第4章 网络模型中的安全体系结构

OSI参考模型和TCP/IP参考模型是研究网络通信时经常使用的。为了增强参考模型的安全性，ISO为其制定了很多安全标准，形成了网络模型的安全体系结构。本章将详细介绍网络模型中安全体系结构及各层所使用的安全协议及其作用。

重点难点

- ☑ 计算机网络安全体系综述
- ☑ 数据链路层的安全协议
- ☑ 网络层的安全协议
- ☑ 传输层的安全协议
- ☑ 应用层的安全协议

4.1 认识网络模型的安全体系

网络模型指的是网络参考模型，网络参考模型包括最常见的开放系统互联参考模型（Open System Interconnect，OSI），即OSI七层参考模型，TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/因特网互联协议）参考模型，即TCP/IP四层参考模型。OSI模型是在协议开发前设计的，具有通用性。TCP/IP是先有协议集然后建立模型，不适用于非TCP/IP网络，具有特殊性。OSI参考模型有七层结构，而TCP/IP有四层结构。网络安全模型就是在网络模型的基础上进行构建的。

知识拓展

TCP/IP五层原理参考模型

为了学习完整体系结构，一般采用一种折中的方法：综合OSI模型与TCP/IP参考模型的优点，采用一种原理参考模型，也就是TCP/IP五层原理参考模型。三种模型的关系如图4-1所示。

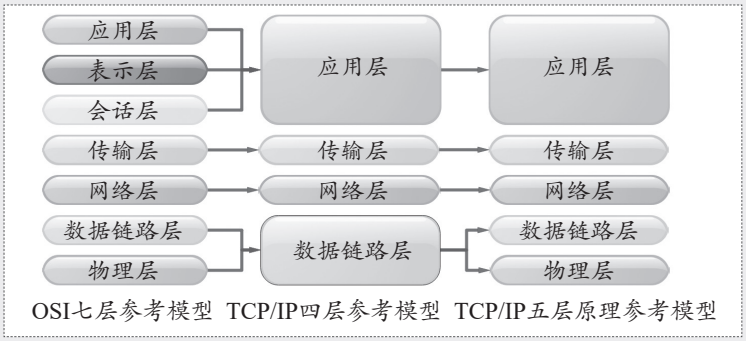

图 4-1

4.1.1 OSI安全体系结构

OSI七层参考模型主要是为了解决异型网络互连时所遇到的兼容性问题。它的最大优点是将服务、接口和协议这三个概念明确地区分开来，也使网络的不同功能模块分担起不同的职责。当网络发展到一定规模时，安全性问题就会变得突出。必须有一套体系结构来解决安全问题，于是OSI安全体系结构应运而生。

1. 安全体系结构的出现

为了增强OSI参考模型的安全性，ISO（International Organization for Standardization，国际标准化组织）在1988年提出了ISO 7489-2标准，提高了ISO 7498标准的安全等级。该标准提出了网络安全系统的体系结构，和以后相应的安全标准给出的网络信息安全架构被称为OSI安全体系结构。OSI安全体系结构指出了计算机网络需要的安全服务和解决方案，并明确了各类安全服务在OSI网络层次中的位置，这种在不同网络层次满足不同安全需求的技术路线对后来网络安全的发展起到了重要的作用。

2. 安全体系结构的作用

OSI安全体系结构的作用如下。

- 提供安全体系结构所配备的安全服务（也称安全功能）和有关安全机制在体系结构下的一般描述。
- 确定体系结构内部可以提供相关安全服务的位置。
- 保证完全准确地配置安全服务，并且一直维持于信息系统安全的生命周期中，安全服务必须满足一定的强度要求。
- 一种安全服务可以通过某种单独的安全机制提供，也可以通过多种安全机制联合提供，一种安全机制可用于提供一种或多种安全服务，在七层协议中除第五层（会话层）外，每一层均能提供相应的安全服务。

3. 安全体系结构的层次

OSI安全体系结构是一个普遍适用的安全体系结构，其核心内容是保证异构计算机系统进程与进程之间远距离交换信息的安全；其基本思想是为了全面而准确地满足一个开放系统的安全需求，必须在七个层次中提供必需的安全服务、安全机制和技术管理，以及它们在系统上的合理部署和关系配置。这个体系结构的示意如图4-2所示。

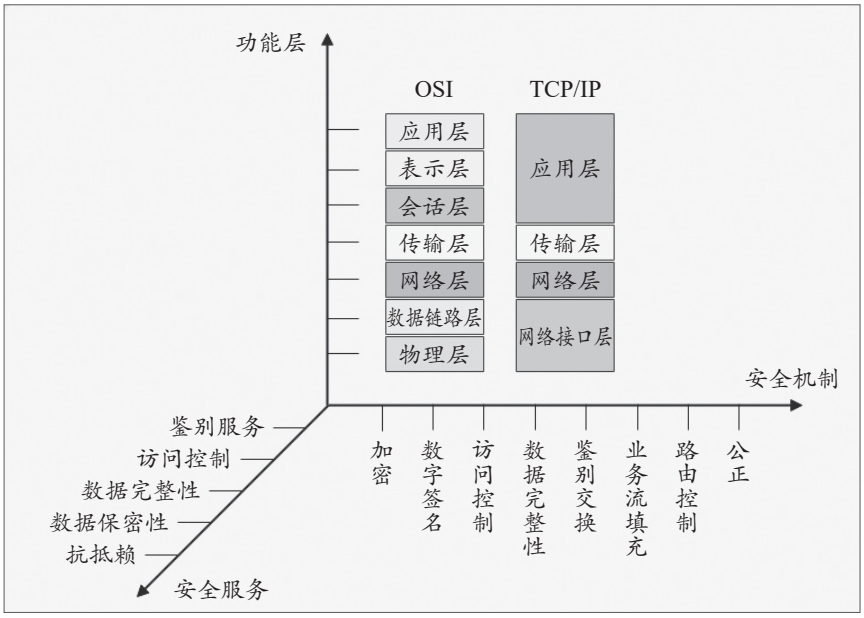

图 4-2

知识拓展

安全服务的位置

实际上，最适合配置安全服务的是物理层、网络层、传输层和应用层，其他层都不宜配置安全服务。从安全体系结构来说，OSI参考模型和TCP/IP参考模型研究的内容是相同的。

4. OSI 安全体系结构的优缺点

OSI安全体系结构具有以下优点。

- **开放性**：OSI安全体系结构是一个开放的标准，任何厂商都可以根据该标准开发安全产品和解决方案。

- **通用性**：OSI安全体系结构可以应用于各种网络环境。
- **层次性**：OSI安全体系结构的层次性使其具有良好的可扩展性和可维护性。

OSI安全体系结构也存在以下一些缺点。

- **复杂性**：OSI安全体系结构的层次性使其具有一定的复杂性。
- **性能**：OSI安全体系结构的一些安全机制可能会影响网络性能。

5. OSI 安全体系结构的应用

OSI安全体系结构被广泛应用于各种网络安全系统中。

（1）计算机操作系统

计算机操作系统的安全子系统通常基于OSI安全体系结构进行设计。例如，Windows操作系统使用Kerberos协议实现身份认证，使用访问控制列表（ACL）实现访问控制。

（2）网络安全设备

网络安全设备包括防火墙、入侵检测系统等，通常支持OSI安全体系结构定义的安全服务和机制。例如，防火墙可以根据访问控制规则过滤网络流量，入侵检测系统可以检测网络中的可疑活动。

（3）应用程序安全

应用程序安全通常使用OSI安全体系结构定义的安全服务和机制来保护数据和应用程序。例如，Web应用程序可以使用SSL/TLS协议加密数据，可以使用身份验证机制控制对应用程序的访问。

4.1.2 OSI安全服务

在OSI安全体系结构中，定义了5类安全服务。

1. 鉴别服务

鉴别服务也叫认证服务，确保通信实体的身份真实性。认证服务通常使用用户名/密码、数字证书等技术来实现。鉴别是最基本的安全服务，是对付假冒攻击的有效方法。鉴别可以分为对等实体鉴别和数据源鉴别。

（1）对等实体鉴别

对等实体鉴别是在开放系统的两个同层对等实体间建立连接和传输数据期间，为证实一个或多个连接实体的身份而提供的一种安全服务。这种服务可以是单向的，也可以是双向的；可以带有有效期检验，也可以不带。从七层参考模型看，当由N层提供这种服务时，将使N+1层实体确信与之打交道的对等实体正是它所需要的对等N+1层实体。

（2）数据源鉴别

数据源鉴别服务是对数据单元的来源提供识别，但对数据单元的重复或篡改不提供鉴别保护。从七层参考模型看，当由N层提供这种服务时，将使N+1层实体确信数据来源正是它所需要的对等N+1层实体。

2. 访问控制

访问控制用于控制对资源的访问，防止资源未授权使用。访问控制服务通常使用访问控制列

表（ACL）、角色-权限模型等技术来实现。在OSI安全体系结构中，访问控制安全目标如下。

- 通过进程对数据、通信或其他计算机资源进行访问控制。
- 在一个安全域内的访问或跨越一个或多个安全域的访问控制。
- 按照其上下文进行的访问控制。如根据试图访问的时间、访问者地点或访问路由等因素进行的访问控制。
- 在访问期间对授权更改做出反应的访问控制。

3. 数据完整性

数据完整性服务用于对抗数据在存储、传输等处理过程中被非法篡改。数据完整性服务通常使用数据签名、哈希函数等技术实现。可分为以下3种重要类型。

- 连接完整性服务。
- 无连接完整性服务。
- 选择字段完整性服务。

知识拓展

按是否具有恢复功能划分

完整性服务还可以按是否具有恢复功能划分为不具有恢复功能的完整性服务和具有恢复功能的完整性服务。

4. 数据保密性

数据保密性是保护信息（数据）不会被窃取或不泄露给那些未授权掌握这一信息的实体。数据保密性服务通常使用加密技术实现。在信息系统安全中需要区分两类保密性服务。

- **数据保密性服务：**使攻击者想要从某个数据项中推出敏感信息变得十分困难。
- **业务流保密性服务：**使攻击者想要通过观察通信系统的业务流来获得敏感信息十分困难的。

根据加密的数据项，保密性服务可以有如下几种类型。

- **连接保密性：**为一次连接上的所有用户数据提供保密性保护。
- **无连接保密性：**为单个无连接的SDU中的全部用户数据提供保密性保护。
- **选择字段保密性：**为那些被选择的字段提供保密性保护。这些字段或处于连接的用户中，或者为单个无连接的SDU中的字段。
- **通信业务流保密性：**使得通过观察通信业务流而不可能推断出其中的机密信息。

5. 抗抵赖

抗抵赖又称抗否认服务。前面介绍的OSI安全服务主要是针对来自未知攻击者的威胁，而抗抵赖服务是防止一方否认曾进行过某项通信。抗抵赖服务的目标是保护通信实体免受来自其他合法实体的威胁。抗否认服务通常使用数字签名、时间戳等技术来实现。OSI定义的抗抵赖服务有两种类型。

- **有数据原发证明的抗抵赖：**为数据的接收者提供数据的原发证据，使发送者不能抵赖这些数据的发送或否认发送内容。

- **有交付证明的抗抵赖：**为数据的发送者提供数据交付证据，使接收者不能抵赖收到这些数据或否认接收内容。

4.1.3 OSI安全服务配置

在OSI安全体系中，针对不同类型的安全服务，可在不同层级中实现各种配置。

1. 安全服务分层及配置原则

安全服务分层以及安全机制在OSI七层上的配置应按照下列原则进行。

- 实现一种服务的不同方法越少越好。
- 在多层上提供安全服务来建立安全系统是可取的。
- 为安全所需的附加功能不应该也没必要重复OSI的现有功能。
- 避免破坏层的独立性。
- 可信功能度的总量应尽量少。
- 只要一个实体依赖于由位于较低层的实体提供的安全机制，那么任何中间层应该按不违反安全的方式构建。
- 只要可能，就应以作为自容纳模块起作用的方法来定义一个层的附加安全功能。本标准被认定用于由包含所有七层的端系统组成的开放系统及中继系统。

2. OSI 各层中的安全服务配置

OSI各层提供的安全服务配置如表4-1所示。不论要求的安全服务是由该层提供还是由下层提供，各层上的服务定义都可能需要修改。

表 4-1

安全服务	协议层						
	1	2	3	4	5	6	7
对等实体鉴别			✓	✓			✓
数据源鉴别			✓	✓			✓
访问控制			✓	✓			✓
连接保密性	✓	✓	✓	✓		✓	✓
无连接保密性		✓	✓	✓		✓	✓
连接字段保密性							✓
通信业务流保密性						✓	✓
带恢复的连接完整性	✓		✓				✓
不带恢复的连接完整性				✓			✓
选择字段连接完整性			✓	✓			✓
无连接完整性							✓
选择字段无连接完整性			✓	✓			✓
有数据原发证明的抗抵赖							✓
有交付证明的抗抵赖							✓

4.1.4 OSI安全机制

OSI安全体系结构没有说明5种安全服务如何实现，但是它给出了8种基本的（特定的）安全机制，使用这8种安全机制，再加上几种普遍性的安全机制，将它们设置在适当的层上，用以提供OSI安全体系结构安全服务。

1. 加密

在OSI安全体系结构的安全机制中，加密涉及三方面的内容。

- 密码体制的类型，对称密码体制和非对称密码体制。
- 密钥管理。
- 加密层的选取。加密层选取时要考虑的因素如表4-2所示，它不推荐在数据链路层上的加密。

表 4-2

加密要求	加密层
对全部通信业务提供加密	物理层
对每个应用提供不同的密钥； 抗抵赖或选择字段保护	表示层
提供保密性与不带恢复的完整性； 对所有端对端之间通信的简单块进行保护； 希望有一个外部的加密设备（如为了给算法和密钥提供物理保护或防止软件错误）	网络层
提供带恢复的完整性以及细粒度保护	传输层

2. 数字签名

数字签名是附加在数据单元上的一些数据，或是对数据单元所做的密码变换，这种附加数据或变换可以起如下作用。

- 供接收者确认数据来源。
- 供接收者确认数据完整性。
- 保护数据，防止他人伪造。

知识拓展

数字签名的过程

数字签名需要确定两个过程。

- 对数据单元签名，使用签名者的私有（独有或机密的）信息。
- 验证签过名的数据单元，使用的规程和信息是公开的，但不能推断出签名者的私有信息。

3. 访问控制

访问控制是一种对资源访问或操作加以限制的策略。此外它还可以支持数据的保密性、数据完整性、可用性以及合法使用的安全目标。访问控制机制可应用于通信联系中的任一端点或任一中间点。

访问控制机制可以建立在下面的一种或多种手段之上。

- 访问控制信息库，保存了对等实体的访问权限。
- 鉴别信息，如口令等。
- 权限。
- 安全标记。
- 试图访问的时间。
- 试图访问的路由。
- 访问持续期。

4. 数据完整性

数据完整性保护的目的是避免未授权的数据乱序、丢失、重放、插入和篡改。数据完整性包括两方面：单个数据或字段的完整性和数据单元流或字段流的完整性。决定单个数据单元的完整性涉及两个实体：一个在发送实体上，一个在接收实体上。发送实体给数据单元附上一个附加量，接收实体也产生一个相应的量，通过比较二者，可以判定数据在传输过程中是否被篡改。

注意事项 保护数据单元的完整性

对于有连接的数据传送，保护数据单元序列的完整性（包括防止乱序、数据丢失、重放或篡改）还需要明显的排序标记，如顺序号、时间标记或密码链；对于无连接的数据传送，时间标记可以提供一定程度的保护，防止个别数据单元重放。

5. 鉴别交换

可用于鉴别交换的技术有鉴别信息，如口令；密码技术；使用该实体特征（生物信息等）或占有物（信物等）。可以结合使用的技术有时间标记与同步时钟、两次握手（单方鉴定）和三次握手（双方鉴定）、数字签名和公证。

6. 业务流填充

业务流填充是一种反分析技术，通过虚假填充将协议数据单元达到一个固定长度，只有受到机密服务保护时才有效。

7. 路由控制

路由控制机制可以使敏感数据只在具有适当保护级别的路由上传输，并且采取如下处理方式。

- 检测到持续攻击，可以为端系统建立不同的路由连接。
- 依据安全策略，使某些带有安全标记的数据禁止通过某些子网、中继或链路。
- 允许连接的发起者（或无连接数据单元的发送者）指定路由选择，或回避某些子网、中继或链路。

8. 公正

公证机制是由可信的第三方提供数据完整性、数据源、时间和目的地等的认证和保证。

知识拓展

安全服务与安全机制之间的关系

在OSI安全服务与安全机制之间的关系可以参考表4-3所示的内容。

表 4-3

安全服务	安全机制							
	加密	数字签名	访问控制	数据完整性	鉴别交换	业务流填充	路由控制	公正
对等实体鉴别	✓	✓			✓			
数据源鉴别	✓	✓						
访问控制			✓					
连接保密性	✓						✓	
无连接保密性	✓						✓	
连接字段保密性	✓							
流量保密性	✓					✓	✓	
带恢复的连接完整性	✓			✓				
不带恢复的连接完整性	✓			✓				
选择字段连接完整性	✓			✓				
无连接完整性	✓	✓		✓				
选择字段无连接完整性	✓	✓		✓				
原发方抗抵赖	✓	✓		✓				✓
接收方抗抵赖		✓		✓				✓

4.1.5 TCP/IP模型的安全体系结构

除了OSI七层模型的安全体系外，TCP/IP模型也有其安全体系结构。

1. TCP/IP 模型安全体系结构的出现

TCP/IP协议簇在设计之初并没有认真地考虑网络安全功能，为了解决TCP/IP协议簇带来的安全问题，Internet工程任务组（IETF）不断地改进现有协议和设计新的安全通信协议来对现有的TCP/IP协议簇提供更强的安全保证，在互联网安全性研究方面取得了丰硕的成果。由于TCP/IP各层协议提供了不同的功能，为各层提供了不同层次的安全保证，因此专家为协议的不同层设计了不同的安全通信协议，为网络的各层提供安全保障。目前，TCP/IP安全体系结构已经制定了一系列的安全通信协议，为各层提供了一定程度上的安全保障。由各层安全通信协议构成

的TCP/IP协议簇的安全架构业已形成。

2. TCP/IP 模型安全体系结构的层次结构

TCP/IP的安全性可分为多层，各安全层包含多个特征实体。在不同层次，可增加不同安全策略和措施，如在传输层提供安全套接层服务SSL和其继任者传输层安全TLS，这是为网络通信提供安全及数据完整性的一种安全协议，以及在网络层提供虚拟专用网VPN技术等。TCP/IP网络安全技术层次体系如图4-3所示。

<table>
<tr><td rowspan="5">应用层

传输层

网络层（IP）

网络接口层</td><td colspan="4">应用层安全协议（如S/MIME、SHTTP、SNMPv3）</td><td rowspan="5">第三方公正（如Kerberos）数字签名</td><td rowspan="5">响应
恢复
审计
日志
入侵检测（IDS）
漏洞扫描</td><td rowspan="5">安全服务管理

安全机制管理

安全设备管理

物理保护</td><td rowspan="5">系统安全管理</td></tr>
<tr><td>用户
身份认证</td><td colspan="2">授权与代理服务器
防火墙、CA</td><td></td></tr>
<tr><td colspan="4">传输层安全协议（如SSL/TLS、PCT、SSH、SOCKS）</td></tr>
<tr><td colspan="4">电路级防火
网络层安全协议（如IPSec）</td></tr>
<tr><td>数据源认证
IPSec-AH</td><td colspan="2">包过滤
防火墙</td><td>如VPN</td></tr>
<tr><td></td><td>相邻节点间的认证（如MS-CHAP）</td><td>子网
划分VLAN
物理
隔绝</td><td>MDC
MAC</td><td>点对点加密(MS-MPPE)</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>认证</td><td>访问控制</td><td>数据完整性</td><td>数据保密性</td><td>抗抵赖</td><td>可控性</td><td>可审计性</td><td>可用性</td></tr>
</table>

图 4-3

3. TCP/IP 模型中的安全隐患和应对

TCP/IP参考模型在设计之初并没有过多考虑网络威胁，随着网络的发展，TCP/IP参考模型中的安全隐患逐渐暴露，如图4-4所示，当然隐患也在被逐渐修补。下面介绍主要的安全隐患及应对方法。

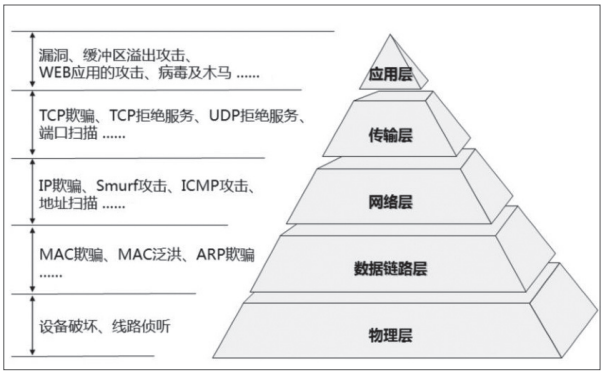

图 4-4

（1）网络接口层的主要安全隐患及应对

TCP/IP模型的网络接口层对应OSI模型的物理层和数据链路层。物理层安全问题是指由网络

环境及物理特性产生的网络设施和线路安全性，致使网络系统出现安全风险，如设备问题、意外故障、信息探测与窃听等。由于以太网上存在交换设备，有些通信采用广播方式。非授权者可能在某个广播域中侦听、窃取并分析信息。为此，保护链路上的设施安全极为重要，物理层的安全措施相对较少，最好采用“隔离技术”保证每两个网络在逻辑上能够连通，同时从物理上隔断，并加强实体安全管理与维护。

网络接口层安全通信协议为通过通信链路连接起来的主机或路由器之间的安全提供了保证，PPTP、L2TP是主要的数据链路层安全通信协议。数据链路层安全通信协议拥有较高的效率，但是通用性和扩展性较差。

（2）网络层的主要安全隐患及应对

网络层主要用于数据包的网络传输，其中IP协议是整个TCP/IP协议体系结构的重要基础。网络层安全通信协议旨在解决网络层通信中产生的安全问题，对TCP/IP协议而言，主要解决IP协议中存在的安全问题。目前，IPSec是最重要的网络层安全通信协议。网络层安全通信协议对网络层以上各层透明，但是难以提供不可否认的服务。

知识拓展

IPv4的安全性

IPv4在设计之初根本没有考虑到网络安全问题，IP包本身不具有任何安全特性，从而导致在网络上传输的数据包很容易泄露或受到攻击，IP欺骗和ICMP攻击都是针对IP层的攻击手段，如伪造IP包地址、拦截、窃取、篡改、重播等。

（3）传输层的主要安全隐患及应对

TCP/IP传输层主要包括传输控制协议TCP和用户数据报协议UDP，其安全措施主要取决于具体的协议。传输层的安全主要包括传输与控制安全、数据交换与认证安全、数据保密性与完整性等。TCP是面向连接的协议，用于多数互联网服务，如HTTP、FTP和SMTP等。为了保证传输层的安全，设计了安全套接层协议（Secure Socket Layer，SSL），现更名为传输层协议（Transport Layer Security，TLS），主要包括SSL握手协议和记录协议。

SSL协议用于数据认证和数据加密的过程，利用多种有效密钥交换算法和机制。SSL记录协议对应用程序提供的信息分段、压缩、认证和加密，此协议提供了身份验证、完整性检验和保密性服务，密钥管理的安全服务可为各种传输协议重复使用。它可以在进程与进程之间实现安全通信，但是需要修改对应程序，同时也不能提供透明的安全保障。

（4）应用层的主要安全隐患及应对

应用层的功能是为应用进程服务，实现不同系统的应用进程之间的互相通信，完成特定的业务处理和服务。应用层提供的服务有电子邮件、文件传输、虚拟终端和远程数据输入等。网络层的安全协议为网络传输和连接建立安全的通信管道，传输层的安全协议保障传输数据的可靠、安全地到达目的地，但无法根据传输内容的不同安全需求予以区别对待。灵活处理具体数据的不同安全需求方案就是在应用层建立相应的安全机制。例如IETF规定了使用强化邮件PEM来为基于SMTP的电子邮件系统提供安全服务；免费电子邮件系统PGP提供数字签名和加密功能；HTTPS是Web上使用的超文本传输协议的安全增强版本。

4.2 数据链路层的安全协议

数据链路层主要负责在网络实体间建立和维持数据链路，并在相邻节点之间传输数据。数据链路层的安全主要依赖于PAP、CHAP、PPTP等协议的支持。

4.2.1 PAP

PAP（Password Authentication Protocol，密码认证协议）是一种简单、易用的网络认证协议，主要用于用户登录网络服务器。PAP由IETF（Internet Engineering Task Force）在1993年发布的RFC 1332中定义。PAP最初是作为PPP（Point-to-Point Protocol）的一部分而设计的，用于在点对点连接上进行用户认证。后来，PAP也被扩展到其他网络协议中，例如IPX/SPX和NetWare。PAP采用明文传输密码，因此安全性较低，不适用于高安全性的网络环境。

1. PAP 的工作原理及流程

PAP的工作原理是客户端向服务器发送PAP请求报文，其中包含用户名和密码。服务器验证用户名和密码是否正确，如果正确则向客户端发送PAP成功报文，如果错误则向客户端发送PAP失败报文。PAP的具体工作流程如下。

步骤 01 客户端向服务器发送PAP请求报文。

步骤 02 服务器收到PAP请求报文后，解析其中的用户名和密码。

步骤 03 服务器将用户名和密码与数据库中的用户名和密码进行匹配。

步骤 04 如果匹配成功，服务器向客户端发送PAP成功报文。

步骤 05 如果匹配失败，服务器向客户端发送PAP失败报文。

步骤 06 客户端收到PAP响应报文后，根据响应报文中的Code字段判断认证是否成功。

2. 协议报文格式

PAP在PPP拨号上网系统中的执行过程为，PAP的包被封装到PPP帧中，PAP认证所使用的三种包如图4-5所示，无论传输哪一种包，它的协议类型字段的值为0xC023。

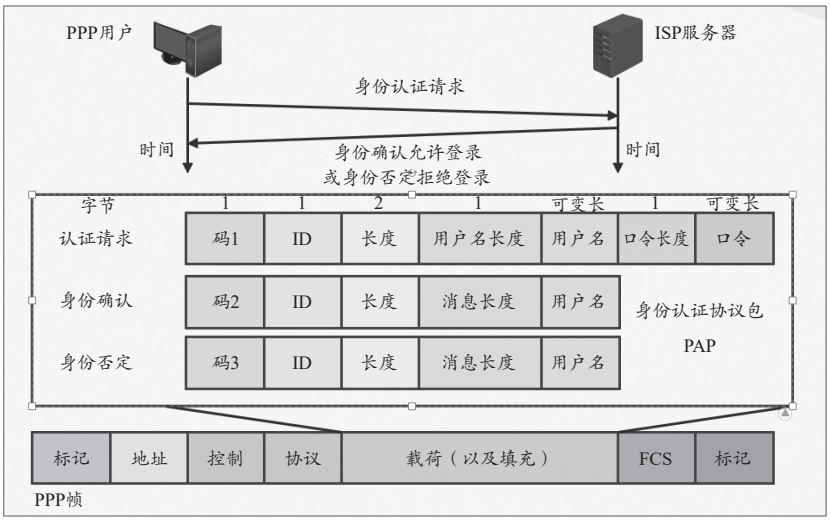

图 4-5

第一种包是身份认证请求（Authentication Request），用户用它向系统发送用户名和口令，请求接入系统。第二种包是身份确认（Authentication- Acknowledgement），系统用它告诉用户，其身份已被认可，允许用户访问系统。第三种包是身份否定（Authentication Nack），系统用它告诉用户，该用户名或口令未通过认证，拒绝其访问系统。PAP协议将用户名和口令用ASCII编码的明文方式在链路上传输，很容易被截获，存在用户名和口令泄露等安全问题。

3. PAP 的优缺点

PAP的优点在于结构简单，易于实现和部署。用户只需输入用户名和密码即可进行认证。另外其兼容性好，支持多种网络操作系统和网络设备。

PAP的缺点在于，由于采用明文传输密码，因此安全性较低，容易被窃听和破解。另外，PAP协议易受字典攻击和暴力攻击。而且PAP的效率比较低，客户端会不断重复发送身份验证信息，这可能会导致网络资源的浪费，尤其是在网络状况不佳的情况下。

在公共网络中应避免使用PAP，以免密码被窃听。在高安全性的网络环境中，应部署更安全的认证协议，例如CHAP、EAP等。如果必须使用PAP，则应使用强度较高的密码，并定期更换密码。

4. PAP 的应用范围

PAP可以应用到以下场景中。

（1）局域网用户登录

在局域网中，用户可以使用PAP登录服务器、路由器等网络设备。例如，用户可以使用PAP登录Windows Server，然后访问服务器上的共享资源。

（2）远程访问

在远程访问场景中，用户可以使用PAP登录远程服务器。例如，用户可以使用PAP登录VPN服务器，然后通过VPN连接访问公司内部网络。

（3）无线网络用户登录

在无线网络中，用户可以使用PAP登录无线AP。例如，用户可以使用PAP登录家用无线路由器，然后连接到无线网络。

4.2.2 CHAP

CHAP（Challenge Handshake Authentication Protocol，挑战-应答认证协议）是一种比PAP更安全的网络认证协议，主要用于用户登录网络服务器。CHAP采用挑战-应答机制来验证用户身份，可以有效抵御字典攻击和暴力攻击。

CHAP由IETF在1993年发布的RFC 1332中定义。CHAP最初是作为PPP（Point-to-Point Protocol）的一部分而设计的，用于在点对点连接上进行用户认证。后来，CHAP也被扩展到其他网络协议中，例如IPX/SPX和NetWare。

1. CHAP 的工作原理及流程

CHAP的工作原理是服务器向客户端发送一个随机数（称为挑战值），客户端使用自己的密码对挑战值进行加密，然后将加密后的结果发送回服务器。服务器使用客户端提供的密码对挑

战值进行加密，并比较两个加密结果是否一致。如果一致，则认证成功；如果不一致，则认证失败。CHAP协议的具体工作流程如下。

步骤 01 客户端向服务器发送CHAP请求报文。

步骤 02 服务器收到CHAP请求报文后，生成一个随机数（称为挑战值），并将其发送给客户端。

步骤 03 客户端收到挑战值后，使用自己的密码对挑战值进行加密，然后将加密后的结果（称为响应值）发送回服务器。

步骤 04 服务器收到响应值后，使用客户端提供的密码对挑战值进行加密，并比较两个加密结果是否一致。

步骤 05 如果一致，服务器向客户端发送CHAP成功报文。

步骤 06 如果不一致，服务器向客户端发送CHAP失败报文。

步骤 07 客户端收到CHAP响应报文后，根据响应报文中的Code字段判断认证是否成功。

2. CHAP 的报文格式

CHAP在PPP拨号上网系统中的执行过程如图4-6所示。CHAP的包被封装到PPP帧中，帧内协议类型字段的值为0xC223。有4种CHAP包：第一种是挑战包，系统向用户发送挑战值。第二种是响应包，用户向系统发送计算结果。第三种是身份确认包，系统告诉用户允许访问系统。第四种是身份否定包，系统告诉用户拒绝访问系统。

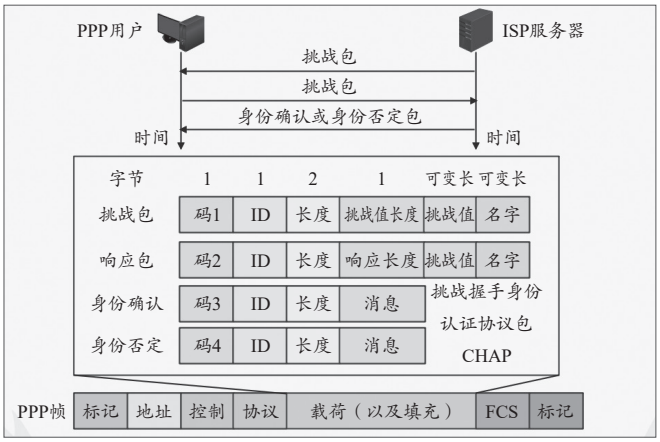

图 4-6

知识拓展

CHAP的优缺点及应对

CHAP采用挑战-应答机制验证用户身份，可以有效抵御字典攻击和暴力攻击。CHAP的结构简单，易于实现和部署。CHAP兼容性好，支持多种网络操作系统和网络设备。但CHAP易受中间人攻击，攻击者可以窃取挑战值和响应值，然后伪造认证请求欺骗服务器。CHAP没有密码保护机制，如果服务器的数据库被泄露，攻击者就可以获得所有用户的密码。

因此在使用CHAP时，在服务器和客户端之间部署SSL/TLS加密，可以防止攻击者窃取挑战值和响应值。另外定期更换密码可以降低密码被泄露的风险。

3. CHAP 的应用

CHAP主要用于计算机网络中的安全身份验证。其应用涉及各种场景，包括远程访问、虚拟专用网络（VPN）、拨号连接等。下面是CHAP在这些场景中的应用。

（1）远程访问

在远程访问场景中，用户需要通过互联网或其他公共网络远程连接到企业内部网络或其他安全网络资源。CHAP可以用于远程用户向服务器进行身份验证，以确保只有授权用户可以访问网络资源。典型的应用场景包括远程办公、远程维护、远程教育等。

（2）虚拟专用网络（VPN）

VPN允许用户通过公共网络安全地访问企业内部网络或其他受限网络资源。CHAP可用于VPN客户端与VPN服务器之间的身份验证，确保用户的身份和访问权限。CHAP的使用可以增加VPN连接的安全性，并防止未经授权的用户访问VPN服务。

（3）拨号连接

在拨号连接场景中，用户通过拨号方式连接到服务器或其他网络设备，以获取对网络资源的访问权限。CHAP可用于拨号客户端与服务器之间的身份验证。传统的拨号连接场景包括远程办公、远程访问公司内部资源等。

（4）无线接入点（WiFi）

在无线网络环境中，CHAP也可以用于WiFi接入点和WiFi客户端之间的身份验证。例如，在企业或公共场所的无线网络中，用户连接到WiFi网络时可以使用CHAP进行安全身份验证。使用CHAP可以确保连接到WiFi网络的用户身份和访问权限，并提供更高的网络安全性。

（5）其他场景

CHAP还可以在其他需要安全身份验证的场景中应用，例如远程设备管理、远程监控等。由于CHAP提供一种安全、灵活和可靠的身份验证机制，因此在各种网络环境中都有广泛的应用。

4.2.3 PPTP

PPTP（Point-to-Point Tunneling Protocol，点对点隧道协议）是一种广泛使用的网络协议，用于在公网上建立虚拟专用网络（VPN）。PPTP通过将非安全网络流量封装在安全隧道中，可有效保护用户隐私和数据安全，使远程用户能够安全地访问企业内部网络或其他私有网络资源。PPTP由微软于1995年发布，最初用于Windows NT 3.51。随后，PPTP被广泛应用于各种操作系统和网络设备中，成为最常用的VPN协议之一。

1. PPTP 的工作原理

客户端创建一个虚拟的点对点连接到VPN服务器，然后将所有非安全的网络流量封装在PPP（Point-to-Point Protocol）数据包中，通过VPN隧道发送到VPN服务器。VPN服务器解密PPP数据包，并将解密后的数据包转发到目的地。

PPTP的协议规范本身并未描述加密或身份验证的部分，它依靠点对点协议（PPP）来实现这些安全性功能。因为PPTP内置在Windows系统家族的各产品中，在微软点对点协议的协议堆栈中，提供了各种标准的身份验证与加密机制来支持PPTP。在Windows系统中，它可以搭配

PAP、CHAP、MS-CHAPv1/v2或EAP-TLS来进行身份验证。通常也可以搭配微软点对点加密（MPPE）或IPSec的加密机制来提高安全性。

PPTP将原始数据包装在GRE（Generic Routing Encapsulation）封装中，然后在IP网络上进行传输。在封装过程中，PPTP还可以对数据进行加密，以确保通信的机密性。

知识拓展

MPPE

PPTP可以使用MPPE（Microsoft Point-to-Point Encryption）协议对PPP数据包进行加密，MPPE协议使用对称加密算法，可以保护用户隐私和数据安全。

2. PPTP 的连接建立步骤

PPTP的连接建立过程如下。

步骤 01 建立连接请求。客户端向VPN服务器发起连接请求。

步骤 02 身份验证。客户端和服务器之间进行身份验证。常见的身份验证方法包括PAP（Password Authentication Protocol）和CHAP。

步骤 03 建立隧道。一旦身份验证成功，客户端和服务器之间建立PPTP隧道。

步骤 04 数据传输。数据在PPTP隧道中进行加密和传输，确保数据的机密性和完整性。

步骤 05 连接终止。当会话结束时，客户端和服务器之间的PPTP连接被终止。

3. PPTP 面临的挑战

PPTP是一种轻量级的VPN协议，易于实现和部署。它通常内置在各种操作系统中，包括Windows、Linux和macOS等。由于PPTP的简单性和易用性，它在早期被广泛应用于远程访问和企业网络连接等场景中。

PPTP的主要安全缺陷体现在其使用的MPPE加密算法上。MPPE算法基于RC4加密算法，而RC4算法已被证明存在严重的缺点。RC4算法容易受到密钥泄露攻击。一旦攻击者窃取了RC4加密密钥，就可以解密所有使用该密钥加密的数据。

知识拓展

RC4算法的安全威胁

RC4算法存在理论上的攻击方法，例如碰撞攻击和相关密钥攻击。尽管这些攻击方法尚未在现实中被成功实施，但仍然对RC4算法的安全构成了威胁。

PPTP只提供用户名和密码的身份验证机制，这并不足以抵御高级攻击者。由于PPTP的加密机制相对较弱（默认情况下不使用TLS/SSL加密），易受到破解和中间人攻击。攻击者可以伪造VPN服务器，窃取用户的用户名和密码以及传输的数据。另外PPTP连接通常需要为客户端分配IP地址，如果IP地址池不足或者配置错误，可能会导致连接问题。

4.3 网络层安全协议

网络层主要解决点到点的数据传输，这里的端点指的是主机或路由器。网络层负责在不同的节点之间进行数据传输，并提供路由、转发和流量控制等功能。网络层的目标是尽最大努力进行数据的交付，涉及数据的保密性和完整性，主要的安全目标是防止在交换过程中数据被非法窃听和篡改。

4.3.1 IPSec安全协议套件

IPSec（Internet Protocol Security）是一组用于在网络层提供安全性的协议套件，用于保护IP数据包的安全传输、身份验证和完整性保护。它通过加密、认证和安全通信协议提供安全保护，适用于各种网络环境，包括互联网、企业内部网络和虚拟专用网络（VPN）。

1. IPSec 的工作原理

IPSec的工作原理可以归纳为加密、认证和安全通信协议。

（1）加密

IPSec使用加密算法对数据包进行加密，以保护数据的机密性。常用的加密算法包括DES、3DES、AES等。

（2）认证

IPSec还使用认证算法对数据包进行认证，以确保数据的发送是合法的。常用的认证算法包括HMAC（Hash-based Message Authentication Code）和Digital Signature Algorithm（DSA）等。

（3）安全通信协议

IPSec使用安全通信协议定义加密算法、认证算法和密钥协商过程。常用的安全通信协议包括IKE（Internet Key Exchange）和ESP（Encapsulating Security Payload）等。

2. IPSec 的功能

IPSec可以实现以下4项功能。

（1）数据机密性

IPSec发送方将包加密后再通过网络发送。

（2）数据完整性

IPSec可以验证IPSec发送方发送的包，以确保数据传输时没有被改变。

（3）数据认证

IPSec接收方能够鉴别IPSec包的发送起源。此服务依赖数据的完整性。

（4）反重放

IPSec接收方能检查并拒绝重放包。

3. IPSec 的组成

IPSec主要由以下协议组成。

（1）认证头（AH）

认证头（Authentication Header，AH）为IP数据报提供无连接数据完整性、消息认证，以及

防重放攻击保护，但不提供加密服务。它通过在IP头部添加一个特殊的AH头部来实现。

（2）封装安全载荷（ESP）

封装安全载荷（Encapsulating Security Payload，ESP）提供机密性、数据源认证、无连接完整性、防重放和有限的传输流（traffic-flow）机密性。ESP可以对IP数据报的内容进行加密，保证数据的私密性。ESP协议将IP数据报封装在ESP报头中，并加密整个IP数据报。

（3）安全关联（SA）

提供算法和数据包，提供AH、ESP操作所需的参数。AH和ESP协议都必须使用SA。IKE协议的主要功能之一是建立和维护SA。IPSec规定，所有AH和ESP的实现都必须支持SA。一个SA是一个单一的“连接”，为其承载的通信提供安全服务。SA的安全服务是通过使用AH或ESP（不能同时使用）来建立的。如果一个通信流需要同时使用AH和ESP进行保护，则要创建两个或更多的SA来提供所需的保护。SA是单向的，为了保证两个主机或两个安全网关之间双向通信的安全，需要建立两个SA，各自负责一个方向。一个SA由一个三元组唯一标识。

知识拓展

三元组的元素

三元组的元素是安全参数索引（SPI）、IP目的地址、安全协议（AH或ESP）标识符。理论上讲，目的地址可以是一个单播地址、组播地址或广播地址。目前，IPSec的SA管理机制只支持单播SA。

（4）密钥协议（IKE）

用于自动协商安全关联（SA），包括密钥的管理和交换。IKE确保了安全参数的协商过程是安全的，并且能够生成和更新所需的密钥。它提供以下功能。

- **协商服务：**通信双方协商所使用的协议、密码算法和密钥。
- **身份鉴别服务：**对参与协商的双方身份进行认证，确保双方身份的合法性。
- **密钥管理：**对协商的结果进行管理。
- **安全交换：**产生和交换所有密钥的密码源物质。

IKE是一个混合型协议，集成了ISAKMP（Internet Security Associations and Key Management Protocol）和部分Oakley密钥交换方案。

4. IPSec 的工作模式

IPSec共有两种工作模式：传输模式和隧道模式。

（1）传输模式

在传输模式下，IPSec协议只对上层协议数据（例如TCP或UDP数据）进行加密，而IP头部信息保持不变，如图4-7所示。传输模式通常用于保护端到端通信，例如主机之间的通信。

（2）隧道模式

在隧道模式中，IP数据报有两个IP头。一个是外部的IP头，用于指明IPSec数据报的目的地；另一个是内部的IP头，用于指明IP数据报的最终目的地，如图4-8所示。隧道模式通常用于连接两个网络设备，例如路由器或VPN服务器。

图 4-7

图 4-8

5. IPSec 的实现模式

IPSec可以采用两种模式实现：主机实现和网关实现。每种实现模式的应用目的和实施方案有所不同，主要取决于用户的网络安全需求。

（1）主机实现

由于主机是一种端节点，因此主机实现模式主要用于保护一个内部网中两个主机之间的数据通信。主机实现方案可分为以下两种类型。

在操作系统上集成实现：由于IPSec是一个网络层协议，因此可以将IPSec协议集成到主机操作系统上的TCP/IP中，作为网络层的一部分来实现。

嵌入协议栈实现：将IPSec嵌入协议栈中，放在网络层和数据链路层之间来实现。

知识拓展

主机实现的优点

能够实现端到端的安全性；能够实现所有的IPSec安全模式；能够基于数据流提供安全保护。

（2）网关实现

由于网关是一种中间节点，因此网关实现模式主要用于保护两个内部网通过公用网络进行的数据通信，通过IPSec网关构建VPN，从而实现两个内部网之间的安全数据交换。网关实现方案有以下两种类型。

在操作系统上集成实现；将IPSec协议集成到网关操作系统的TCP/IP中，作为网络层的一部分来实现。

嵌入网关物理接口上实现：将实现IPSec的硬件设备直接连接网关物理接口来实现。

知识拓展

网关实现的优点

能够在公用网上构建VPN来保护内部网之间进行的数据交换；能够对进入内部网的用户身份进行验证。

6. SA 的组合使用

一个单一的SA只能从AH或ESP中选择一种安全协议对IP数据报提供安全保护。在有些情况下，一个安全策略要求对一个通信实施多种安全服务，这是用一个SA无法实现的。在这种情况下，需要利用多个SA来实现所需的安全策略。

在多个SA的情况下，必须将一个SA序列组合成SA束，经过SA束处理后的通信能够满足一个安全策略。SA束中的SA顺序是由安全策略定义的，各SA可以终止于不同的端点。将多个SA组合成SA束的方法有以下两种。

（1）传输邻接

传输邻接方法是将AH和ESP的传输模式组合使用来保护一个IP数据报，它不涉及隧道，如

图4-9所示。通常这种方法只允许一层组合。因为每个协议只要使用足够健壮的密码算法，其安全性是有保证的，并不需要多层嵌套使用，以减小协议的处理开销。

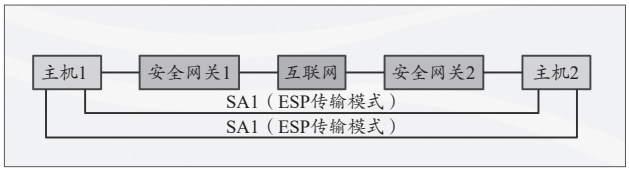

图 4-9

（2）多重隧道

多重隧道方法是由多个SA组合成一个多重隧道来保护IP数据报，每个隧道都可以在不同的IPSec节点（可以进行IPSec处理的设备）上开始或终止。多重隧道可以分成以下三种形式。

① 多重隧道是由两个多SA端点组合而成的，每个隧道都可以用AH或ESP建立，如图4-10所示，主机1和主机2都是多SA端点。

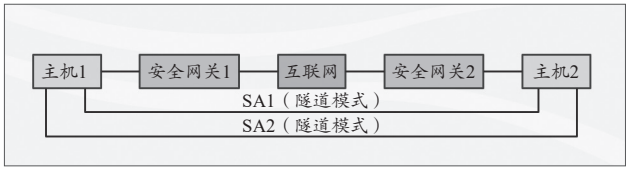

图 4-10

② 多重隧道是由一个多SA端点和一个单SA端点组合而成的，每个隧道都可以用AH或ESP建立，如图4-11所示，主机1是多SA端点，安全网关2和主机2都是单SA端点。

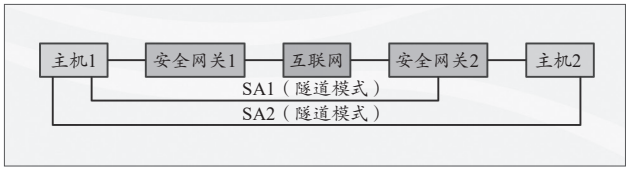

图 4-11

③ 多重隧道是由多个单SA端点组合而成的，这里没有多SA端点，每个隧道都可以用AH或ESP建立，如图4-12所示，主机1、安全网关1、安全网关2和主机2都是单SA端点。

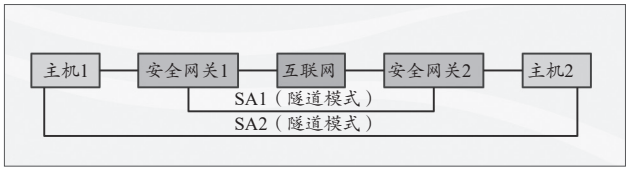

图 4-12

知识拓展

传输模式和隧道模式的组合使用

传输模式和隧道模式还可以组合使用，例如，用一个隧道模式的SA和一个传输模式的SA按顺序组合成一个SA束。对于安全协议的使用顺序，在传输模式下，如果AH和ESP组合使用，则AH应当位于ESP之前，AH作用于ESP生成的密文；在隧道模式下，可以按照不同的顺序使用AH和ESP。

4.3.2 网络层的安全协议

网络层的安全协议主要以IPSec为基础，其中包含网络层的主要安全协议。

1. ESP 协议

ESP是插入IP数据报内的一个协议头，为IP数据报提供数据保密性、数据完整性、抗重播以及数据源验证等安全服务。ESP可以单独使用，也可以利用隧道模式嵌套使用，或者和AH组合起来使用。ESP头格式如图4-13所示。

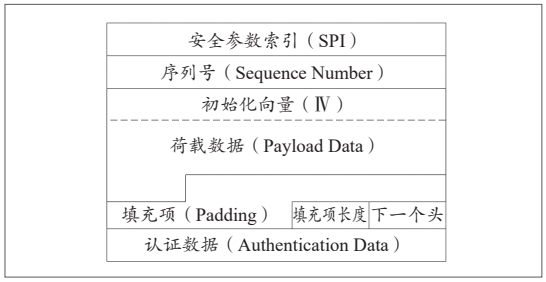

图 4-13

（1）安全参数索引（SPI）

安全参数索引是一个32位的随机数。SPI、目的IP地址和安全协议标识符组成一个三元组，用来唯一地确定一个特定的SA，以便对该数据报进行安全处理。

（2）序列号

序列号是一个单向递增的32位无符号整数。通过序列号，使ESP具有抗重播攻击的能力。尽管抗重播服务是可选的，但是发送端必须产生和发送序列号字段，只是接收端不一定要处理。

（3）初始化向量（IV）

对称加密算法为了增强加密的安全性，往往会引入一个随机数，这个随机数就是初始化向量（32位）。其作用是每次加密时，即使使用相同的密钥，也能产生不同的密文。这使得攻击者更难以通过分析大量密文来破解密钥。

（4）载荷数据

被ESP保护的数据报包含在载荷数据字段中，其字段长度由数据长度决定。如果密码算法需要密码同步数据（如初始化向量（IV）），则该数据要显式地包含在载荷数据中。

（5）填充项

填充项有0～255字节，填充内容可以由密码算法来指定。如果密码算法没有指定，则由ESP指定，填充项的第一个字节值是1，后面的所有字节值都是单向递增的。

（6）填充项长度

填充项字段为8位，指明填充项的长度，接收端利用它恢复载荷数据的实际长度。该字段必须存在，当没有填充项时，其值为0。

（7）下一个头

下一个头字段为8位，指明载荷数据的类型。如果在隧道模式下使用ESP，则其值为4，表示IP-in-IP；如果在传输模式下使用，则其值为上层协议的类型，如TCP对应的值为6。

（8）认证数据

认证数据字段是可变长的，它是由认证算法对ESP数据报进行哈希计算得到的完整性检查值（ICV）。

知识拓展

加密器与验证器

ESP使用一个加密器提供数据保密性，使用一个验证器提供数据完整性认证。加密器和验证器所采用的专用算法是由ESP安全关联的相应组件决定的。因此，ESP是一种通用的、易于扩展的安全机制，它将基本的ESP功能定义和实际提供安全服务的专用密码算法分离开，有利于密码算法的更换和更新。

ESP可采用传输模式或隧道模式对IP数据报进行保护。在传输模式中，ESP头是在IP头和上层协议头之间，如图4-14所示。

在隧道模式中，整个IP数据报都封装在一个ESP头中进行保护，并增加一个新的IP头，如图4-15所示。

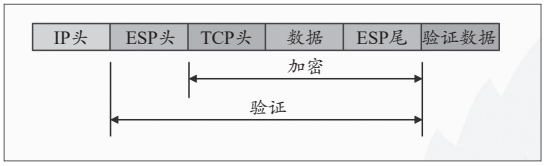

图 4-14

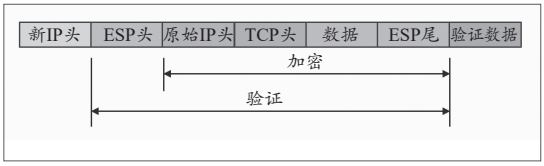

图 4-15

2. AH 协议

AH协议为IP数据报提供数据完整性、数据源验证以及抗重播等安全服务，但不提供数据保密性服务。也就是说，除了数据保密性之外，AH提供了ESP所能提供的一切服务。

AH可以采用隧道模式来保护整个IP数据报，也可以采用传输模式只保护一个上层协议报文。在任何一种模式下，AH头都会紧跟在一个IP头之后。AH不仅可以为上层协议提供认证，还可以为IP头某些字段提供认证。

知识拓展

不受保护的内容

由于IP头中的某些字段在传输中可能会被改变，如服务类型、标志、分段偏移、生存期以及头校验和等字段，发送方无法预测最终到达接收方时这些字段的值，因此，这些字段不能受AH保护。

AH可以单独使用，也可以和ESP结合使用，或者利用隧道模式以嵌套方式使用。AH提供的数据完整性认证的范围和ESP有所不同，AH可以对外部IP头的某些固定字段（包括版本、头长度、报文总长度、标识、协议号、源IP地址、目的IP地址等字段）进行认证。

（1）AH头格式

在任何模式下，AH头总是跟随在一个IP头之后，AH头格式如图4-16所示。

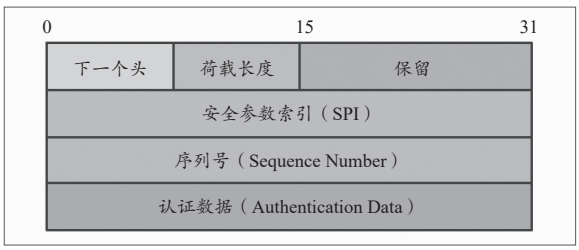

图 4-16

在IPv4 中，IP头的协议号字段值为51，表示在IP头之后是一个AH头。跟随在AH头后的内容取决于AH的应用模式，如果是传输模式，则是一个上层协议头（TCP/UDP），如果是隧道模式，则是另一个IP头。

① 下一个头：8位，与ESP头中对应字段的含义相同。

② 载荷长度：8位，以32位为长度单位，指定了AH的长度，其值是AH头的实际长度减2。

知识拓展

载荷长度的计算

因为AH是一个IPv6扩展头，而IPv6扩展头长度的计算方法是实际长度减1。由于IPv6是以64位为长度单位，而AH是以32位为长度单位进行计算的，所以将减1变换为减2（1个64位长度单位=2个32位长度单位）。如果采用标准的认证算法，认证数据字段长度为96位，加上3个32位固定长度的部分，则载荷长度字段值为4（96/32+3−2=4）。如果使用“空”认证算法，将不会出现认证数据字段，则载荷长度字段值为1。

③ 保留：16位，保留给将来使用，其值必须为0。该字段值包含在认证数据计算中，但被接收者忽略。

④ 安全参数索引（SPI）：32位，与ESP头中对应字段的含义相同。

⑤ 序列号：32位，与ESP头中对应字段的含义相同。

⑥ 认证数据：可变长字段，它是认证算法对AH数据报进行完整性计算所得到的完整性检查值（ICV）。该字段的长度必须是32位的整数倍，因此可能会包含填充项。SA使用的认证算法必须指明ICV的长度、比较规则以及认证的步骤。

（2）AH应用模式

AH可采用传输模式或隧道模式对IP数据报进行保护。在传输模式中，AH头插在IP头和上层协议头之间，如图4-17所示。

在隧道模式中，整个IP数据报都封装在一个AH头中进行保护，并增加一个新的IP头，如图4-18所示。无论是哪种模式，AH都要对外部IP头的固定不变字段进行认证。

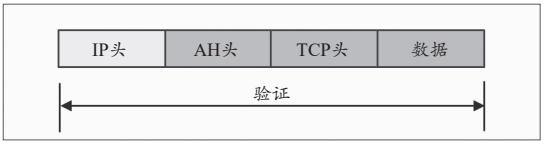

图 4-17

图 4-18

3. 密钥管理协议

在使用IPSec保护一个IP数据报之前，必须先建立一个SA，SA可以手工创建，也可以自动建立。在自动建立SA时，要使用IKE协议。IKE代表IPSec进行SA的协商，并将协商好的SA填入SAD中。IKE确保安全参数的协商过程是安全的，并且能够生成和更新所需的密钥。IKE是一种混合型协议，它建立在以下三个协议的基础上。

（1）ISAKMP协议

ISAKMP协议是一种密钥交换框架，独立于具体的密钥交换协议。在这个框架上，可以支持多种不同的密钥交换协议。

（2）Oakley协议

Oakley协议描述一系列的密钥交换模式，以及每种模式所提供服务的细节，例如，密钥的完美向前保护、身份保护和认证等。

（3）SKEME协议

SKEME协议描述一种通用的密钥交换技术。这种技术提供基于公钥的身份鉴别和快速密钥更新。

IKE通过ISAKMP框架，借鉴了Oakley和SKEME的密钥交换机制，并定义了自己独特的密钥生成和验证方法。

4.3.3 虚拟专用网及其安全协议

虚拟专用网络（Virtual Private Network，VPN）是一种通过加密隧道在公网上创建安全连接的技术。它可以使远程用户安全地访问公司内部网络，也可以使位于不同地理位置的办公室之间进行安全通信。VPN技术可以有效防止数据被窃取、篡改或破坏，确保网络通信的可靠性和完整性。

1. VPN 的工作原理及过程

VPN的基本原理是将用户的数据封装在加密隧道中，并在公网上传输。加密隧道可以防止第三方窃取或篡改数据。VPN通常使用以下步骤建立连接。

步骤 01 客户端软件在用户设备上安装。

步骤 02 客户端软件连接到VPN服务器。

步骤 03 客户端软件和VPN服务器进行身份验证。

步骤 04 如果身份验证成功，客户端软件和VPN服务器建立加密隧道。

步骤 05 用户的数据将通过加密隧道传输。

2. VPN 的安全协议

VPN涉及多个层次，例如在网络层使用IPSec协议，在传输层使用SSL/TLS安全协议。下面介绍一些常用的其他协议。

知识拓展

L2TP协议与IPSec

L2TP是一种在数据链路层提供虚拟专用网络连接的协议，同时使用IPSec加密和认证L2TP通信，用于创建安全的VPN。L2TP与IPSec中使用的加密算法、认证算法、密钥管理是相同的。

（1）MPLS VPN

多协议标签交换虚拟专用网络（MPLS VPN）是一种基于MPLS技术的VPN解决方案，可以为VPN连接提供安全保障。MPLS VPN将VPN流量封装在MPLS隧道中，并使用IPSec协议加密隧道中的数据。该协议的优点如下。

- 性能高，传输效率快。
- MPLS技术可以提供高效的路由机制，因此MPLS VPN的传输效率比传统的IP VPN更高。

● 可扩展性强，MPLS VPN可以支持大规模的网络部署。

● 安全性高，MPLS VPN使用IPSec协议加密隧道中的数据，可以提供强大的安全保障。

但需要部署MPLS网络，成本较高，配置也稍复杂，需要一定的专业知识。

（2）GRE VPN

通用路由封装虚拟专用网络（GRE VPN）是一种基于GRE协议的VPN解决方案，可以为VPN连接提供安全保障。GRE VPN将VPN流量封装在GRE隧道中，并使用IPSec协议加密隧道中的数据。该协议的优点如下。

● 部署简单，成本低廉，GRE VPN不需要部署MPLS网络。

● 灵活性和可扩展性强，GRE VPN可以支持多种封装方式和路由协议。

● 兼容性好，GRE VPN可以与大多数网络设备兼容。

但GRE VPN本身的安全性相对较低，需要使用其他安全协议，例如IPSec，以保护VPN连接的安全。GRE VPN 的封装和解封装过程会增加额外的开销，因此效率相对较低。

4.4 传输层安全协议

传输层是计算机网络体系结构中的重要组成部分，位于应用层之下、网络层之上。它负责在两个主机上的进程之间提供逻辑通信，并为应用层提供可靠、有序和高效的数据传输服务。

4.4.1 SSL/TLS协议

SSL/TLS（Secure Sockets Layer/Transport Layer Security，安全套接层/传输层安全）协议是用于在传输层为数据提供安全保障的协议。它可以加密数据、验证数据完整性和防止数据重放攻击，从而确保网络通信的安全性和可靠性。SSL/TLS协议是互联网安全的基础，被广泛应用于各种网络应用程序中，例如Web浏览器、电子邮件、即时通信等。

1. 发展历史

SSL是最早用于保护网络通信的安全协议，由Netscape公司于1995年推出。它通过加密和认证机制来确保数据的安全传输，最初用于保护Web浏览器和Web服务器之间的通信。

TLS是SSL的继任者，IETF（Internet Engineering Task Force）在1999年发布的TLS 1.0版本取代了SSL 3.0版本。TLS协议继承了SSL的基本原理，并对其进行了改进和修订，提高了安全性和性能。目前，TLS 1.3是最新版本，也是最安全的版本。

2. 工作原理

SSL/TLS协议的工作原理可以分为握手协议、记录协议和警报协议三部分。

（1）握手协议

客户端和服务器之间的通信开始时，首先进行SSL/TLS握手协议，用于协商通信双方支持的加密算法、密钥长度、认证方式等参数。

握手协议包括服务器端证书的传输、密钥交换、客户端身份验证等步骤，最终双方协商确定通信参数，建立安全通道。

（2）记录协议

一旦安全通道建立完成，SSL/TLS协议就会开始记录协议阶段。

在记录协议阶段，数据被分割成适当大小的记录，在加密和压缩后发送到目标主机，确保数据的安全传输。

（3）警报协议

警报协议用于在SSL/TLS通信中处理异常情况，如握手失败、证书验证错误等，以确保通信的可靠性和安全性。

3. 加密和认证机制

SSL/TLS协议主要通过以下机制保护通信的安全性。

（1）加密

SSL/TLS协议使用对称加密算法和非对称加密算法来保护数据的机密性。对称加密算法用于加密数据传输过程中的数据，非对称加密算法用于在通信开始时协商对称加密算法所需的密钥。

（2）认证

SSL/TLS协议使用数字证书来验证通信双方的身份。服务器通过向客户端提供数字证书来证明自己的身份，并通过客户端验证证书的有效性。客户端也可以提供证书来进行身份验证，这称为双向身份验证。

（3）数据完整性

SSL/TLS协议可以使用消息认证码（例如HMAC）来验证数据的完整性，防止数据被篡改。

（4）抗重放攻击

SSL/TLS协议可以使用序列号和时间戳来防止数据重放攻击。

4. 协议的优缺点

SSL/TLS协议是网络安全领域的一个重要组成部分，它们通过复杂的密码学机制保护数据的安全传输。该协议具有以下优缺点。

（1）优点

- 安全性高，SSL/TLS协议使用强大的加密技术和身份验证机制来保护数据传输，可以有效防止数据被窃取、篡改或破坏。
- 易于使用，SSL/TLS协议易于部署和使用，客户端和服务器通常无须进行任何特殊的配置即可使用SSL/TLS协议。
- 兼容性好，SSL/TLS协议得到大多数浏览器、操作系统和网络设备的支持。

（2）缺点

SSL/TLS协议的加密和解密过程会增加额外的开销，可能会降低网络传输速率。SSL/TLS协议需要使用数字证书来验证身份，证书管理可能会比较复杂。

5. 协议的应用

SSL/TLS协议被广泛应用于各种网络应用程序中。

- Web浏览器。Web浏览器使用SSL/TLS与Web服务器进行通信，以保护Web页面内容的安

全性和隐私性。

- 电子邮件。邮件客户端可以使用SSL/TLS加密电子邮件内容，以防止电子邮件被窃取或阅读。
- 即时通信。即时通信软件可以使用SSL/TLS加密语音和视频通话以及文本消息，以保护通信内容的隐私性。
- 远程访问。SSH可以安全地远程登录计算机，并传输文件。
- 文件传输。SFTP可以用于安全传输文件。

4.4.2 DTLS协议

DTLS（Datagram Transport Layer Security，数据传输层安全）协议是一种基于UDP协议的安全协议，用于在不安全的网络中为数据传输提供安全保障。它与TLS传输层安全协议类似，但DTLS针对无连接的UDP协议进行了优化，适用于对性能和延迟要求较高的应用场景。

知识拓展

设计目的

DTLS的设计目的是在不可靠的传输层协议（如UDP）上提供安全通信。由于UDP不像TCP那样有内置的可靠传输机制，因此DTLS需要在设计上考虑数据包可能丢失、重复或乱序到达的情况。

1. 工作原理

DTLS协议的工作原理与TLS协议类似，但DTLS协议在握手阶段和数据传输阶段都进行了优化，以提高性能和降低延迟。

（1）握手阶段

DTLS协议的握手阶段比TLS协议更简洁，因为它省略了一些TLS协议中不必要的步骤。例如，DTLS协议不需要客户端发送ClientHello消息，也不需要服务器发送CertificateRequest消息。

（2）数据传输阶段

DTLS协议的数据传输阶段也进行了优化，以提高性能和降低延迟。具体来说，DTLS协议做了以下改进。

- 使用更小的数据包。DTLS协议使用更小的数据包来减少网络传输延迟。
- 减少握手开销。DTLS协议减少了握手阶段的开销，以提高连接建立速度。
- 支持重传。DTLS协议支持数据包重传，以确保数据传输的可靠性，以解决数据丢失、重排和重复等情况。

知识拓展

与TLS的关系

DTLS基于TLS，使用与TLS相同的加密和认证机制，包括对称加密算法、非对称加密算法和数字证书。但DTLS 1.0是基于TLS 1.1，而DTLS 1.2是基于TLS 1.2。由于UDP的不可靠性，DTLS在握手过程中使用了改进的机制来处理可能的数据包丢失或乱序问题。

2. 特点与应用

DTLS协议具有以下特点和应用场景。

- 适用于UDP通信。DTLS协议专门用于保护UDP通信的安全性，适用于实时通信和流媒体传输等场景。
- 适用于广播和多播。DTLS协议常用于广播和多播应用，因为它可以高效地向多个接收者传输数据。
- 保护移动设备通信。由于移动设备对UDP通信的需求增加，DTLS协议在移动通信领域得到了广泛应用，如VoIP、视频通话等。
- 支持多种应用协议。DTLS协议可以用于保护多种应用协议的UDP通信，如DNS、SNMP等。

DTLS协议的最新版本是DTLS 1.3，它修复了早期版本中存在的一些安全漏洞，并提高了性能和安全性。

3. 优缺点

DTLS的优点包括以下几方面。

- 性能高。DTLS协议针对无连接的UDP协议进行了优化，可以提供更高的性能和更低的延迟。
- 易于部署。DTLS协议易于部署和使用，因为它可以与现有的UDP应用和网络基础设施一起使用。
- 安全性高。DTLS协议提供与TLS协议相同的安全功能，可以有效防止数据被窃取、篡改或破坏。

DTLS的缺点是，DTLS协议比UDP协议更复杂，因此需要在客户端和服务器端实现额外的代码。DTLS协议的兼容性不如UDP协议，因为它需要客户端和服务器都支持DTLS协议。

4.4.3 QUIC协议

QUIC（Quick UDP Internet Connections，快速UDP互联网连接）是一种由Google设计的传输层协议，旨在提供更快的网络连接速度和更强的安全性。QUIC基于UDP协议，并结合了TLS加密和HTTP/2多路复用等技术，以解决TCP的一些性能和安全性问题。QUIC协议的开发始于2013年，它是基于Google自身网络实践以及对TCP和TLS协议的改进而设计的。

1. 工作原理

QUIC协议的工作原理主要包括连接建立、多路复用、0-RTT握手、头部压缩和流控制等。

（1）连接建立

QUIC协议通过UDP协议建立连接，并结合TLS协议提供安全连接。它使用Google自定义的QUIC握手协议，实现快速连接建立和迁移。

（2）多路复用

QUIC协议支持多路复用技术，允许在单个连接上并行传输多个数据流。这样可以减少连接建立和关闭的开销，提高网络资源的利用效率。

（3）0-RTT握手

QUIC协议支持0-RTT（Zero Round Trip Time）握手，这意味着客户端可以在首次与服务器建立连接时就发送数据，在后续的连接中，客户端可以重用之前交换的加密密钥，从而无须再次进行握手过程。

（4）头部压缩

QUIC协议使用头部压缩技术，将HTTP头部信息压缩传输，减少了数据传输的开销和网络带宽的占用，提高了传输效率。

（5）流控制

QUIC协议支持流级别的流控制机制，可以根据不同数据流的需求动态调整传输速率，提高网络的稳定性和公平性。

2. 协议的安全性

QUIC协议在安全性方面具有以下特点。

（1）加密传输

QUIC协议使用TLS 1.3协议作为其加密层，通过TLS的安全机制对通信数据进行加密保护，包括对数据的机密性、完整性和身份认证等方面的保护。TLS 1.3协议采用更强的加密算法和安全机制，如ChaCha20-Poly1305加密套件和前向保密（Forward Secrecy）机制，提高了通信数据的安全性。

（2）减少中间人攻击风险

QUIC协议使用了TLS的安全特性来防止中间人攻击。通过数字证书和证书验证，客户端和服务器可以互相验证对方的身份，确保通信的安全性。

QUIC协议在连接建立过程中，通过TLS的公钥加密机制，防止中间人篡改握手过程或伪造服务器身份，确保通信的真实性和完整性。

（3）快速连接建立和0-RTT握手

QUIC协议支持快速连接建立和0-RTT握手，可以减少连接建立的延迟，提高连接的安全性。0-RTT握手允许客户端在首次连接时发送数据，而不需要等待服务器的确认，但需要适当的安全措施来防止重放攻击。

（4）防止流量分析

QUIC协议使用了连接ID（Connection ID）来识别和管理连接状态，而不像TCP协议那样使用固定的IP地址和端口号。这样可以防止基于网络流量分析的攻击，提高通信的隐私性和安全性。

（5）快速更新和迁移

QUIC协议设计了快速更新和迁移的机制，允许在网络切换或连接状态变化时快速更新连接参数，确保通信的持续性和安全性。

4.5 应用层安全协议

应用层是计算机网络体系结构中的最高层，它直接为应用程序提供服务。应用层协议定义了应用程序之间通信的规则和格式，使得应用程序可以相互交换信息。

应用层安全性主要是解决面向应用的信息安全问题，涉及信息交换的保密性和完整性，防止在信息交换过程中数据被非法窃听和篡改。

有些应用层安全协议是对应用层协议的安全性增强，即在应用层协议的基础上增加安全算法协商和数据加密/解密等安全机制，如S-HTTP（Secure HTTP）协议、S/MIME（Secure/MIME）协议等；还有些应用层安全协议是为解决特定应用的安全问题而开发的，如PGP（Pretty Good Privacy）协议等。

4.5.1 HTTPS协议

HTTPS（Hypertext Transfer Protocol Secure，安全超文本传输协议）是HTTP协议的加密版本，用于在Web浏览器和Web服务器之间建立安全的通信通道，以保护数据的机密性、完整性和真实性。HTTPS协议使用TLS/SSL协议加密数据传输，并支持服务器身份验证和数据完整性保护。HTTPS被广泛应用于网站、电子商务和个人隐私保护等领域。

HTTPS使用默认的443端口，而不是HTTP的80端口。HTTPS的请求-应答模式、报文结构、请求方法等都与HTTP相同，但是所有传输的数据都被加密。

知识拓展

HTTPS协议的特殊性

HTTPS协议是应用层协议，但它与其他应用层协议（例如HTTP、FTP、SMTP等）有所不同。HTTPS协议建立在传输层协议（TCP/IP）之上，它使用TLS/SSL协议加密数据传输，并支持服务器身份验证和数据完整性保护。因此，HTTPS协议也可以被视为一种传输层协议，因为它为应用程序通信提供了安全的传输通道。

1. 产生背景

Web系统是互联网中应用最为广泛的应用系统，它基于客户/服务器模式，整个系统由Web服务器、浏览器和通信协议三部分组成。其中，通信协议为超文本传输协议（HTTP），它是为分布式超媒体信息系统设计的一种应用层协议，能够传送任意类型的数据对象，以满足Web服务器与客户之间多媒体通信的需要。

HTTP协议是一种面向TCP连接的协议，客户与服务器之间的TCP连接是一次性连接。它规定每次连接只处理一个请求，服务器返回本次请求的应答后便立即关闭连接，在下次请求时再重新建立连接。这种一次性连接主要考虑到Web服务器面向互联网中的成千上万个用户，只能提供有限个连接，及时地释放连接可以提高服务器的执行效率，避免服务器连接的等待状态。同时，服务器不保留与客户交易时的任何状态，可减轻服务器的存储负担，从而保持较快的响应速度。HTTP协议允许传送任意类型的数据对象，通过数据类型和长度来标识所传送的数据内容和大小，并允许对数据进行压缩传送。

用户在浏览器或HTML文档中定义了一个超文本链接后，浏览器将通过HTTP协议请求与指定的服务器建立连接。如果该服务器一直在HTTP端口上侦听连接请求，该连接便会建立起来。然后客户通过该连接发送一个包含请求方法的请求消息块。HTTP协议定义了7种请求方法，每种请求方法规定了客户和服务器之间不同的信息交换方式，常用的请求方法是GET和POST。服

务器将根据客户请求完成相应的操作，并以应答消息块的形式返回给客户，最后关闭连接。

HTTPS协议最早由网景公司（Netscape）于1994年提出，旨在解决HTTP传输中的安全问题。随后，HTTPS被标准化，并得到了广泛应用。

在实际应用中，HTTPS协议使用比较简便。如果一个Web服务器提供基于HTTPS协议的安全服务，并在客户机上安装该服务器认可的数字证书，则用户可以使用支持SSL协议的浏览器（通常浏览器都支持SSL协议，如IE浏览器等），并通过“https://www.服务器名.com”域名来访问该Web服务器，Web服务器与浏览器之间通过SSL协议进行安全通信，提供身份鉴别、数据加密和数据认证等安全服务。

2. 工作原理

HTTPS的工作原理包含以下几方面。

（1）TLS加密通信

HTTPS使用TLS协议来加密通信数据。TLS协议使用对称加密、非对称加密和消息摘要等技术，保护数据在传输过程中的机密性、完整性和真实性。

（2）数字证书身份验证

HTTPS使用数字证书来验证Web服务器的身份。服务器在建立连接时向客户端发送其数字证书，客户端通过证书链和信任机构（CA）签名验证服务器的身份。

（3）加密密钥协商

客户端和服务器在建立连接时通过TLS协议协商加密密钥，用于对通信数据进行加密和解密。密钥协商过程通常使用Diffie-Hellman密钥交换算法或基于共享密钥的密钥交换算法。

（4）HTTPS连接过程

HTTPS连接过程包括以下几个阶段。

步骤 01 客户端和服务器首先建立TCP连接。

步骤 02 客户端向服务器发送客户端Hello消息，其中包含客户端支持的加密算法和协议版本等信息。

步骤 03 服务器向客户端发送服务器Hello消息，其中包含服务器选择的加密算法和协议版本等信息。

步骤 04 客户端和服务器使用协商好的加密算法进行密钥交换。

步骤 05 客户端和服务器使用交换的密钥建立加密通道。

步骤 06 客户端和服务器通过加密通道进行应用层数据传输。

知识拓展

HTTPS使用的加密算法

HTTPS支持多种加密算法，包括对称加密算法（如AES）、非对称加密算法（如RSA）和消息摘要算法（如SHA）。这些加密算法可以根据安全要求和性能需求进行灵活配置。

3. HTTPS 的部署和优化

部署HTTPS协议通常需要在Web服务器上安装和配置SSL/TLS证书，并进行相关的服务器配置。常见的Web服务器软件如Apache、Nginx和Microsoft IIS都支持HTTPS协议，并提供相应的

配置选项。

HTTPS协议可以与HTTP/2协议结合使用，以提高Web页面的加载速度和性能。HTTP/2协议支持多路复用、头部压缩和服务器推送等特性，与HTTPS协议配合使用可以实现更快的Web传输。

4. HTTPS 的应用

HTTPS协议被广泛应用于各种Web应用中。

- 网上银行需要传输敏感的个人信息和财务数据，因此必须使用HTTPS协议来保护数据安全。
- 网上购物需要传输信用卡信息等敏感数据，因此也必须使用HTTPS协议来保护数据安全。
- 社交网站上包含大量个人信息，因此也应该使用HTTPS协议来保护用户隐私。
- 电子邮件中可能包含敏感信息，因此也应该使用HTTPS协议来保护电子邮件安全。

4.5.2 S-HTTP协议

S-HTTP（Secure Hypertext Transfer Protocol，安全超文本传输协议）和HTTPS是20世纪90年代中期提出的两种竞争性的安全HTTP协议，它们都旨在为HTTP通信提供安全保障，但S-HTTP的设计更加灵活，支持多种加密算法和消息格式。但由于缺乏广泛的行业支持，HTTPS逐渐成为事实上的标准。

1. 工作原理

S-HTTP协议与HTTP类似，是基于请求-响应模式的协议，每个请求和响应都在单独的连接上进行，S-HTTP支持服务器端和客户端身份验证。这有助于确保用户与正确的服务器通信，并且服务器不会被恶意行为者冒充。

S-HTTP协议通过对HTTP消息进行封装和加密，实现对消息的保护。S-HTTP使用RSA公钥密码学加密客户端和服务器之间所有通信。这可以保护数据不被未经授权的第三方拦截和读取。每个HTTP消息被封装成一个安全消息，包括消息头部和消息体。S-HTTP协议使用对称密钥加密算法对消息进行加密，每个会话生成一个唯一的会话密钥，用于加密和解密消息内容。S-HTTP协议还支持数字签名技术，用于验证消息的真实性和完整性。服务器可以在响应中包含数字签名，客户端可以验证签名以确保消息的来源和完整性。

S-HTTPS支持多种安全操作模式，密钥管理机制、信任模型，密码算法和封装格式。在使用S-HTTP协议通信之前，通信双方可以协商加密、认证和签名等算法以及密钥管理机制、信任模型、消息封装格式等相关参数。在通信过程中，双方可以使用RSA、DSS等密码算法进行数字签名和身份鉴别，以保证用户身份的真实性；使用DES，3DES、RC2、RC4等密码算法来加密数据，以保证数据的保密性；使用MD2、MD5、SHA等单向散列函数来验证数据和签名，以保证数据的完整性和签名的有效性，从而增强Web应用系统中客户和服务器之间通信的安全性。

在S-HTTP客户和服务器中，主要采用CMS（Cryptographic Message Syntax）和MOSS（MIME Object Security Services）消息格式，但并不限于CMS和 MOSS，它还可以融合其他多种

加密消息格式及其标准，并且支持多种与HTTP相兼容的系统实现。S-HTTP只支持对称密码操作模式，不需要客户提供公钥证书或公钥，这意味着客户能够自主地产生个人事务，并不要求具有确定的公钥。

S-HTTP支持端到端的安全事务，客户可以事先初始化一个安全事务。S-HTTP中的密码算法模式和参数是可伸缩的，客户和服务器之间可以协商事务模式（如请求/响应是否加密和签名）、密码算法（RSA或DSA签名算法，DES或RC2加密算法）以及证书选择等。

2. 与 HTTPS 对比

S-HTTP和HTTPS都是旨在保护互联网上传输数据安全的安全通信协议。然而，两种协议之间存在一些关键差异。

- **加密：**S-HTTP使用RSA公钥密码学进行加密，而HTTPS使用TLS/SSL。TLS/SSL被认为比RSA更安全，并且得到更广泛的浏览器和服务器支持。
- **身份验证：**S-HTTP支持服务器端和客户端身份验证，而HTTPS仅支持服务器端身份验证。这意味着在某些情况下，S-HTTP可以提供更高的安全级别。
- **性能：**S-HTTP通常被认为性能不如HTTPS。这是因为RSA公钥密码学比TLS/SSL更耗费计算资源。

3. S-HTTP 的部署

S-HTTP协议的部署和配置与HTTPS类似，需要在Web服务器上安装和配置相应的安全证书，并进行相关的服务器配置和参数设置。

知识拓展

S-HTTP的劣势

尽管具有安全优势，S-HTTP最终并未获得广泛采用，原因如下。

- **复杂性：**S-HTTP比HTTPS更复杂，导致实施和部署更加困难。
- **支持不足：**与HTTPS相比，S-HTTP获得的浏览器和服务器支持更少。这使得网站难以采用S-HTTP，因为它们需要同时支持S-HTTP和HTTPS才能覆盖广泛的用户群体。
- **专利问题：**S-HTTP使用的部分关键技术受专利保护。这使得S-HTTP的实施更加昂贵和困难。

4.5.3 SSH协议

SSH（Secure Shell，安全外壳）协议是一种用于在不安全网络上进行安全连接的协议。SSH使用对称加密和非对称加密来加密数据传输，并支持服务器身份验证和数据完整性保护。SSH通常用于远程登录、文件传输和端口转发。

1. 协议原理

SSH协议通过在客户端和服务器之间建立加密的隧道来保护数据免受窃听和篡改。这个隧道使用多种加密算法来确保传输的数据保持机密性和完整性。SSH协议的工作模式可以概括为以下几个步骤。

步骤 01 客户端向服务器发送SSH客户端Hello消息，其中包含客户端支持的加密算法和协议

版本等信息。

步骤 02 服务器向客户端发送SSH服务器Hello消息，其中包含服务器选择的加密算法和协议版本等信息。

步骤 03 客户端和服务器使用协商好的加密算法进行密钥交换。

步骤 04 客户端向服务器发送认证请求，可以使用用户名/密码、公钥/私钥或其他认证方式进行认证。

步骤 05 服务器验证客户端认证信息，如果验证成功，则建立SSH安全连接。

步骤 06 客户端和服务器通过SSH安全连接进行应用层数据传输。

2. 协议安全性

SSH协议支持多种加密算法和密钥交换算法，包括对称加密算法（如AES、3DES）、非对称加密算法（如RSA、DSA）和消息摘要算法（如SHA）。这些算法可以根据安全要求和性能需求进行配置和选择。SSH使用以下几种安全机制来保障安全性。

- SSH协议提供通信数据的端到端加密保护，防止数据被窃听和篡改。
- SSH协议通过身份验证机制，确保用户身份的真实性和合法性，防止未授权的访问和入侵。
- SSH协议还支持会话加密和完整性保护，确保通信数据的完整性和可靠性。

3. 协议应用

SSH协议的部署需要在客户端和服务器端安装SSH客户端和SSH服务器软件。SSH客户端通常预装在大多数Linux和UNIX操作系统中，SSH服务器软件可以从网上下载并安装。

SSH协议被广泛应用于各种网络管理和安全场景中。

- **远程登录：**SSH协议可以用于远程登录Linux和UNIX服务器，而无须担心数据被窃取或泄露。
- **文件传输：**SSH协议可以用于安全地传输文件，例如使用SFTP协议或SCP命令。
- **端口转发：**SSH协议可以用于转发端口，例如将本地端口转发到远程服务器端口，或将远程服务器端口转发到本地端口。

4.5.4 PGP协议

PGP（Pretty Good Privacy）是一种用于电子邮件加密和数字签名的协议套件，用于数据通信加密和验证的协议，并保护电子邮件的机密性和完整性。PGP协议由Phil Zimmermann于1991年开发，旨在解决电子邮件传输中的安全和隐私问题。PGP结合了哈希、数据压缩、对称密钥加密以及公钥加密算法来保护信息的安全。

1. 工作原理

PGP协议使用多种加密算法和哈希算法，包括非对称加密算法（如RSA、DSA）、对称加密算法（如IDEA、3DES、AES）和消息摘要算法（如SHA1、SHA256）等。这些算法可以根据安全要求和性能需求进行选择和配置。发送者使用接收者的公钥对邮件进行加密，接收者使用自己的私钥解密邮件。

PGP协议使用数字签名技术对电子邮件进行签名，以确保邮件的真实性和完整性，防止邮件

被伪造和篡改。发送者使用自己的私钥对邮件进行签名，接收者使用发送者的公钥验证签名。

PGP协议使用密钥对来管理加密和签名操作，包括公钥对和私钥对。用户可以生成自己的密钥对，并将公钥发送给其他用户，以便进行加密和签名操作。

2. 部署方式

部署和配置PGP协议通常需要安装和配置PGP软件，包括PGP Desktop、GnuPG（GNU Privacy Guard）等。

3. 应用领域

PGP协议被广泛应用于各种需要保密和安全的通信场景中。

- **电子邮件通信：**PGP可以用于加密和签名电子邮件，以保护电子邮件内容的隐私性和完整性。
- **文件存储：**PGP可以用于加密文件，以保护文件内容的隐私性。
- **数字签名：**PGP可以用于对数字文件进行签名，以验证文件的来源和完整性。

知识拓展

PGP协议的优势与局限性

PGP协议使用公钥密码学技术，具有很高的安全性。PGP协议易于使用，即使是非技术用户也能轻松使用。PGP协议是开放标准，任何人都可以免费使用和实施。

但PGP协议需要用户管理自己的公钥和私钥，这对用户来说可能是一项负担。另外PGP协议的加密和解密操作可能比较耗时。

4.5.5 S/MIME协议

S/MIME（Secure/Multipurpose Internet Mail Extensions，安全多用途互联网邮件扩展）协议是一种用于在互联网上安全地发送电子邮件的协议。S/MIME基于MIME协议，并使用公钥密码学技术来加密和签名电子邮件。它提供加密、数字签名和证书管理等功能，用于保护电子邮件的机密性、完整性和真实性。

1. 工作原理

S/MIME通过在电子邮件消息中添加特殊的头部信息来实现安全功能。这些头部信息包含加密和签名的指令以及所需的密钥信息。S/MIME协议的工作原理如下。

（1）加密通信

S/MIME协议使用非对称加密算法对邮件进行加密，发送者使用接收者的公钥对邮件进行加密，接收者使用自己的私钥解密邮件。S/MIME支持多种加密算法，包括RSA、DSA、ECDSA等。

（2）数字签名

S/MIME协议使用数字签名技术对邮件进行签名，以确保邮件的真实性和完整性。发送者使用自己的私钥对邮件进行签名，接收者使用发送者的公钥验证签名。S/MIME支持多种哈希算法，包括SHA1、SHA256等。

（3）证书管理

S/MIME协议使用X.509数字证书来管理加密和签名操作，包括证书颁发、证书签名和证书验证等。用户需要获取和安装数字证书，以便进行加密和签名操作。

2. 协议步骤

S/MIME协议的工作步骤如下。

步骤 01 发件人使用自己的私钥对邮件内容进行签名，生成数字签名。

步骤 02 发件人使用收件人的公钥加密邮件内容，生成加密邮件。

步骤 03 发件人将加密邮件和数字签名发送给收件人。

步骤 04 收件人使用自己的私钥验证数字签名，以确保邮件来源和完整性。

步骤 05 收件人使用发件人的公钥解密邮件，以读取邮件内容。

3. 消息格式

S/MIME消息是MIME体和CMS对象的组合，使用了多种 MIME类型和CMS对象。被保护的数据总是一个规范化的MIME实体和其他便于对CMS对象进行处理的数据，如证书和算法标识符等，CMS对象将被嵌套封装在MIME实体中。为了适应多种特定的签名消息环境，S/MIME提供多种消息格式：一种只封装数据格式、多种只签名数据格式、多种签名加封装数据格式，多种消息格式主要是为了适应多种特定的签名消息环境。

S/MIME是用来保护MIME实体的。一个MIME实体由MIME头和MIME体两部分组成，被保护MIME实体可以是“内部”MIME实体，即一个大的MIME消息中“最里面”的对象；还可以是“外部”MIME实体，把整个MIME实体处理成CMS对象。

在发送端，发送代理首先按照本地保护协议创建一个MIME实体，保护方式可以是签名、封装或签名加封装等；然后对MIME实体进行规范化处理和转移编码，构成一个规范化的S/MIME消息；最后发送该S/MIME消息。

在接收端，接收代理接收到一个S/MIME消息后，首先将该消息中的安全服务处理成一个MIME实体，然后解码并展现给用户或应用。

4. 密码算法

S/MIME密码算法包括消息摘要算法、数字签名算法以及密钥交换算法。

（1）消息摘要算法

S/MIME V3支持两种消息摘要算法：SHA和MD5，通过对消息摘要的哈希和认证来保证消息的完整性。提供 MD5算法的目的是保持与S/MIME V2的向后兼容性，因为S/MIME V2的消息摘要是基于MD5算法的。

（2）数字签名算法

S/MIME V3支持两种数字签名算法：RSA 和DSA，通过对外出消息的数字签名来实现对消息源的抗抵赖性。对于外出的消息，将使用发送用户的私钥来签名，其私钥长度是在生成密钥时确定的。对于S/MIME V2，只支持基于RSA的数字签名算法。

（3）密钥交换算法

S/MIME V3在加密消息内容时采用了对称密码算法，如DES、3DES等，密钥必须经过加

密后才能传送给对方。S/MIME V3支持两种密钥交换算法：Diffie-Hellman和RSA。使用RSA算法时，在进入的加密消息中包含了加密密钥，必须使用接收用户的私钥来解密。对于S/MIME V2，只支持基于RSA 的密钥交换算法。

4.6 知识延伸：OSI安全管理

OSI安全管理活动有三类：系统安全管理、安全服务管理和安全机制管理。

1. 系统安全管理

系统安全管理主要针对OSI的总体环境管理，具体活动包括以下几点。

① 总体安全策略的管理，包括一致性修改与维护。

② 与别的OSI安全管理的相互作用。

③ 与安全服务管理和安全机制管理的交互。

④ 事件处理管理。在OSI中可以看到的是事件管理的实例，是远程报告的明显违反安全的企图，以及对用来触发事件报告的阈值的修改。

⑤ 安全审计管理，包括选择将被记录和被远程收集的事件、授予或取消对所选事件进行审计跟踪日志记录的能力、所选审计记录的收集、准备安全审计报告。

⑥ 安全恢复管理，包括维护用于对现有的或可疑的安全事件做出反应的规则、远程报告明显的系统安全违规、安全管理者的交互。

2. 安全服务管理

安全服务管理指特定安全服务的管理。在管理一种特定安全服务时，典型的活动如下。

- 为该种服务决定并指派安全保护的目标。
- 在可以选择的情况时，指定与维护选择规则。
- 对需要事先取得管理者同意的安全机制进行协商。
- 通过适当的安全机制管理功能，调用特定的安全机制。
- 与其他安全服务管理功能和安全机制管理功能交互。

3. 安全机制管理

安全机制管理指特定安全机制的管理。典型的安全机制管理如下。

（1）密钥管理

- 间歇性地产生与所要求的安全级别相称的合适密钥。
- 根据访问控制的要求，决定每个密钥应分发给哪个实体。
- 用可靠办法使这些密钥对开放系统中的实体是可用的，或将这些密钥分配给它们。

（2）加密管理

- 与密钥管理交互。
- 建立密码参数。
- 密码同步。

（3）数字签名管理

- 与密钥管理交互。
- 建立密码参数与密码算法。
- 在通信实体与可能有的第三方之间使用协议。

（4）访问控制管理

- 安全属性（包括口令）的分配。
- 对访问控制表或权力表进行修改。
- 在通信实体与其他提供访问控制服务的实体之间使用协议。

（5）数据完整性管理

- 与密钥管理交互。
- 建立密码参数与密码算法。
- 在通信实体间使用协议。

（6）鉴别管理

- 将说明信息、口令或密钥（使用密钥管理）分配给要求执行鉴别的实体。
- 在通信的实体与其他提供鉴别服务的实体之间使用协议。

（7）通信业务填充管理

- 指定数据率。
- 指定随机数据率。
- 指定报文特性，例如长度等。
- 可能按时间或日历改变这些规定。

（8）路由选择控制管理

主要功能是确定那些按特定准则被认为是安全可靠和可信任的链路或子网络。

（9）公证管理

- 分配有关公证的信息。
- 在公证方与通信的实体之间使用协议。
- 与公证方的交互作用。

4. OSI 管理的安全

所有OSI管理功能的安全以及OSI管理信息的通信安全是OSI安全的重要部分。这一类安全管理将对上面所列的OSI安全服务与机制进行适当的选取，以确保OSI管理协议与信息获得足够的保护。例如，在管理信息库的管理实体之间的通信一般要求某种形式的保护。