第 1 篇
网络安全技术基础

第1章

网络安全概述

随着网络技术的普及，网络的安全性显得更加重要。这是因为怀有恶意的攻击者会窃取、篡改网络上的传输信息，通过网络非法入侵获取存储在远程主机上的机密信息，或者构造大量的数据报文占用网络资源，以阻止其他合法用户的正常使用等。然而，网络作为开放的信息系统必然存在诸多潜在的安全隐患，因此，网络安全技术作为一个独特的领域越来越受到人们的关注。

随着全球信息高速公路的建设和发展，个人、企业乃至整个社会对信息技术的依赖程度越来越高。一旦网络系统的安全性受到严重威胁，不仅会对个人、企业造成不可避免的损失，而且，严重时甚至会给企业、社会乃至整个国家带来巨大的经济损失。因此，提高对网络安全重要性的认识、增强防范意识、强化防范措施，不仅是各个企业、组织要重视的问题，也是保证信息产业持续稳定发展的重要保证和前提条件。

本章将帮助读者建立相对完整的网络安全理论观念、了解网络安全需求与攻击威胁，即安全技术要解决的问题，以及理解目前网络安全技术的基本架构和具体技术分类。

1.1 本章目标

学习完本章，应该能够达成以下目标。

(1) 了解 OSI 参考模型。

(2) 理解 TCP/IP 协议原理。

(3) 理解 TCP/IP 协议存在的安全隐患。

(4) 理解针对 TCP/IP 协议栈各层常见攻击的技术原理。

1.2 什么是网络安全

从本质上来讲，网络安全就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。从广义上来讲，凡是涉及网络信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。技术方面主要侧重于如何防范外部非法攻击，管理方面则侧重于内部人为因素的管理。如何更有效地保护重要的信息数据、提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和必须解决的一个重要问题。本书主要基于技术的维度为学员介绍网络安全技术的基础知识。

要掌握网络安全技术首先必须对网络有一个基本的认识。下面首先介绍网络的一些基础概念,以及目前网络面临的一些安全问题。

1.3 OSI 参考模型

1.3.1 OSI 参考模型产生背景

如今,人们可以方便地使用不同厂家的设备构建计算机网络,而不需要过多考虑不同产品之间的兼容性问题。而在 OSI 参考模型出现(20 世纪 80 年代)之前,实现不同设备间的互通并不容易。这是因为在计算机网络发展的初期,许多研究机构、计算机厂商和公司都推出了自己的网络系统,如 IBM 公司的 SNA 协议、NOVELL 公司的 IPX/SPX 协议、APPLE 公司的 AppleTalk 协议,DEC 公司的 DECnet 协议,以及广泛流行的 TCP/IP 协议等。同时,各大计算机厂商针对自己的协议生产出了不同的硬件和软件。然而,这些协议和设备之间互不兼容。没有一种统一标准存在,就意味着,这些不同厂家的网络系统之间无法相互连接。

为了解决网络兼容性的问题、帮助各个厂商生产出可兼容的网络设备,国际标准化组织(International Organization for Standardization,ISO)于 1984 年提出了开放系统互联参考模型(open system interconnection reference model,OSI 参考模型)。该参考模型很快成为计算机网络通信的基础模型。

OSI 参考模型的设计目的在于构建一个所有销售商都能实现的开放网络模型,用以克服使用众多专网模型所带来的困难和低效性。它是网络技术的基础,也是分析、评判各种网络技术的依据;它揭开了网络的神秘面纱,让其有理可依、有据可循。

OSI 参考模型很重要的一个特性是其分层体系结构。分层设计的方法可以将庞大而复杂的问题转化为若干较小且易于处理的子问题。它将复杂的网络通信过程分解到各个功能层,各个功能层的设计和测试相对独立,并不依赖于操作系统或其他因素。并且,各个功能层之间也无须了解彼此的实现方法。

OSI 参考模型在设计时遵循了以下原则。

(1) 各个功能层之间有清晰的边界,便于理解。

(2) 每个功能层实现特定的功能,且不相互影响。

(3) 每个功能层是服务者又是被服务者,即其既为上一层服务,又被下一层服务。

(4) 功能层的划分有利于国际标准协议的制订。

(5) 功能层的数目需足够多,以避免各层功能重复。

OSI 参考模型具有以下优点。

(1) 提供设备间的兼容性和标准接口,使各个厂商能够设计出互操作的网络设备,促进了标准化工作,加快了数据通信网络的发展。

(2) 采用分层体系结构,各个功能层可以根据需要,独立进行修改或扩充功能。分层设计方法也可以将庞大而复杂的问题转化为若干较小且易于处理的子问题,有利于大家学习、理解数据通信网络。

1.3.2 OSI 参考模型层次结构

如图 1-1 所示,OSI 参考模型层次结构共分为七层,即 OSI 七层模型,这七个对等功能层数据统称为协议数据单元(protocol data unit,PDU)。

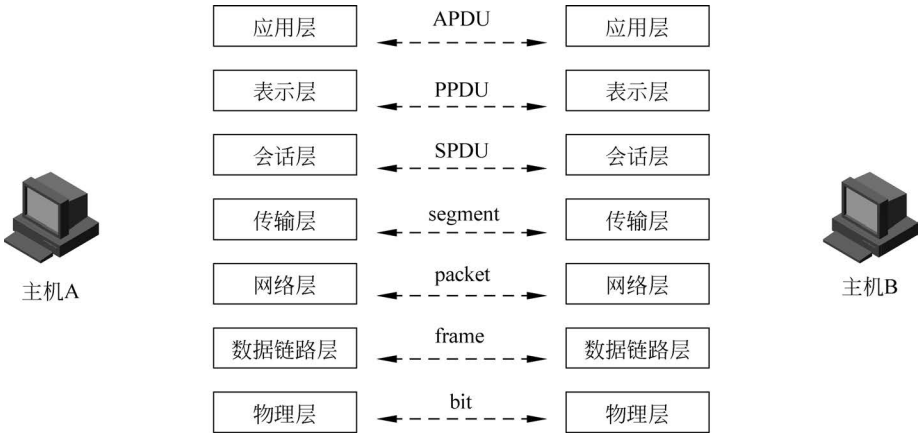


图 1-1　OSI 七层模型

1. 物理层

物理层为上层提供物理连接，实现比特流的透明传输，其数据称为比特流(bit)。

物理层并不是物理媒体本身，而是开放系统中利用物理媒体实现物理连接的功能描述和执行连接的规则。物理层所涉及的在通信信道(channel)上传输的原始比特流，是 OSI 参考模型的基础，它可实现传输数据所需要的机械、电气功能特性。它不关心单个比特流(0,1)所代表的含义，如代表地址还是应用数据，而只关注如何把比特流通过不同的物理链路传输至对端。典型的如中继器、集线器(hub)就属于物理层设备。

2. 数据链路层

数据链路层提供可靠的通过物理介质传输数据的方法，其数据称为帧(frame)。

两台终端设备之间进行通信，连接生存期内，收发两端可以进行一次或多次数据通信，每次通信都要经过建立通信联络和拆除通信联络两个过程。这种建立起来的数据收发关系称为数据链路。但是，物理媒体上传输的数据难免受到各种不可控因素的影响而产生差错，为了弥补物理层上的不足，为上层提供无差错的数据传输，就需要对数据进行检错和纠错。数据链路的建立、拆除，对数据的检错、纠错是数据链路层的基本任务。

3. 网络层

网络层寻址和路由选择，其数据称为数据包(packet)。

网络层规定了网络连接的建立和拆除规程，以及数据传输规程等，为上层提供服务。它具备以下主要功能：路由选择和中继；激活、终止网络连接；在一条数据链路上复用多条网络连接；检测与恢复；排序、流量控制；服务选择；网络管理。

网络层检查网络拓扑结构，以决定传输报文的最佳路由，转发数据包。其关键问题是确定数据包从源端到目的端如何选择路由。网络层设备通过运行路由协议(routing protocol)来计算到目的地的最佳路由，找到数据包应该转发的下一个网络设备，然后利用网络层协议封装数据包，利用传输层提供的服务把数据发送到下一个网络设备。

4. 传输层

传输层提供端到端报文的正确传输，其数据称为段(segment)。

传输层位于 OSI 参考模型的第 4 层，是端开放系统之间的数据传送控制层，主要功能是端开放系统之间数据的收妥确认。同时，还用于弥补各种通信网络的质量差异，对经过下三层

之后仍然存在的传输差错进行恢复，进一步提高数据可靠性。另外，还通过复用、分段和组合、连接和分离、分流和合流等技术措施，提高数据吞吐量和服务质量。

5. 会话层

会话层建立、维护和管理会话，其数据称为会话层协议数据单元（session protocol data unit，SPDU）。

在会话层及以上的高层次中，数据传输的单位不再另外命名，而是统称报文。会话层是会话单位的控制层，其主要功能是按照在应用进程之间约定的原则，按照正确的顺序收、发数据，进行各种形态的对话。会话层规定了会话服务用户间会话连接的建立和拆除规程，以及数据传输规程。

6. 表示层

表示层处理编码、数据格式转换和加密解密等，其数据称为表示层协议数据单元（presentation protocol data unit，PPDU）。

表示层是数据表示形式的控制层，其主要功能是把应用层提供的信息转换为能够共同理解的形式，提供字符代码、数据格式、控制信息格式、加密等的统一表示。它将需要转换的数据从适合某一用户的抽象语法，转换为适合 OSI 参考模型系统内部使用的传输语法，为异种机通信提供了一种公共语言，即提供格式化的表示和转换数据服务。数据的压缩和解压缩、加密和解密等工作都由表示层负责。

7. 应用层

应用层提供应用程序间的通信，其数据称为应用层协议数据单元（application protocol data unit，APDU）。

应用层是 OSI 参考模型的最高层，是直接为应用进程提供服务的。其作用是在实现多个系统应用进程相互通信的同时，完成一系列业务处理所需的服务。应用层直接和应用程序接口，并提供常见的网络应用服务。此外，应用层也向表示层发出请求。

1.3.3 数据封装与解封装

封装（encapsulation）是指网络节点将要传输的数据用特定的协议打包后传输。多数协议通过在原有数据之前加上封装头（header）来实现封装，另外，一些协议还要在数据之后加上封装尾（trailer），而原有数据此时便成为载荷（payload）。在发送方，OSI 七层模型的每一层都对上层数据进行封装，以保证数据能够正确无误地到达目的地；而在接收方，OSI 七层模型的每一层又对本层的封装数据进行解封装，并传送给上层，以便数据被上层所理解。

图 1-2 所示为 OSI 参考模型中数据的封装与解封装过程。首先，源主机的应用程序生成能够被对端应用程序识别的应用层数据；然后，数据在表示层加上表示层头，协商数据格式、是否加密，并转换成对端能够理解的数据格式；之后，数据在会话层又加上会话层头；以此类推，传输层加上传输层头形成段，网络层加上网络层头形成包，数据链路层加上数据链路层头形成帧；在物理层数据转换为比特流，传送到网络上。比特流到达目的主机后，也会被逐层解封装。首先，由比特流获得帧；然后，剥去数据链路层帧头获得包；之后，剥去网络层包头获得段；以此类推，最终，获得应用层数据提交给应用程序。

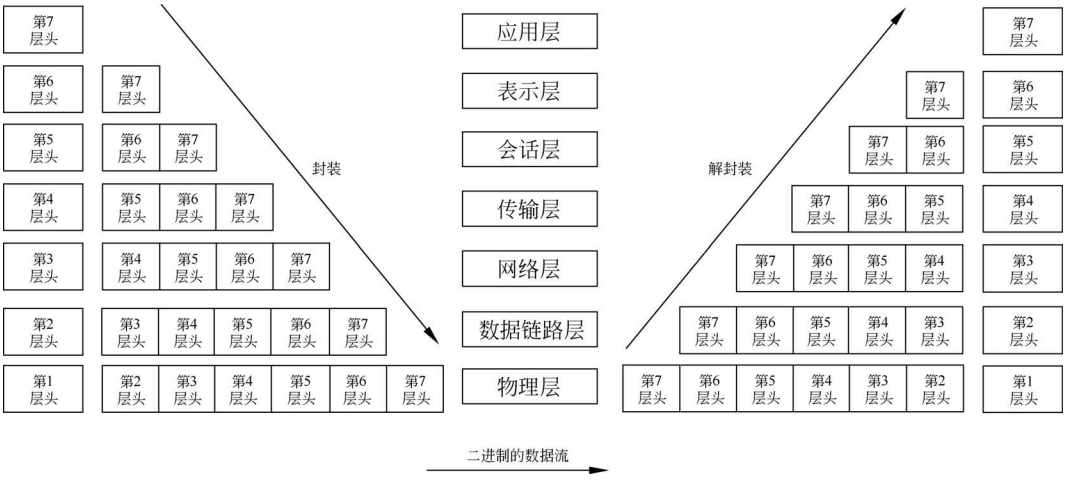


图 1-2　OSI 参考模型中数据的封装与解封装过程

1.4　TCP/IP 参考模型

1.4.1　TCP/IP 参考模型概述

OSI 参考模型的诞生为清晰地理解互联网、开发网络产品和网络设计等带来了极大的方便。但是，由于 OSI 参考模型过于复杂，难以完全实现，并且，其各层功能具有一定的重复性，效率较低，再加上，在 OSI 参考模型提出时，TCP/IP 协议已逐渐占据主导地位，因此，OSI 参考模型并没有得到广泛应用，且从未生成过完全遵守 OSI 参考模型的协议族。

TCP/IP 协议起源于 20 世纪 60 年代末期美国政府资助的一个分组交换网络研究项目，到 20 世纪 90 年代已发展成为计算机之间最常用的网络协议。这个体系结构在它的两个主要协议出现以后称为 TCP/IP 参考模型(TCP/IP reference model)。TCP/IP 参考模型具有良好的开放性和易用性，在实践中得到广泛应用，从而使 TCP/IP 协议栈成为 Internet 事实上的标准协议。

如图 1-3 所示，TCP/IP 参考模型与 OSI 参考模型的不同点在于 TCP/IP 参考模型把表示层和会话层都归入应用层，把数据链路层和物理层都归入网络接入层，所以，TCP/IP 参考模型从下至上分为网络接入层、网络层、传输层和应用层 4 层。

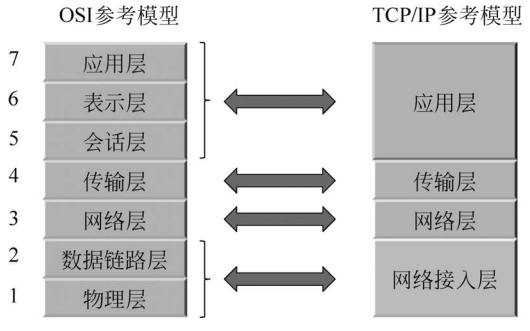


图 1-3　TCP/IP 参考模型层次结构

如图 1-4 所示，TCP/IP 参考模型每一层都有对应的相关协议，且均为达成某一网络功能而设计。

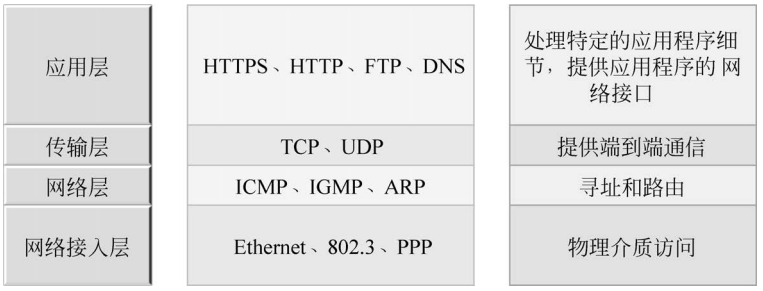


图 1-4 TCP/IP 参考模型协议栈各层作用

TCP/IP 参考模型没有单独的会话层和表示层，其功能融合在应用层中。应用层直接与用户和应用程序对接，负责对软件提供接口以使程序能使用网络服务。这里的网络服务包括文件传输、文件管理、电子邮件的消息处理等。典型的应用层协议包括 Telnet、FTP、SMTP、SNMP 等。

(1) 超文本传输协议(hypertext transfer protocol，HTTP)：用来访问在 Web 服务器上的各种页面。

(2) 文件传输协议(file transfer protocol，FTP)：为文件传输提供途径，它允许数据从一台主机传输到另一台主机上。

(3) 域名服务系统(domain name system，DNS)：用于实现从主机域名到 IP 地址之间的转换。

TCP/IP 参考模型的传输层位于应用层和网络层之间，主要负责为两台主机的应用程序提供端到端的通信，使源、目的端主机上的对等实体可以进行会话。TCP/IP 参考模型的传输层协议主要包括传输控制协议(transmission control protocol，TCP)和用户数据报协议(user datagram protocol，UDP)。

(1) TCP：为应用程序提供可靠的、面向连接的通信服务，适用于要求得到响应的应用程序。目前，许多流行的应用程序均使用 TCP。

(2) UDP：提供了无连接通信，且不对传送数据包进行可靠的保证。适合一次传输少量数据，可靠性则由应用层来负责。

网络层是 TCP/IP 参考模型的关键部分，其主要功能是使主机能够将信息发往任何网络，并传送到正确目标。基于这些要求，网络层定义了包格式及其协议——互联网协议(internet protocol，IP)。网络层使用 IP 地址(IP address)标识网络节点；使用路由协议生成路由信息，并且，根据这些路由信息实现包的转发，使包能够准确地传输到目的地；使用互联网控制消息协议(internet control message protocol，ICMP)、互联网组管理协议(internet group management protocol，IGMP)这样的协议协助管理网络。TCP/IP 参考模型网络层在功能上与 OSI 参考模型网络层极为相似。

(1) IP：IP 和路由协议协同工作，寻找能够将数据包传输到目的端的最优路径。IP 不关心数据报文的内容，只提供无连接的、不可靠的服务。

(2) 地址解析协议(address resolution protocol，ARP)：把已知的 IP 地址解析为媒体访问控制地址(media access control address，MAC 地址)。

(3) ICMP：定义了网络层控制和传递消息的功能。

(4) IGMP：用于组播组成员管理。

对于网络接入层，TCP/IP 参考模型本身对网络层之下并没有严格的描述。但是，TCP/IP 参考模型主机必须使用某种下层协议连接到网络，以便进行通信。而且，TCP/IP 参考模型必须能运行在多种下层协议上，以便实现端到端、与链路无关的网络通信。TCP/IP 参考模型的网络接入层负责处理与传输介质相关的细节，为上层提供一致的网络接口。因此，TCP/IP 参考模型的网络接入层大体对应于 OSI 参考模型的数据链路层和物理层，通常包括计算机和网络设备的接口驱动程序和网络接口卡等。

TCP/IP 参考模型可以基于大部分局域网或广域网技术运行，这些协议便可以划分到网络接入层中。工作在网络接入层中的协议主要有逻辑链路控制子层(logic link control sublayer，LLC)、介质访问控制子层(media access control sublayer，MAC)。

1.4.2　IP 介绍

网络层处理数据分组在网络中的活动，如分组的路由选择。在 TCP/IP 参考模型中，网络层包括 IP、ICMP 和 IGMP。

IP 报文格式如图 1-5 所示。

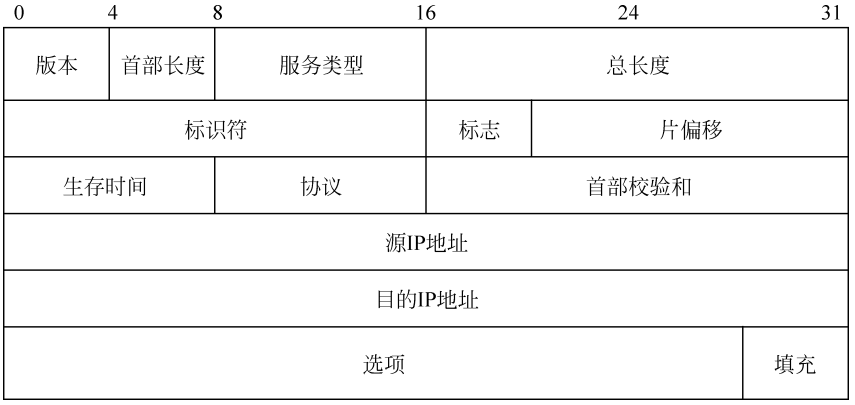


图 1-5　IP 报文格式

(1) 版本(version)：占 4b，标识 IP 封包的版本，目前使用的版本是 IPv4。

(2) 首部长度(header length)：占 4b，描述 IP 包头的长度，单位为字节(byte)。

(3) 服务类型(type of service)：占 8b，前三位定义包的优先级，后五位分别表示为时延(D)、吞吐量(T)、可靠性(R)、传输成本(M)和保留位(0)。

(4) 总长度(total length)：占 16b，以字节为单位计算的 IP 包的长度(包括头部和数据)，IP 包最大长度 65535B。

(5) 标识符(identifier)：占 16b，该字段和 flags、fragment offset 字段联合使用，对较大的上层数据报文进行分段(fragment)操作。

(6) 标志(flags)：占 3b，第 1 位不使用，第 2 位是 DF(don't fragment)位，1 表示不能对数据包分段，0 表示可分段，第 3 位是 MF(more fragments)位，1 表示后面还有分段，0 表示该数据包为最后 1 个分段数据包。

(7) 片偏移(fragment offset)：占 13b，表示该 IP 包在该组分片包中位置。

(8) 生存时间(TTL)：占 8b,数据包每经过一个路由器会将 IP 包的 TTL 值减少 1。

(9) 协议(protocol)：占 8b,标识了上层所使用的协议。和端口号类似,IP 用协议号区分上层协议；TCP 的协议号为 6；UDP 的协议号为 17。

(10) 首部校验和(head checksum)：计算 IP 头部的校验和,检查报文头部的完整性。

(11) 源 IP 地址和目的 IP 地址：标识数据包的源端设备和目的端设备。

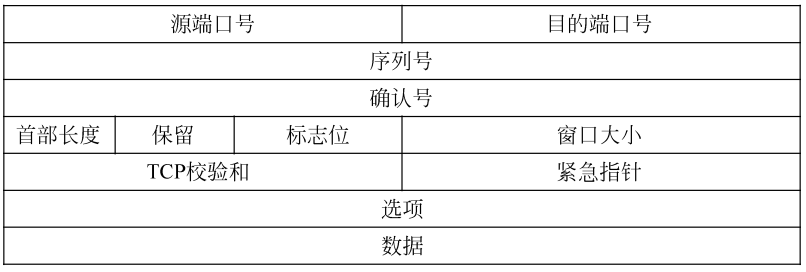
(12) 选项(option)：这是一个可变长度的字段。

(13) 填充(padding)：因为 IP 包头长度部分的单位为 32b,所以 IP 包头的长度必须为 32b 的整数倍。因此,在选项后面,IP 会填充若干个 0,以达到 32b 的整数倍。

1.4.3 TCP 介绍

如图 1-6 所示,在 TCP/IP 参考模型中,有两个不同的传输协议：TCP 和 UDP。UDP 报文与 TCP 报文的格式有所不同,TCP 明显比 UDP 长度更长、字段更多,因此,TCP 也相应有更多的功能,如可靠性等。

• UDP报文格式



• TCP报文格式

图 1-6 传输层协议报文格式

TCP 报文格式如下。

(1) 源端口号(source port)和目的端口号(destination port)：用于标识和区分源端设备和目的端设备的应用进程。

(2) 序列号(sequence number)：即发送序号。发送主机端会在 TCP 报文封装时,确定一个初始号码,后续报文序号会依次递增,接收端可以根据此序号来检测报文是否接收完整。

(3) 确认号(acknowledgement number)：即回应序号。接收端接收到的 TCP 报文通过检验确认之后,会根据发送序号产生一个回应序号,发送端根据此序号确定报文被成功接收。

(4) 首部长度：包头固定长度。如果 option 没设定,则其长度为 20B。

(5) 保留(reserved)：这是保留区间,暂时还没被使用。

(6) 标志位(U、A、P、R、S、F)：

① URG 为 1,表示紧急报文。

② ACK 为 1,表示需要回应的报文。

③ PSH 为 1,表示此报文所携带的数据会直接上传给上层应用程序而无须经过 TCP