第 3 章　网络层安全协议

IP 网络安全一直是一个备受关注的领域，如果缺乏一定的安全保障，无论是公共网络还是企业专用网络，都难以抵挡网络攻击和非法入侵。对于某个特定的企业内部网 Intranet 来说，网络攻击既可能来自网络内部，也可能来自外部的 Internet，其结果均可能导致企业内部网络毫无安全性可言，单靠口令访问控制不足以保证数据在网络传输过程中的安全性。

3.1　网络攻击与防御

3.1.1　常见的网络攻击

如果没有适当的安全措施和安全的访问控制方法，在网络上传输的数据很容易受到各式各样的攻击。网络攻击既有被动型的，也有主动型的。被动攻击通常指信息受到非法侦听，而主动攻击则往往意味着对数据甚至网络本身恶意的篡改和破坏。以下列举几种常见的网络攻击类型。

1. 窃听

一般情况下，绝大多数网络通信都以一种不安全的“明文”形式进行，这就给攻击者很大的机会。只要获取数据通信路径，就可轻易“侦听”或者“解读”明文数据流。窃听型攻击者虽然不破坏数据，却可能造成通信信息外泄，甚至危及敏感数据安全。对于多数普通企业来说，这类网络窃听行为已经构成网管员面临的最大的网络安全问题。

2. 数据篡改

网络攻击者非法读取数据后，下一步通常就想去篡改它，而且这种篡改一般可以做得让数据包的发送方和接收方无知无觉。但作为网络通信用户，即使并非所有的通信数据都是高度机密的，也不想看到数据在传输过程中出现任何差错。比如在网上购物，一旦我们提交了购物订单，谁也不希望订单中的任何内容被人肆意篡改。

3. 身份欺骗（IP 地址欺骗）

大多数网络操作系统使用 IP 地址来标识网络主机。然而，一些貌似合法的 IP 地址很有可能是经过伪装的，这就是所谓的 IP 地址欺骗，也就是身份欺骗。另外，网络攻击者还可以使用一些特殊的程序，对某个从合法地址传来的数据包做些手脚，借此合法地址来非法侵入某个目标网络。

4. 盗用口令攻击(Password-Based Attack)

基于口令的访问控制是一种最常见的安全措施。这意味着对某台主机或网络资源的访问权限决定于谁,也就是说,这种访问权是基于用户名和账号密码的。

攻击者可以通过多种途径获取用户合法账号,一旦拥有了合法账号,也就拥有了与合法用户同等的网络访问权限。因此,假设账号被盗的用户具有网管权限,攻击者甚至可以借机给自己再创建一个合法账号,以备后用。有了合法账号进入目标网络后,攻击者也就可以随心所欲地盗取合法用户信息以及网络信息;修改服务器和网络配置,包括访问控制方式和路由表;篡改、重定向、删除数据等。

5. 拒绝服务攻击(Denial-of-Service Attack)

与盗用口令攻击不同,拒绝服务攻击的目的不在于窃取信息,而是要使某个设备或网络无法正常运作。在非法侵入目标网络后,这类攻击者惯用的攻击手法如下。

(1) 首先设法转移网管员注意力,使之无法立刻察觉有人入侵,从而给自己争取时间。

(2) 向某个应用系统或网络服务系统发送非法指令,致使系统出现异常行为或异常终止。

(3) 向某台主机或整个网络发送大量数据洪流,导致网络因不堪过载而瘫痪。

(4) 拦截数据流,使授权用户无法取得网络资源。

6. 中间人攻击(Man-in-the-Middle Attack)

顾名思义,中间人攻击发生在用户与通信对象之间,即通信过程以及通信数据遭到第三方的监视、截取和控制,例如攻击者可以对数据交换进行重定向等。如果通信中使用网络底层协议,通信两端的主机是很难区分出不同对象的,因此也不大容易察觉这类攻击。中间人攻击有点类似于身份欺骗。

7. 盗取密钥攻击(Compromised-Key Attack)

一般来说,盗取密钥是很困难的,但并非不可能。通常把被攻击者盗取的密钥称为“已泄密的密钥”。攻击者可以利用这个已泄密的密钥,对数据进行解密和修改,甚至还能试图利用该密钥计算其他密钥,以获取更多加密信息。

3.1.2 防御方法及优点

1. 边界防御

众所周知,网络攻击常常可能导致系统崩溃及敏感数据的外泄,因此数据资源必须受到足够的保护,以防被侦听、篡改或非法访问。

常规网络保护策略有使用防火墙、安全路由器(安全网关)以及对拨号用户进行身份

认证等。这些措施通常被称为“边界保护”，往往只着重于抵御来自网络外部的攻击，但不能阻止网络内部的攻击行为。例如，一台主机由多个用户共享，往往会发生人不在了，而机器却仍处于登录状态的情况，从而导致系统出现不安全因素。访问控制法最大的缺陷是一旦用户账号被窃，就根本无法阻止攻击者盗取网络资源。

还有一种比较少见的保护策略是物理级保护，就是保护实际的网络线路和网络访问结点，禁止任何未经授权的使用。但采用这种保护方式，当数据需要从数据源通过网络传输到目的地时，无法做到保证数据的全程安全。

2. 用 IPSec 抵御网络攻击

IPSec 采用端到端加密模式，基本工作原理是发送方在数据传输前（即到达网线之前）对数据实施加密。在整个传输过程中，报文都是以密文方式传输，直到数据到达目的结点，才由接收端进行解密。IPSec 对数据的加密以数据包而不是整个数据流为单位，这不仅更灵活，也有助于进一步提高 IP 数据包的安全性。通过提供强有力的加密保护，IPSec 可以有效防范网络攻击，保证专用数据在公共网络环境下的安全性。

一个完善的企业安全计划，应该是多种安全策略的有机组合，将 IPSec 与用户访问控制、边界保护以及物理层保护相结合，可以为企业数据通信提供更高层次的纵深防护。网络攻击者要破译经过 IPSec 加密的数据，即使不是完全不可能，也是非常困难的。根据不同类别数据的不同保密需求，IPSec 策略中有多种等级的安全强度可供选择，使用 IPSec 可以显著地减少或防范前面谈到的几种网络攻击。

（1）窃听。Sniffer 可以读取数据包中的任何信息，因此对抗窃听最有效的方法就是对数据进行加密。IPSec 的封装安全载荷 ESP 协议通过对 IP 包进行加密来保证数据的私密性 。

（2）数据篡改。IPSec 用密钥为每个 IP 包生成一个检查和，该密钥为且仅为数据的发送方和接收方共享。对数据包的任何篡改都会改变检查和，从而让接收方得知包在传输过程中遭到了修改。

（3）身份欺骗，盗用口令，应用层攻击。IPSec 的身份交换和认证机制不会暴露任何信息，不给攻击者可乘之机，双向认证在通信系统之间建立信任关系，只有可信赖的系统才能彼此通信。

（4）中间人攻击。IPSec 结合双向认证和共享密钥，足以抵御中间人攻击。

（5）拒绝服务攻击。IPSec 使用 IP 包过滤法，依据 IP 地址范围、协议甚至特定的协议端口号来决定哪些数据流需要受到保护，哪些数据流可以被允许通过，哪些需要拦截。

3. 第三层保护的优点

通常，IPSec 提供的保护需要对系统作一定修改，但是 IPSec 在 IP 传输层，即第三层的“策略执行”（Strategic Implementation），几乎不需要什么额外开销就可以实现为绝大多数应用系统、服务和上层协议提供较高级别的保护；为现有的应用系统和操作系统配置，IPSec 几乎无须作任何修改，安全策略可以在 Active Directory 里集中定义，也可以在某台主机上进行本地化管理。

IPSec 策略在 ISO 参考模型第三层即网络层上实施的安全保护，范围几乎涵盖了 TCP/IP 协议族中所有 IP 协议和上层协议，如 TCP、UDP、ICMP、Raw(第 255 号协议)，甚至包括在网络层发送数据的客户自定义协议。在第三层上提供数据安全保护的主要优点就在于所有使用 IP 协议进行数据传输的应用系统和服务都可以使用 IPSec，而不必对这些应用系统和服务本身作任何修改。

运作于第三层以上的其他一些安全机制，如安全套接层 SSL，仅对知道如何使用 SSL 的应用系统(如 Web 浏览器)提供保护，这极大地限制了 SSL 的应用范围；而运作于第三层以下的安全机制，如链路层加密，通常只保护了特定链路间的数据传输，而无法做到在数据路径所经过的所有链路间提供安全保护，这使得链接层加密无法适用于 Internet 或路由 Intranet 方案中的端对端数据保护。

3.2 IPSec 体系结构

3.2.1 IPSec 体系结构

IPSec (Internet 协议安全)是一个工业标准网络安全协议，为 IP 网络通信提供透明的安全服务，保护 TCP/IP 通信免遭窃听和篡改，可以有效抵御网络攻击，同时保持易用性。IPSec 有两个基本目标：

① 保护 IP 数据包安全；

② 为抵御网络攻击提供防护措施。

IPSec 基于一种端到端的安全模式。这种模式有一个基本前提假设，就是假定数据通信的传输媒介是不安全的，因此通信数据必须经过加密。而掌握加解密方法的只有数据流的发送端和接收端，两者各自负责相应的数据加解密处理，而网络中其他只负责转发数据的路由器或主机无须支持 IPSec。该特性有助于企业用户在下列方案中成功地配置 IPSec。

(1) 局域网：C/S 模式，对等模式。

(2) 广域网：路由器到路由器模式，网关到网关模式。

(3) 远程访问：拨号客户机，专网对 Internet 的访问。

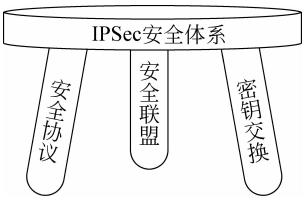

图 3-1 IPSec 组成结构

IPSec 结合安全联盟、安全协议组和动态密钥管理三者来实现上述两个目标，如图 3-1 所示，不仅能为企业局域网与拨号用户、域、网站、远程站点以及 Extranet 之间的通信提供强有力且灵活的保护，而且还能用来筛选特定数据流。

IPSec(IP Security)协议是 IETF 安全工作组制定的一套可以用于 IPv4 和 IPv6 上的、具有互操作性的、基于密码学的安全协议。IPv4 可选支持 IPSec，IPv6 必须支持 IPSec。IPSec 提供的安全服务包括访问控制、无连接的完整性、数据源头的认证、防重放功能、数据保密和一定的数据流保密等。IPSec 协议产生的初衷是解决 Internet 上 IP 传输的安全性问题，它包括从 RFC 2401 到 RFC 2412 的一系列 RFC，定义了一套默认的、

强制实施的算法，以保证不同的实施方案可以互通。IPSec 标准包含了 IP 安全体系结构、IP 认证 AH 头、IP 封装安全载荷 ESP 和 Internet 密钥交换（IKE）4 个核心的基本规范，组成了一个完整的安全体系结构，如图 3-2 所示。

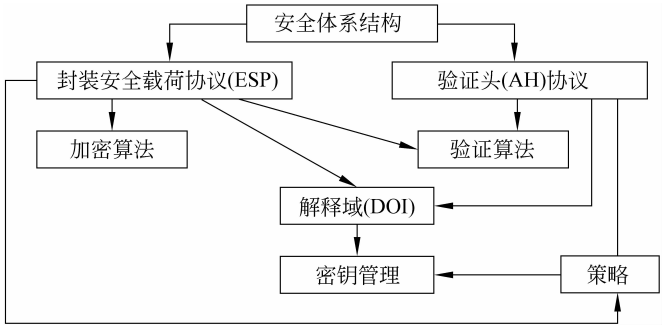

图 3-2　IPSec 安全体系结构

（1）安全体系结构。包含一般的概念、安全需求和定义 IPSec 的技术机制。

（2）ESP 协议。加密 IP 数据包的默认值、头部格式以及与加密封装相关的其他条款。

（3）AH 协议。验证 IP 数据包的默认值、头部格式以及与认证相关的其他条款。

（4）加密算法。描述各种加密算法如何用于 ESP 中。

（5）验证算法。描述各种身份验证算法如何用于 AH 和 ESP 身份验证选项。

（6）密钥管理。描述因特网 IETF 标准密钥管理方案。其中 IKE 是默认的密钥自动交换协议。

（7）解释域 DOI。是因特网统一协议参数分配权威机构（Internet Assigned Number Authority，IANA）中数字分配机制的一部分，它描述的值是预知的。包括彼此相关各部分的标志符及运作参数。

（8）策略。决定两个实体之间能否通信，以及如何进行通信。策略的核心由三部分组成：SA、SAD、SPD。SA（安全关联）表示了策略实施的具体细节，包括源/目的地址、应用协议、SPI（安全策略索引）等；SAD 为进入和外出包处理维持一个活动的 SA 列表；SPD 决定了整个 VPN 的安全需求。策略部分是唯一尚未成为标准的部件。

3.2.2　IPSec 驱动程序

1. IPSec 驱动程序

IPSec 驱动程序负责监视、筛选和 IP 通信。它负责监视所有出入站的 IP 数据包，并将每个 IP 数据包与作为 IP 策略一部分的 IP 筛选器相匹配。一旦匹配成功，IPSec 驱动程序通知 IKE 开始协商，图 3-3 为 IPSec 驱动程序服务示意图。

协商成功完成后，发送端 IPSec 驱动程序执行以下步骤。

（1）从 IKE 处获得 SA 和会话密钥。

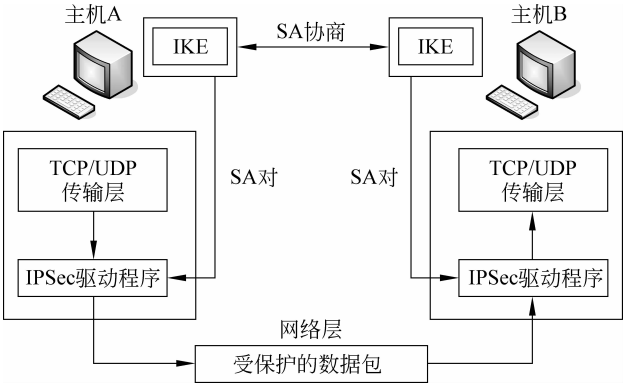

图 3-3　IPSec 驱动程序服务示意图

(2) 在 IPSec 驱动程序数据库中查找相匹配的出站 SA,并将 SA 中的 SPI 插入 IPSec 包头。

(3) 对数据包签名(完整性检查);如果要求机密,则另外加密数据包。

(4) 将数据包随同 SPI 发送 IP 层,然后进一步转发至目的主机。

接收端 IPSec 驱动程序执行以下步骤。

(1) 从 IKE 处获得会话密钥,SA 和 SPI。

(2) 通过目的地址和 SPI,在 IPSec 驱动程序数据库中查找相匹配的入站 SA。

(3) 检查签名,对数据包进行解密(如果是加密包的话)。

(4) 将数据包递交给 TCP/IP 驱动程序,然后再交给接收应用程序。

2. IPSec 工作流程

IPSec 的流程如下所述,为简单起见,本书假设这是一个 Intranet 例子,每台主机都有处于激活状态的 IPSec 策略。

(1) 用户甲(在主机 A 上)向用户乙(在主机 B 上)发送一消息。

(2) 主机 A 上的 IPSec 驱动程序检查 IP 筛选器,查看数据包是否需要以及需要受到何种保护。

(3) 驱动程序通知 IKE 开始协商。

(4) 主机 B 上的 IKE 收到请求协商通知。

(5) 两台主机建立第一阶段 SA,各自生成共享"主密钥"。若两机在此前通信中已经建立起第一阶段 SA,则可直接进行第二阶段 SA 协商。

(6) 协商建立第二阶段 SA 对:入站 SA 和出站 SA。SA 包括密钥和 SPI。

(7) 主机 A 上的 IPSec 驱动程序使用出站 SA,对数据包进行签名(完整性检查)与加密。

(8) 驱动程序将数据包递交 IP 层,再由 IP 层将数据包转发至主机 B。

(9) 主机 B 网络适配器驱动程序收到数据包并提交给 IPSec 驱动程序。

(10) 主机 B 上的 IPSec 驱动程序使用入站 SA,检查签名完整性并对数据包进行

解密。

(11) 驱动程序将解密后的数据包提交上层 TCP/IP 驱动程序,再由 TCP/IP 驱动程序将数据包提交主机 B 的接收应用程序。

以上是 IPSec 的一个完整工作流程,虽然看起来很复杂,但所有操作对用户是完全透明的。中介路由器或转发器仅负责数据包的转发,如果中途遇到防火墙、路由器或代理服务器,则要求它们具有 IP 转发功能,以确保 IPSec 和 IKE 数据流不会遭拒绝。

这里需要指出的是,使用 IPSec 的数据包不能通过网络地址译码 NAT。因为 IKE 协商中所携带的 IP 地址是不能被 NAT 改变的,对地址的任何修改都会导致完整性检查失效。

3.2.3 IPSec 采用的安全技术

1. IPSec 的安全特性

IPSec 有两个基本安全目标,决定它应该拥有以下 5 个安全特性。

(1) 不可否认性。"不可否认性"可以证实消息发送方是唯一可能的发送者,发送者不能否认发送过消息。"不可否认性"是采用公钥技术的一个特征,当使用公钥技术时,发送方用私钥产生一个数字签名,随消息一起发送,接收方用发送者的公钥来验证数字签名。在理论上,只有发送者才唯一拥有私钥;"不可否认性"不是基于认证的共享密钥技术的特征,因为在基于认证的共享密钥技术中,发送方和接收方掌握相同的密钥。

(2) 反重播性。"反重播"确保每个 IP 包的唯一性,保证信息万一被截取复制后,不能再被重新利用、重新传输回目的地址。该特性可以防止攻击者截取破译信息,再用相同的信息包冒取非法访问权(即使这种冒取行为发生在数月之后)。

(3) 数据完整性。防止传输过程中数据被篡改,确保发出数据和接收数据的一致性。IPSec 利用 Hash 函数,为每个数据包产生一个加密检查和,接收方在打开包前,先计算检查和,若包遭篡改导致检查和不相符,数据包即被丢弃。

(4) 数据可靠性(加密)。传输前对数据进行加密,可以保证即使传输过程中数据包遭截取,信息也无法被读。该特性在 IPSec 中为可选项,与 IPSec 策略的具体设置相关。

(5) 认证。数据源发送信任状,由接收方验证信任状的合法性,只有通过认证的系统才可以建立通信连接。

2. 基于电子证书的公钥认证

一个架构良好的公钥体系,在信任状的传递中不造成任何信息外泄,能解决很多安全问题。IPSec 与特定的公钥体系相结合,可以提供基于电子证书的认证。公钥证书认证在 Windows 2000 中,适用于对非 Windows 2000 主机、独立主机、非信任域成员的客户机或者不运行 Kerberos v5 认证协议的主机进行身份认证。

3. 预置共享密钥认证

IPSec 也可以使用预置共享密钥进行认证。预共享意味着通信双方必须在 IPSec 策

略设置中就共享的密钥达成一致。之后，在安全协商过程中，信息在传输前使用共享密钥加密，接收端使用同样的密钥解密。如果接收方能够解密，即被认为可以通过认证。但在Windows 2000 IPSec策略中，这种认证方式被认为不够安全，而一般不推荐使用。

4. 公钥加密

IPSec的公钥加密用于身份认证和密钥交换。使用公钥加密法，每个用户拥有一个密钥对，其中私钥仅为个人所知，公钥则可分发给任意需要与之进行加密通信的人。例如：A想要发送加密信息给B，则A需要用B的公钥加密信息，之后只有B才能用他的私钥解密该加密信息。虽然密钥对中两把钥匙彼此相关，但要想从其中一把推导出另一把，以目前计算机的运算能力来看，这种做法非常困难。因此，在这种加密法中，公钥可以广为分发，而私钥则需要仔细地妥善保管。

5. Hash函数保证数据完整性

Hash信息验证码(Hash Message Authentication Codes，HMAC)验证接收消息和发送消息的完全一致性(完整性)。这在数据交换中非常关键，尤其当传输媒介，如公共网络中不提供安全保证时更显重要。

HMAC结合Hash算法和共享密钥提供完整性。Hash散列通常也被当成是数字签名，但这种说法不够准确，两者的区别在于：Hash散列使用共享密钥，而数字签名基于公钥技术。Hash算法也称为消息摘要或单向转换。称它为单向转换的原因如下。

(1) 双方必须在通信的两端各自执行Hash函数计算。

(2) 使用Hash函数很容易从消息计算出消息摘要，但以目前计算机的运算能力，其逆向反演过程几乎不可实现。

Hash散列本身就是所谓加密检查和或消息完整性编码(Message Integrity Code，MIC)，通信双方必须各自执行函数计算来验证消息。举例来说，发送方首先使用HMAC算法和共享密钥计算消息检查和，然后将计算结果A封装进数据包中一起发送；接收方再对所接收的消息执行HMAC计算得出结果B，并将B与A进行比较。如果消息在传输中遭篡改，致使B与A不一致，接收方丢弃该数据包。

有两种最常用的Hash函数，内容如下。

(1) HMAC-MD5。MD5(消息摘要5)基于RFC 1321。MD5对MD4做了改进，计算速度比MD4稍慢，但安全性能得到了进一步改善。MD5在计算中使用了64个32位常数，最终生成一个128位的完整性检查和。

(2) HMAC-SHA。安全Hash算法定义在NIST FIPS 180-1，其算法以MD5为原型。SHA在计算中使用了79个32位常数，最终产生一个160位完整性检查和。SHA检查和长度比MD5更长，因此安全性也更高。

6. 加密保证数据可靠性

IPSec使用的数据加密算法是DES-Data Encryption Standard(数据加密标准)。DES密钥长度为56位，在形式上是一个64位数。DES以64位(8字节)为分组对数据加

密，每 64 位明文，经过 16 轮置换生成 64 位密文，其中每字节有 1 位用于奇偶校验，所以实际有效密钥长度是 56 位。IPSec 还支持 3DES 算法，3DES 可提供更高的安全性，但计算速度更慢。

7. 密钥管理

(1) 动态密钥更新。IPSec 策略使用“动态密钥更新”法决定一次通信中新密钥产生的频率。在通信过程中，动态密钥指数据流被划分成一个个“数据块”，每一个“数据块”都使用不同的密钥加密，这可以保证万一攻击者中途截取了部分通信数据流和相应的密钥后，也不会危及到其余通信信息的安全。动态密钥更新服务由 Internet 密钥交换(Internet Key Exchange，IKE)提供，详见 IKE 介绍部分。

IPSec 策略允许专家级用户自定义密钥生命周期。如果该值没有设置，则按默认时间间隔自动生成新密钥。

(2) 密钥长度。密钥长度每增加一位，可能的密钥数就会增加一倍，相应地，破解密钥的难度也会随之呈指数级加大。IPSec 策略提供多种加密算法，可生成多种长度不等的密钥，用户可根据不同的安全需求加以选择。

(3) Diffie-Hellman 算法。要启动安全通信，通信两端必须首先得到相同的共享密钥(主密钥)，但共享密钥不能通过网络相互发送，因为这种做法极易泄密。

Diffie-Hellman 算法是用于密钥交换的最早最安全的算法之一。DH 算法的基本工作原理如下：通信双方公开或半公开交换一些准备用来生成密钥的“素材数据”，彼此交换过密钥生成“素材”后，两端可以各自生成出完全一样的共享密钥。在任何时候，双方都绝不交换真正的密钥。

通信双方交换的密钥生成“素材”，长度不等，“素材”长度越长，所生成的密钥强度也就越高，密钥破译就越困难。除进行密钥交换外，IPSec 还使用 DH 算法生成所有其他加密密钥。

3.3 IPSec 安全协议

IPSec 在 IP 层提供安全服务，它使系统能按需选择安全协议，决定服务所使用的算法及放置需求服务所需密钥到相应位置。IPSec 用来保护一条或多条主机与主机间、安全网关与安全网关间、安全网关与主机间的路径。

IPSec 能提供的安全服务集包括访问控制、无连接的完整性、数据源认证、拒绝重发包(部分序列完整性形式)、保密性和有限传输流保密性。因为这些服务均在 IP 层提供，所以任何高层协议均能使用它们，例如 TCP、UDP、ICMP、BGP 等。

这些目标是通过使用两大传输安全协议，头部认证(AH)和封装安全负载(ESP)以及密钥管理程序和协议的使用来完成的。所需的 IPSec 协议集内容及其使用方式是由用户、应用程序和/或站点、组织对安全和系统的需求来决定。

IPSec 结构包括众多协议和算法，这些协议之间的相互关系如图 3-2 所示。由图可知，IPSec 协议不是一个单独的协议，它给出了应用于 IP 层上网络数据安全的一整套体

系结构，包括网络认证协议 Authentication Header（AH）、封装安全载荷协议（Encapsulating Security Payload，ESP）、密钥管理协议（Internet Key Exchange，IKE）和用于网络认证及加密的一些算法等。IPSec 规定了如何在对等层之间选择安全协议、确定安全算法和密钥交换，向上提供访问控制、数据源认证、数据加密等网络安全服务。

IPSec 提供了两种机制：认证和加密。认证机制使 IP 通信的数据接收方能够确认数据发送方的真实身份，以及数据在传输过程中是否遭篡改。加密机制通过对数据进行编码来保证数据的机密性，以防数据在传输过程中被窃听。其中，AH 协议定义了认证的应用方法，提供数据源认证和完整性保证；ESP 协议定义了加密和可选认证的应用方法，提供可靠性保证。在实际进行 IP 通信时，可以根据实际需求同时使用这两种协议或选择使用其中的一种。AH 和 ESP 都可以提供认证服务，不过，AH 提供的认证服务要强于 ESP。

3.3.1 Authentication Header 协议

1. Authentication Header 协议结构

Authentication Header（AH）协议主要提供认证机制，保证数据包接收者得到的源地址是可靠的，同时也提供了数据的完整性，抗重播攻击的能力。它使通信免受篡改，但不能防止窃听，适合用于传输非机密数据。

AH 的工作原理是在每一个数据包上添加一个身份验证包头。此包头包含一个带密钥的 Hash 散列（可以将其当做数字签名，只是它不使用证书），此 Hash 散列在整个数据包中计算，因此对数据的任何更改将致使散列无效，提供对数据的完整性保护。

AH 包头位置在 IP 包头和传输层协议包头之间，如图 3-4 所示。AH 由 IP 协议号“51”标识，该值包含在 AH 包头之前的协议包头中，如 IP 包头。AH 可以单独使用，也可以与 ESP 协议结合使用。

图 3-4　AH 为整个数据包提供完整性检查

AH 由 5 个固定长度域和一个变长的认证数据域组成，如图 3-5 所示。

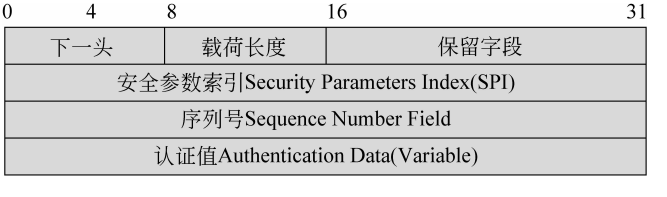

图 3-5　AH 包头格式

其中的字段意义如下。

（1）下一头：（8 位），识别这个包头之后紧跟的包头类型。在传输模式下，表示处于保护中的上层协议的值，比如 TCP 或 UDP 的值。