用了 IPv6 就能彻底保证安全,因为 IPv6 虽然内在具有一些安全的特性,但是应用系统、各种各样的基础设施,要充分利用这些特性才行。

参考文献:

- [1] 华为 3COM 技术有限公司. IPv6 技术[M]. 北京:清华大学出版社,2004.
- [2] 江伟. 基于 Linux 的 IPv4 和 IPv6 的互连研究[D]. 合肥:合肥工业大学,2005.
- [3] Kent S, Athinson R. RFC2403. IP Encapsulating Security Payload[S]. 1998.
- [4] Kent S, Athinson R. RFC2402. IP Authentication for the Internet Protocol[S]. 1998.
- [5] Kent S, Athinson R. RFC2401. Security Architecture for the Internet Protocol[S]. 1998.
- [6] 陈卓. IPsec 中 ASP 和 ESP 协议的比较与应用[J]. 计算机应用与软件,2004(7):105-106.
- [7] 刘玉山. IPsec 原理及其在网络安全中的应用[J]. 山东电子,2004(1):39-41.

(上接第 127 页)

报识别模块,数据库存储模块(包括程序与数据库数据同步部分)。

4 总结

两类通信总线的结合使用节约了成本也使系统层次更为突出,加入调度算法后的数据通信,增强了数据的可靠性和实时性。可配制和智能化可自动识别的数据格式使系统更具适用性。系统的数据采集与处理部分具有以下特点:

* 当硬件变动和通道使用情况变更时,保证用户最小程度上的配置变动,安装简便。

* 数据调度使数据冲突概率减小,通信更具实时性,通信更安全。

* 采样时间由用户自定义,根据采样时间的间隔适应不同数据通道、仪表,甚至不同采油站点对数据通信实时性的不同要求。

* 系统具有较好的可扩展性,简单配置就可以增

加需要采样的输油管线,增加采样管线,管线需要采样的数据类型,以及为某个数据采样点增设多条采样备用管道。

* 具有智能的用户连接,能自动断开和恢复与服务

参考文献:

- [1] 缪学勤. 论六种实时以太网的通信协议[J]. 自动化仪表,2005,26(4):26-31.
- [2] 杨仕平,桑楠,熊光泽. 基于 Ethernet 技术的安全关键实时网络[J]. 软件学报,2005,16(1):121-134.
- [3] 冯冬琴,廖智军. 基于以太网的工业控制网络实时通信模型研究[J]. 仪器仪表学报,2003,24(4):714-718.
- [4] 王智,王天然,孙优贤. 工业实时通讯网络(现场总线)的基础理论与现状(上)[J]. 信息与控制,2002,31(2):146-163.
- [5] 陈积明,王智, Song Ye-qiong, 等. 基金会现场总线非周期实时信息的调度问题研究[J]. 浙江大学学报,2003,37(3):273-277.