# IPv6的安全协议研究

沈 莉*

(四川师范大学计算机科学学院 成都 610066)

【摘要】IPv6的安全协议研究从IPSec协议的安全体系、工作原理、工作模式、主要协议、解决安全问题的实现方法以及在VPN飞速发展中的应用等方面对IPv6的安全协议进行分析，用IPSec的AH协议及ESP协议针对IP层的认证、加密解决现有网络安全机制只能在应用层对数据进行保护而不能实现对IP层保护的问题。

关 键 词 安全; 协议; IPv6安全协议; 认证协议头; 安全加载封装

中图分类号 TP309

## 1 提出问题

目前Internet正与电话网、电视网、无线网、卫星网相结合，在商业运作的驱动下，更加迅猛地发展，对安全性的要求也越来越高。可现有的安全机制只建立于应用程序级，无法从IP层来保证Internet的安全。其实IP层是一个附加安全措施的好场所，因为IP层处于整个协议体系的中间点，既能捕获所有从高层来的报文，也能捕获所有从低层来的报文；从IP层的定义来看，在这一层附加安全措施是与低层协议无关的，可对高层协议和应用进程透明。所以，从IP层提供安全保障越来越受到重视，而IPSec也就脱颖而出了。

## 2 IPSec协议简介

IPSec(IP Security)产生于IPv6的制定之中，用于提供IP层的安全性。由于所有支持TCP/IP协议的主机进行通信时都要经过IP层的处理，所以提供了IP层的安全性就相当于为整个网络提供了安全通信的基础。

### 2.1 IPSec的安全体系

IPSec是由IETF下属的一个IPSec工作组起草的，在IP协议层上保证数据分组在Internet网络中具有互操作性、高可靠性和基于密码技术的安全服务标准。IPSec的有关标准以请求注释(RFC)的方式予以公开，这些标准由RFC1825(Internet协议安全体系结构)、RFC1826(IP鉴别头)、RFC1827(IP封装安全载荷)及用于鉴别和封装载荷的若干算法标准构成一个体系。

### 2.2 IPSec的工作原理

IPSec的工作原理类似于包过滤防火墙，可以看作是对包过滤防火墙的一种扩展。当接收到一个IP数据包时，包过滤防火墙使用其头部在一个规则表中进行匹配。当找到一个相匹配的规则时，包过滤防火墙就按照该规则制定的方法对接收到的IP数据包进行处理。

## 3 IPSec的主要协议

在IPSec中由三个主要协议来提供认证、数据完整、机密性三种保护形式，分别为认证协议(AH)、安全加载封装(ESP)和Internet密钥交换协议(IKE)。需要先引入一个非常重要的术语——SA(Security Association安全关联)[1]。所谓安全关联是指安全服务与它服务的载体之间的一个“连接”。AH和ESP

2001年11月14日收稿

* 女 24岁 硕士

都需要使用SA，而IKE的主要功能就是SA的建立和维护。

### 3.1 AH

AH是在所有数据包头加入一个密码。AH通过一个只有密钥持有人才知道的"数字签名"来对用户进行认证。这个签名是数据包通过特别的算法得出的独特结果；AH还能维持数据的完整性，因为在传输过程中无论多小的变化被加载，数据包头的数字签名都能把它检测出来。由于AH不能加密数据包所加载的内容，因而它不保证任何的机密性。两个最普遍的AH标准是MD5和SHA-1，MD5使用最高到128位的密钥，而SHA-1通过最高到160位密钥提供更强的保护。

### 3.2 ESP

ESP通过对数据包的全部数据和加载内容进行全加密来严格保证传输信息的机密性，可以避免其他用户通过监听来打开信息交换的内容，因为只有受信任的用户拥有密钥打开内容。ESP也能提供认证和维持数据的完整性，最主要的ESP标准是数据加密标准(DES)，DES最高支持56位的密钥，而Triple-DES使用三套密钥加密，相当于使用最高到168位的密钥。由于ESP实际上加密所有的数据，因而比AH需要更多的处理时间，从而导致性能下降。

### 3.3 IKE

IKE协议主要是对密钥交换进行管理，它主要包括对使用的协议、加密算法和密钥进行协商；方便的密钥交换机制；跟踪对以上这些约定的实施三个功能。

### 3.4 封装及处理过程

#### 3.4.1 Ah头的处理

AH只涉及到认证，不涉及到加密，实现和处理都比ESP简单。封装：原节点选择恰当的协议模式和验证算法，以32位字的形式封装成AH扩展头后，并将其前一扩展头的“下一个头”字段标为51，然后插在IPv6报头的合适位置。接收：目标节点在接收到含有AH头的IP包后，检查是否是分段的IP包，如果是则将其保留下来，直到这个包的其他分段都收齐时，重新组合成一个完整的IP包。根据AH头中的SPI检查对应的SA是否存在，如果不存在，则丢弃此包。再根据序列号检查是否是重播的包，如果是，同样丢弃此包，否则将这个完整的包传递到身份验证器(存在于相应的SA中)中进行身份验证，并将验证出的结果数据与从包中提取出的身份验证数据进行比较，如果一致，接收并拆封IP包，否则，发送错误信息并丢弃IP包。

#### 3.4.2 ESP头的处理

ESP的处理涉及到加、解密，类似AH头的处理。封装[4]：选取恰当的协议模式和验证算法，根据ESP报文的内容和格式进行封装，最后重新计算位于ESP前面的IP头的校验和，形成最终的IP包。接收[3]：目标节点在接收到含有ESP头的IP数据包后，如果收到的是一个分段，必须将其保留下来，直到这个报的其他分段都收齐为止，并装配成一个完整的IP包。根据ESP头中的SPI检查对应的SA是否存在，如果不存在，则丢弃此IP包。再根据序列号检查此包是否是重播的包，如果是，同样丢弃此包，否则，利用相应的密钥(密钥的交换、管理由IKE协议负责)，将这个完整的包传递到身份验证器(存在于相应的SA)中进行身份验证[2]，并将验证出的结果数据与包中的身份验证数据进行比较，如果一致，则从SA中取出密钥和解密算法对IP包进行解密。否则，丢弃此包。当身份验证和解密成功之后，对结果数据包进行模式检查，检查此包与SA中标明的模式(隧道模式或传送模式)是否相符，否则，便将此包丢弃。最后，对此包进行正确性验证和拆封还原，得到真实的原始数据。由数据包的处理过程可以看到IPSec已经实现了IP层的数据安全保护。

## 4 IPSec的工作模式

IPSec的工作模式分为传送模式和隧道模式。

传送模式：使用原明文IP头，在IP层对上层TCP或UDP的协议数据单元进行封装，并根据具体

配置提供安全保护，通常当ESP在一台主机(客户机或服务器)上实现时使用，其结构如图1所示。

隧道模式：通常当ESP在关联到多台主机的网络访问介入装置实现时使用。保护整个IP数据包，包括全部TCP/IP或UDP/IP头和数据，用自己的地址作为源地址加入到新的IP头。当它用在用户终端设置时，可提供更多的便利来隐藏内部服务器主机和客户机的地址，其结构如图2所示。


图1 传输模式IP包结构


图2 隧道模式IP包结构

## 5 IPSec解决的安全问题的应用分析

目前可以用于实现VPN的技术很多，其中IPSec是主要用于在网络层实现VPN的技术。所谓VPN(虚拟私有网络)是指将物理上分布在不同地点的网络通过公用骨干网联接而成逻辑上的虚拟子网[1]，这里的公用网主要指Internet。为了保障信息在Internet上传输的安全性，VPN技术采用了认证、存取控制、机密性、数据完整性等措施，以保证了信息在传输中不被偷看、篡改、复制。由于使用Internet进行传输相对于租用专线费用极为低廉，所以VPN的出现使企业通过Internet既安全又经济地传输私有的机密信息成为可能。简单地说，IPSec在实现数据通信的两端提供安全的数据传输隧道。由自己定义哪些数据包应该受到保护，应该被放在安全隧道中传输。通过标识隧道的安全属性，可以定义用于保护这些敏感数据的安全参数。更精确地说，这些安全的数据传输隧道是建立在两个IPSec对端的一系列SA上，这些安全关联参数定义了哪些协议和算法可以被应用到敏感数据，IPSec对端应用的密钥等。IPSec的实现是靠两个IPSec的对端维系的，因此实际上是一种端到端的安全实现，从技术的角度上说，在端到端客户的路由器上实现是最安全合理的方式，中间任何一个路由器都不需要做相应设置。因此，IPSec实现的是一种与接入网络无关的VPN技术，已完成了标准化的工作，可以对VPN提供安全保障。

## 6 结 束 语

从IPSec协议数据包处理过程可以看出，拥有IP级的安全保护已经成为事实。IPSec在为VPN提供安全保障的同时，还可为各种分布式应用，包括远程登录、客户/服务器、电子邮件、文件传输、Web访问等提供安全，可保证LAN、专用和公用WAN以及Internet的通信安全。因为所有由网络管理员指定的通信都是经过加密和认证的，所以IPSec的使用就可以使其安全级别在原有的基础上更进一步。

## 参 考 文 献

1　Carlton R, Davis. IPSec：VPN的安全实施. 北京：清华大学出版社，2002

2　Naganand Doraswamy, Dan Harkins. IPSEC新一代因特网安全标准. 北京：机械工业出版社，2000

3　王茂忠，方志聪，周明天. 基于IPv6的安全机制. 电脑技术信息, 2000, (11): 30-31

4　秦忠林，黄本雄. IPSEC研究及实现. 计算机应用，2001，21(4): 25-27

# The Research About Secure Protocol of Ipv6

Shen　Li

(Sichuan Normal University Institute of Computer Science　Chengdu　610066)

**Abstract**　The research about secure protocol of IPv6 discusses the IPv6's secure protocol in aspects of IPSec's secure systems, the working principles, the working patterns, the methods of solving the secure problem and the application of it in VPN. IPSec's AH and ESP protocols provide authentication and encoding for IP layer's transmission. This character can solve the problem that today's secure system which can not protect the data in the IP layer but can protect the data in the application layer.

**Key words**　security;　protocol;　IPSec;　authentication header;　encapsulating security payload

---

**(上接第56页)**

# Design Oriented-object Relative Data Base

Chen Wenyu

(College of Computer Scince and Engineering，UEST of China　Chengdu　610054)

**Abstract**　Based on the character of oriented-object and relative data base management system，we can join the oriented-object technology to relative data base .The system supports the SQL，complex object and the complex action of complex objects. It is the rejoin of oriented-object technology and trade relative data base technology. It has the strong function of relative data base and the model function of object. This paper supply the method of the relative data base design and map object to relative data base. The method is easy and useful.

**Key words**　oriented-object;　relative data base;　map;　object oriented