第 5 章 Internet 安全

随着 Internet 的不断普及，TCP/IP 体系结构成为当前计算机网络的基础，TCP/IP 网络已基本成为现代计算机网络的代名词。但是，由于 TCP/IP 体系结构在设计之初的局限性，Internet 存在的安全问题日益突出，各种安全隐患日渐严重。因此，人们设计了不同的安全机制来应对 Internet 面临的安全挑战。

事实上，可以在 TCP/IP 体系结构上的任何层次实现安全机制，各层机制有不同的特点，提供不同的安全性。本章首先介绍 3 种典型的在 TCP/IP 不同层次提供的安全机制：IPSec、SSL/TLS 和 PGP，然后介绍常见的 Internet 欺骗及防范手段。

5.1 IP 安 全

在 TCP/IP 协议分层模型中，IP 层是可能实现端到端安全通信的最底层。通过在 IP 层上实现安全性，不仅可以保护各种带安全机制的应用程序，而且可以保护许多无安全机制的应用。典型地，IP 协议实现在操作系统中，因此，在 IP 层实现安全功能，可以不必修改应用程序。

互联网工程任务组(IETF)于 1998 年颁布了一套开放标准网络安全协议：IP 层安全标准 IPSec(IP Security)，其目标是为 IPv4 和 IPv6 提供具有较强的互操作能力、高质量和基于加密的安全。IPSec 将密码技术应用在网络层，提供端对端通信数据的私有性、完整性、真实性和防重放攻击等安全服务。IPSec 对于 IPv4 是可选的，对于 IPv6 是强制性的。

IPSec 能支持各种应用的原理在于它可以在 IP 层实现加密/认证功能，这样就可以在不修改应用程序的前提下保护所有的分布式应用，包括远程登录、电子邮件、文件传输和 Web 访问等。

IPSec 通过多种手段提供了 IP 层安全服务：允许用户选择所需安全协议，允许用户选择加密和认证算法，允许用户选择所需的密码算法的密钥。IPSec 可以安装在路由器或主机上，若 IPSec 安装在路由器上，则可在不安全的 Internet 上提供一个安全的通道；若安装在主机上，则能提供主机端对端的安全性。

5.1.1 IPSec 体系结构

IPSec 规范相当复杂，因为它不是一个单独的协议。IPSec 规范给出了应用于 IP 层的网络数据安全的一整套体系结构，包括认证头协议、封装安全载荷协议、Internet 密钥

交换协议和用于网络认证和加密的一些算法等。IPSec的主要构成组件如图5-1所示。

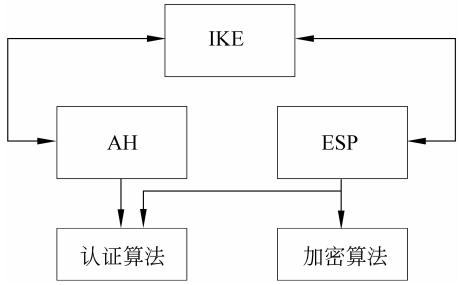


图5-1 IPSec组件

IPSec的安全功能主要通过IP认证头(Authentication Header,AH)协议以及封装安全载荷(Encapsulating Security Payload,ESP)协议实现。AH提供数据的完整性、真实性和防重放攻击等安全服务,但不包括机密性。而ESP除了实现AH的功能外,还可以实现数据的机密性。AH和ESP可以分开使用或一起使用。完整的IPSec还应包括AH和ESP中所使用密钥的交换和管理,也就是Internet密钥交换(Internet Key Exchange,IKE)协议,IKE用于动态地认证IPSec参与各方的身份。

IPSec规范中要求强制实现的加密算法是CBC模式的DES和NULL算法,而认证算法是HMAC-MD5,HMAC-SHA-1和NULL认证算法。NULL加密和认证分别是不加密和不认证。

在IP的认证和保密机制中出现的一个核心概念是安全关联(SA)。一个安全关联是发送方和接收方之间受到密码技术保护的单向关系,该关联对所携带的通信流量提供安全服务:要么对通信实体收到的IP数据包进行"进入"保护,要么对实体外发的数据包进行"流出"保护。如果需要双向安全交换,则需要建立两个安全关联,一个用于发送数据,另一个用于接收数据。安全服务可以由AH或ESP提供,但不能两者都提供。

一个安全关联由3个参数确定:

- 安全参数索引(SPI)。一个与SA相关的位串,仅在本地有意义。这个参数被分配给每一个SA,并且每一个SA都通过SPI进行标识。发送方把这个参数放置在每一个流出数据包的SPI域中,SPI由AH和ESP携带,使得接收系统能选择合适的SA处理接收包。SPI并非全局指定,因此SPI要与目标IP地址、安全协议标识一起来唯一地标识一个SA。
- 目标IP地址。目前IPSec SA管理机制中仅仅允许单播地址。所以这个地址表示SA的目的端点地址,可以是用户终端系统、防火墙或路由器。它决定了关联方向。
- 安全协议标识。标识该关联是一个AH安全关联或ESP安全关联。

处理与SA有关的流量时有两个数据库,即安全关联数据库(Security Association Database,SAD)和安全策略数据库(Security Policy Database,SPD)。SAD包含了与每一个安全关联相联系的参数,SPD则指定了主机或网关的所有IP流量的流入和流出分配策略。

5.1.2 IPSec 工作模式

IPSec 的安全功能主要通过 IP 认证头(AH)协议以及封装安全载荷(ESP)协议实现。AH 和 ESP 均支持两种模式：传输模式和隧道模式，如图 5-2 所示。

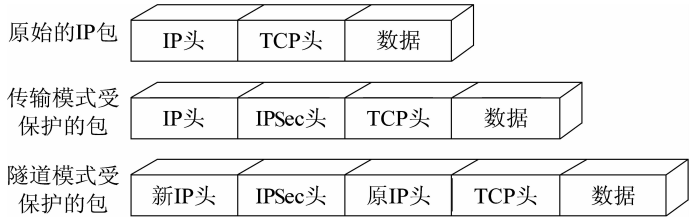


图 5-2 IPSec 工作模式

1. 传输模式

传输模式主要为直接运行在 IP 层之上的协议(如 TCP、UDP 和 ICMP)提供安全保护，一般用于在两台主机之间的端到端通信。传输模式是指在数据包的 IP 头和载荷之间插入 IPSec 信息。当一个主机在 IPv4 上运行 AH 或 ESP 时，其载荷是跟在 IP 报头后面的数据；对 IPv6 而言，其载荷是跟在 IP 报头后面的数据和 IPv6 的任何扩展头。传输模式使用原始明文 IP 头。

传输模式的 ESP 可以加密和认证 IP 载荷，但不包括 IP 头。传输模式的 AH 可以认证 IP 载荷和 IP 报头的选中部分。

2. 隧道模式

隧道模式对整个 IP 包提供保护。为了达到这个目的，当 IP 数据包附加了 AH 或 ESP 域之后，整个数据包加安全域被当作一个新 IP 包的载荷，并拥有一个新的外部 IP 包头。原来(内部)的整个 IP 包利用隧道在网络之间传输，沿途路由器不能检查内部 IP 包头。由于原来的包被封装，新的、更大的包可以拥有完全不同的源地址与目的地址，以增强安全性。当 SA 的一端或两端为安全网关时使用隧道模式，如使用 IPSec 的防火墙或路由器。防火墙内的主机在没有 IPSec 时也可以实现安全通信：当主机生成的未保护包通过本地网络边缘的防火墙或安全路由器时，IPSec 提供隧道模式的安全性。

IPSec 操作隧道模式的例子如下。网络中的主机 A 生成以另一个网络中的主机 B 作为目的地址的 IP 包，该 IP 包从源主机 A 被发送到 A 网络边界的防火墙或安全路由器。防火墙过滤所有的外发包。根据对 IPSec 处理的请求，如果从 A 到 B 的包需要 IPSec 处理，则防火墙执行 IPSec 处理，给该 IP 包添加外层 IP 包头，外层 IP 包头的源 IP 地址为此防火墙的 IP 地址，目的地址可能为 B 本地网络边界的防火墙的地址。这样，包被传送到 B 的防火墙，而其间经过的中间路由器仅检查外部 IP 头；在 B 的防火墙处，除去外部 IP 头，内部的包被送往主机 B。

ESP 在隧道模式中加密和认证(可选)整个内部 IP 包，包括内部 IP 报头。AH 在隧道模式中认证整个内部 IP 包和外部 IP 头中的选中部分。

当 IPSec 被用于端到端的应用时，传输模式更合理一些。在防火墙到防火墙或者主

机到防火墙这类数据仅在两个终端节点之间的部分链路上受保护的应用中，通常采用隧道模式。而且，传输模式并不是必需的，因为隧道模式可以完全替代传输模式。但是隧道模式下的IP数据包有两个IP头，处理开销相对较大。

5.1.3 AH协议

IP认证头(AH)协议为IP数据包提供数据完整性校验和身份认证，还有可选择的抗重放攻击保护，但不提供数据加密服务。数据完整性确保包在传输过程中内容不可更改；认证确保终端系统或网络设备能对用户或应用程序进行认证，并相应地提供流量过滤功能，同时还能防止地址欺诈攻击和重放攻击。认证基于消息鉴别码(MAC)，双方必须共享同一个密钥。

由于AH不提供机密性保证，所以它也不需要加密算法。AH可用来保护一个上层协议(传输模式)或一个完整的IP数据报(隧道模式)。它可以单独使用，也可以和ESP联合使用。

认证头由如下几个域组成，如图5-3所示。

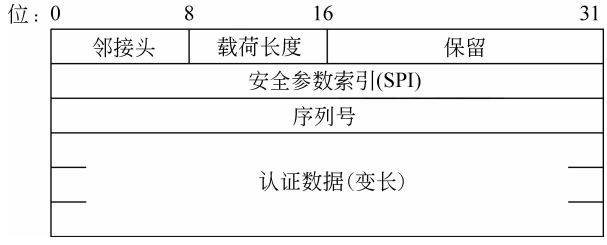


图5-3 IPSec认证头

- 邻接头(8位)。标识AH字段后面下一个负载的类型。
- 有效载荷长度(8位)。字长为32位的认证头长度减2。例如，认证数据域的默认长度是96位或3个32位字，另加3个字长的固定头，总共6个字，则载荷长度域的值为4。
- 保留(7位)。保留给未来使用。当前，这个字段的值设置为0。
- 安全参数索引(32位)。这个字段与目的IP地址和安全协议标识一起，共同标识当前数据包的安全关联。
- 序列号(32位)。单调递增的计数值，提供了反重放的功能。在建立SA时，发送方和接收方的序列号初始化为0，使用此SA发送的第一个数据包序列号为1，此后发送方逐渐增大该SA的序列号，并把新值插入到序列号字段。
- 认证数据(变量)。变长域，包含了数据包的完整性校验值(Integrity Check Value，ICV)或包的MAC。这个字段的长度必须是32位字的整数倍，可以包含填充。

1. AH传输模式

AH的传输模式只保护IP数据包的不变部分，它保护的是端到端的通信，通信的终点必须是IPSec终点，如图5-4所示。

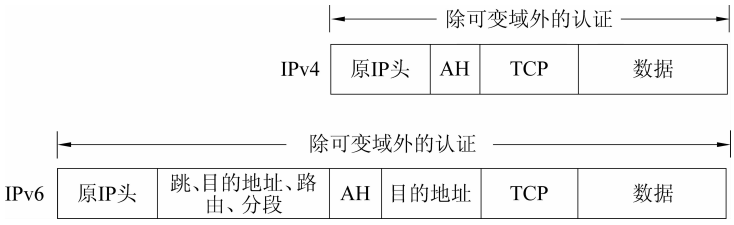


图 5-4 AH 的传输模式

在 IPv4 的传输模式 AH 中，AH 插入到原始 IP 头之后，IP 载荷（如 TCP 分段）之前。认证包括了除 IPv4 报头中可变的、被 MAC 计算置为 0 的域以外的整个包。

在 IPv6 中，AH 被作为端到端载荷，即不被中间路由器检查或处理。因此，AH 出现在 IP 头以及跳、路由和分段扩展头之后。目的地址作为可选报头在 AH 前面或后面，由特定语义决定。同样，认证包括了除 IPv6 报头中可变的、被 MAC 计算置为 0 的域以外的整个包。

2. AH 隧道模式

AH 用于隧道模式时，整个原始 IP 包被认证，AH 被插入到原始 IP 头和新 IP 头之间。原 IP 头中包含了通信的原始地址，而新 IP 头则包含了 IPSec 端点的地址，如图 5-5 所示。

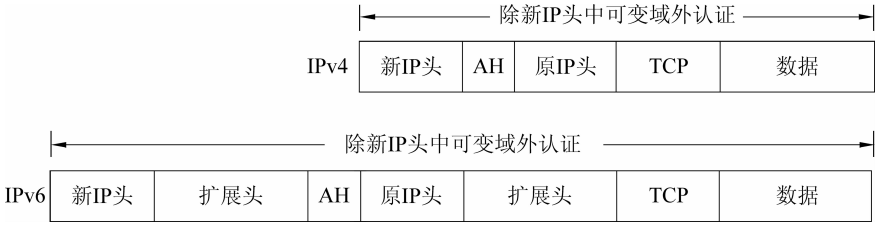


图 5-5 AH 隧道模式

使用隧道模式，整个内部 IP 包，包括整个内部 IP 头均被 AH 保护。外部 IP 头（IPv6 中的外部 IP 扩展头）除了可变且不可预测的域之外均被保护。隧道模式可用来替换端到端安全服务的传输模式。但由于这一协议中没有提供机密性，因此，相当于没有隧道封装这一保护措施，所以它没有什么用处。

5.1.4 ESP 协议

封装安全载荷（ESP）协议为 IP 数据包提供数据完整性校验、身份认证和数据加密，还有可选择的抗重放攻击保护。即除了 AH 提供的所有服务外，ESP 还提供数据保密服务，包括报文内容保密和流量限制保密。ESP 用一个密码算法提供机密性，数据完整性则由身份验证算法提供。ESP 通过插入一个唯一的、单向递增的序列号提供抗重放服务。保密服务可以独立于其他服务而单独选择，数据完整性校验和身份认证用作保密服务的联合服务。只有选择了身份认证时，才可以选择抗重放服务。

ESP 可以单独使用，也可以和 AH 联合使用，还可以通过隧道模式使用。ESP 可以

提供主机到主机、防火墙到防火墙、主机到防火墙之间的安全服务。

图5-6是ESP包的格式，它包含如下各域：

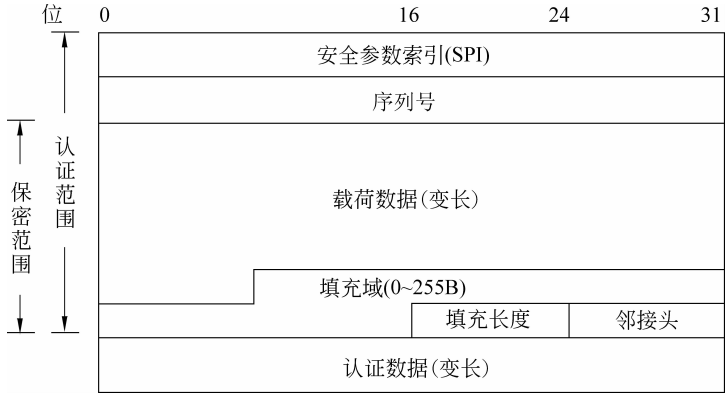


图5-6 ESP格式

- 安全参数索引SPI(32位)。标识安全关联。ESP中的SPI是强制字段，总要提供。
- 序列号(32位)。单调递增计数值，提供反重放功能。这是强制字段，并且总要提供，即使接收方没有选择对特定SA的反重放服务。如果开放了反重放服务，则计数值不允许折返。
- 载荷数据(变长)。变长的字段，包括被加密保护的传输层分段(传输模式)或IP包(隧道模式)。该字段的长度是字节的整数倍。
- 填充域(0～255字节)。可选字段，但所有实现都必须支持该字段。该字段满足加密算法的需要(如果加密算法要求明文是字节的整数倍)，还可以提供通信流量的保密性。发送方可以填充0～255字节的填充值。
- 填充长度(8位)。紧跟填充域，指示填充数据的长度，有效值范围是0～255。
- 邻接头(8位)。标识载荷中第一个报头的数据类型(如IPv6中的扩展头或上层协议TCP等)。
- 认证数据(变长)。一个变长域(必须为32位字长的整数倍)，包含根据除认证数据域外的ESP包计算的完整性校验值。该字段长度由所选择的认证算法决定。

载荷数据、填充数据、填充长度和邻接头域在ESP中均被加密。如果加密载荷的算法需要初始向量IV这样的同步数据，则必须从载荷数据域头部取，IV通常作为密文的开头，但并不被加密。

对加密来说，发送方封装ESP字段，添加必要的填充并加密结果。发送方使用SA和IV(密码同步数据)指定的密钥、加密算法、算法模式来加密字段。如果加密算法要求IV，则这个数据被显式地携带在载荷字段中。加密在认证之前执行，并且不包含认证数据。这种方式有利于接收方在解密之前快速地检测数据包，拒绝重放和伪造的数据包。

接收方使用密钥、解密算法和IV来解密ESP载荷数据、填充、填充长度和邻接头。如果指明使用了显式IV，则这个数据从负载中取出，输入到解密算法中。如果使用隐式

IV，则接收方构造一个本地 IV 输入到解密算法中。

认证算法由 SA 指定。与 AH 相同，ESP 支持使用默认为 96 位的 MAC，且应支持 HMAC-MD5-96 和 HMAC-SHA-1-96。发送方针对去掉认证数据部分的 ESP 计算 ICV。SPI、序列号、载荷数据、填充数据、填充长度和邻接头都包含在 ICV 的计算中。

1. 传输模式 ESP

传输模式 ESP 用于加密和认证(可选)IP 携带的数据(如 TCP 分段)，如图 5-7 所示。

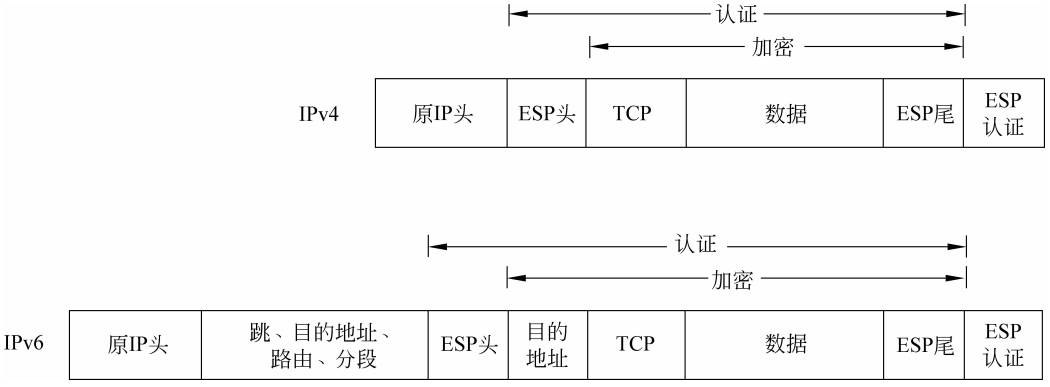


图 5-7 传输模式 ESP

在此模式下使用 IPv4，ESP 头位于传输头(TCP、UDP、ICMP)之前，ESP 尾(填充数据、填充长度和邻接头域)放入 IP 包尾部。如果选择了认证，则将 ESP 的认证数据域置于 ESP 尾之后。整个传输层分段和 ESP 尾一起加密。认证覆盖 ESP 头和所有密文。

在 IPv6 中，ESP 被视为端到端载荷，即不被中间路由器校验和处理。因此，ESP 头出现在 IPv6 基本头以及跳、路由和分段扩展头之后，目的可选扩展头可根据安全防护的需求出现在 ESP 头之前或之后。如果可选扩展头在 ESP 头之后，则加密包括整个传输段、ESP 尾和目的可选扩展头。认证覆盖了 ESP 头和所有密文。

传输模式 ESP 操作可归纳如下：

(1) 在源端，包括 ESP 尾和整个传输层分段的数据块被加密，块中的明文被密文替代，形成要传输的 IP 包，如果选择了认证，则加上认证。

(2) 将包送往目的地。中间路由器需要检查和处理 IP 头和任何附加的 IP 扩展头，但不需要检查密文。

(3) 目的节点对 IP 报头和任何附加的 IP 扩展头进行处理后，利用 ESP 头中的 SPI 解密包的剩余部分，恢复传输层分段数据。

传输模式操作为任何使用它的应用提供保护，而不需要在每个单独的应用中实现。同时，这种方式也是高效的，仅增加了少量的 IP 包长度。它的一个弱点是可能对传输包进行流量分析。

2. 隧道模式 ESP

隧道模式 ESP 用于加密整个 IP 包，如图 5-8 所示。

在此模式中，将 ESP 头作为包的前缀，并在包后附加 ESP 尾，然后对其进行加密。该模式用于对抗流量分析。

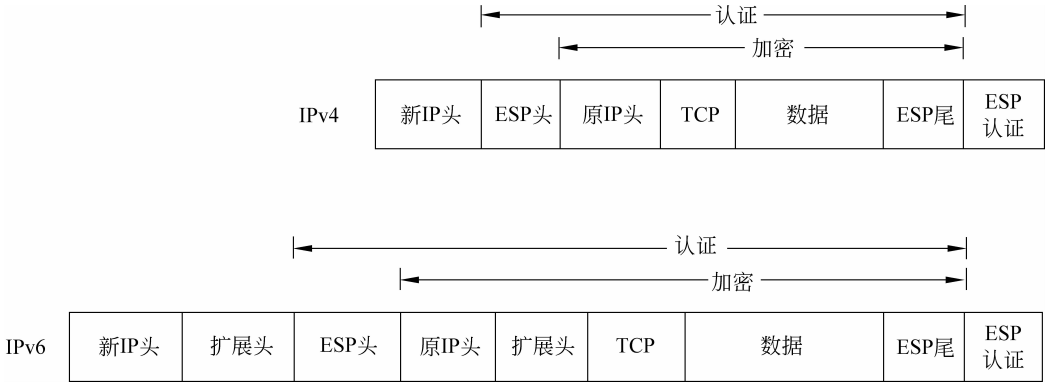


图 5-8 隧道模式 ESP

由于IP头中包含目的地址和可能的路由以及跳的信息，不可能简单地传输带有ESP头的被加密的IP包，因为这样中间路由器就不能处理该数据包。因此，必须用新的IP报头封装整个数据块(ESP头、密文和可能的认证数据)，其中拥有足够的路由信息，却没有为流量分析提供信息。

传输模式适用于保护支持ESP特性的主机之间的连接，而隧道模式则适用于防火墙或其他安全网关，保护内部网络，隔离外部网络。后者加密仅发生在外部网络和安全网关之间或两个安全网关之间，从而内部网络的主机不负责加密工作，通过减少所需密钥数目简化密钥分配任务。另外，它阻碍了基于最终目的地址的流量分析。

5.1.5 IKE

IPSec的密钥管理包括密钥的建立和分发。密钥建立是依赖于加密的数据保护的核心，密钥分发则是数据保护的基础。IPSec体系结构文档要求支持以下两种密钥管理类型：

- 手动。系统管理员手动地为每个系统配置自己的密钥和其他通信系统密钥。这种方式适用于小规模、相对静止的环境。
- 自动。在大型分布系统中使用可变配置为SA动态地按需创建密钥。

Internet密钥交换(IKE)用于动态建立SA和会话密钥。在建立安全会话之前，通信双方需要一种协议，用于自动地以受保护的方式进行双向认证，建立共享的会话密钥和生成IPSec的SA，这一协议叫做Internet密钥交换协议。IKE的目的是使用某种长期密钥(如共享的秘密密钥、签名公钥和加密公钥)进行双向认证并建立会话密钥，以保护后续通信。IKE代表IPSec对SA进行协商，并对安全关联数据库(SAD)进行填充。

IETF设计了IKE的整个规范，主要由3个文档定义：RFC 2407，RFC 2408和RFC 2409。RFC 2407定义了因特网IP安全解释域(IPSec DOI)，RFC 2408描述因特网安全关联和密钥管理协议ISAKMP，RFC 2409则描述了IKE如何利用Oakley、SKEME和ISAKMP进行安全关联的协商。

ISAKMP为认证和密钥交换提供了一个框架，用来实现多种密钥交换。ISAKMP自身不包含特定的交换密钥算法，而是定义了一系列使用各种密钥交换算法的报文格式，规

定了通信双方的身份认证，安全关联的建立和管理，密钥产生的方法，以及安全威胁（例如重放攻击）的预防。

Oakley 是一个基于 Diffie-Hellman 算法的密钥交换协议，描述了一系列称为“模式”的密钥交换，并且定义了每种模式提供的服务。Oakley 允许各方根据本身的速度来选择使用不同的模式。以 Oakley 为基础，IKE 借鉴了不同模式的思想，每种模式提供不同的服务，但都产生一个结果：通过验证的密钥交换。在 Oakley 中，并未定义模式进行一次安全密钥交换时需要交换的信息，而 IKE 对这些模式进行了规范，将其定义成正规的密钥交换方法。

SKEME 是另外一种密钥交换协议，定义了验证密钥交换的一种类型。其中，通信各方利用公钥加密实现相互间的验证；同时“共享”交换的组件。每一方都要用对方的公钥来加密一个随机数字，两个随机数（解密后）都会对最终的会话密钥产生影响。通信的一方可选择进行一次 Diffie-Hellman 交换，或者仅仅使用另一次快速交换对现有的密钥进行更新。IKE 在它的公共密钥加密验证中，直接借用了 SKEME 这种技术，同时也借用了快速密钥刷新的概念。

DOI（Domain Of Interpretation，解释域）是 ISAKMP 的一个概念，规定了 ISAKMP 的一种特定用法，其含义是，对于每个 DOI 值，都应该有一个与之相对应的规范，以定义与该 DOI 值有关的参数。IKE 实际上是一种常规用途的安全交换协议，适用于多方面的需求，如 SNMPv3、OSPFv3 等。IKE 采用的规范是在 DOI 中制定的，它定义了 IKE 具体如何协商 IPSec SA。如果其他协议要用到 IKE，每种协议都要定义各自的 DOI。

因此，由 RFC 2409 文档描述的 IKE 属于一种混合型协议。它创建在 ISAKMP 定义的框架上，沿用了 Oakley 的密钥交换模式以及 SKEME 的共享和密钥更新技术，还定义了它自己的两种密钥交换方式，从而定义出自己独一无二的验证加密材料生成技术以及协商共享策略。

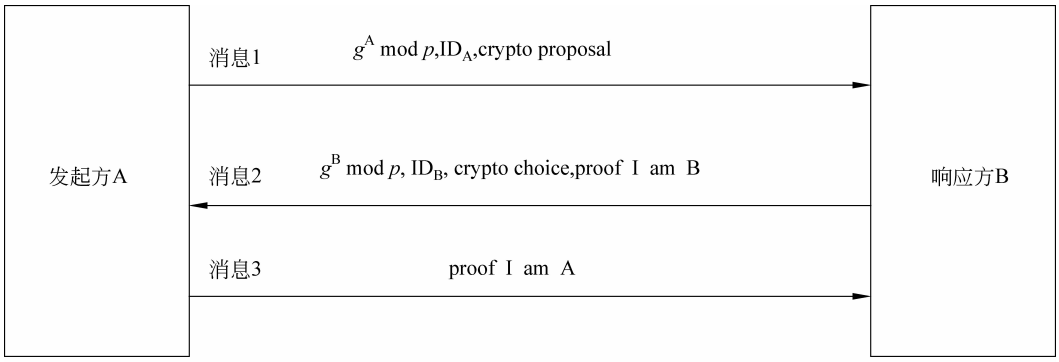
IKE 定义了两个阶段的 ISAKMP 交换。阶段 1 建立 IKE SA，对通信双方进行双向身份认证，并建立会话密钥；阶段 2 使用阶段 1 的会话密钥，建立一个或多个 ESP 或 AH 使用的 SA。IKE SA 定义了双方的通信形式，如使用哪种算法来加密 IKE 通信，怎样对远程通信方的身份进行验证等。随后，便可用 IKE SA 在通信双方之间建立任何数量的 IPSec SA。因此，在具体的 IPSec 实现中，IKE SA 保护 IPSec SA 的协商，IPSec SA 保护最终的网络中的数据流量。

1. IKE 阶段 1

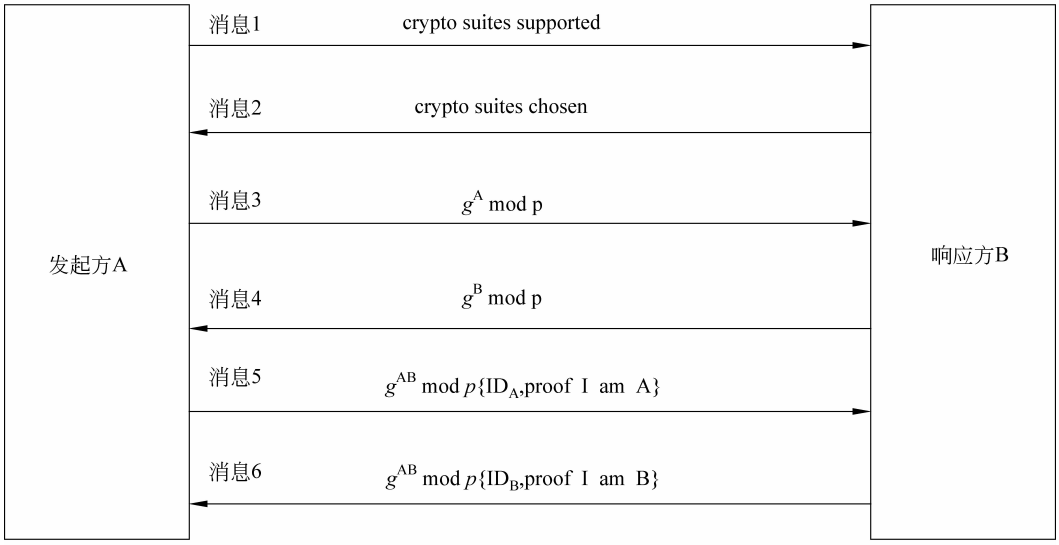
阶段 1 的交换有两种模式：积极模式和主模式，如图 5-9 所示。

积极模式（aggressive mode）使用 3 条消息完成，前两条消息是 Diffie-Hellman 交换，用于建立会话密钥；消息 2 和消息 3 完成了双向认证。在消息 1 中，发起方可以提议密码算法。但是因为发起方还要发送一个 Diffie-Hellman 数，所以必须指定一种唯一的 Diffie-Hellman 组，并期望响应方能够支持。如果不能支持，则响应方会拒绝本次链接请求，而且不会告诉发起方自己能够支持的算法。

主模式（main mode）则需要 6 条消息。在第一对消息中，发起方发送一个 cookie 并请求对方的密码算法，响应方回应自己的 cookie 和能够接受的密码算法。消息 3 和消息



(a) 积极模式



(b) 主模式

图 5-9 IKE 阶段 1 的模式

4 是一次 Diffie-Hellman 交换过程。消息 5 和消息 6 用消息 3 和消息 4 商定的 Diffie-Hellman 数值进行加密，完成双向身份认证的过程。主模式可以协商所有密码参数：加密算法、散列算法、认证方式和 Diffie-Hellman 组，由发起方提议，响应方选择。IKE 为每类密码参数规定了必须实现的算法，加密算法必须支持 DES，散列算法要实现 MD5，认证方式要支持预先共享密钥的方式，Diffie-Hellman 组则是特定的 g 和 p 的模指数。

积极模式的消息 2 和消息 3、主模式的消息 5 和消息 6 都包含一个身份证据，用于证明发送方知道与其身份相关的秘密，同时作为以前发送的消息的完整性保护。在 IKE 中，身份证据随着认证方式的不同而不同。IKE 阶段 1 可以接受的认证方法包括预先共享的秘密密钥、加密公钥、签名公钥等。通常，身份证据由某种密钥的散列值、Diffie-