网络技术系列丛书、
普通高等教育“十三五”应用型人才培养规划教材

计算机网络安全

李芳　唐磊　张智◎主编

西南交通大学出版社

网络技术系列丛书
普通高等教育“十三五”应用型人才培养规划教材

计算机网络安全

主　编　李　芳　唐　磊　张　智
副主编　梁雪梅　张文科　罗　勇
参　编　程书红　姜继勤　杨　超

西南交通大学出版社
·成　都·

图书在版编目（CIP）数据

计算机网络安全 / 李芳，唐磊，张智主编. —成都：
西南交通大学出版社，2017.10
网络技术系列丛书　普通高等教育“十三五”应用型
人才培养规划教材
ISBN 978-7-5643-5838-9

Ⅰ. ①计… Ⅱ. ①李… ②唐… ③张… Ⅲ. ①计算机
网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2017）第 259434 号

网络技术系列丛书
普通高等教育“十三五”应用型人才培养规划教材

计算机网络安全

主　编／李　芳　唐　磊　张　智

责任编辑／李芳芳
助理编辑／王小龙
封面设计／严春艳

西南交通大学出版社出版发行
（四川省成都市二环路北一段 111 号西南交通大学创新大厦 21 楼　610031）
发行部电话：028-87600564　　028-87600533
网址：http://www.xnjdcbs.com
印刷：成都中铁二局永经堂印务有限责任公司

成品尺寸　185 mm × 260 mm
印张　20.5　　字数　538 千
版次　2017 年 10 月第 1 版　　印次　2017 年 10 月第 1 次

书号　ISBN 978-7-5643-5838-9
定价　49.50 元

课件咨询电话：028-87600533
图书如有印装质量问题　本社负责退换

前　言

目前，计算机网络安全问题是大家比较关注的话题之一，当然也是学者研究的一个重要课题。计算机网络安全是一门涉及计算机科学、网络技术、通信技术、密码学技术、信息安全技术等多种学科的综合性学科。计算机网络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，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续可靠正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及到网络上信息的保密性、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。

影响计算机网络安全的因素很多，除了信息的不安全性以外，层出不穷的电脑病毒也给网络安全带来了威胁。另外，黑客对于网络安全的威胁则日趋严重。网络所面临的威胁很多，其中包括：物理威胁（偷窃、废物搜寻、间谍行为、身份识别错误）、系统漏洞（乘虚而入、不安全服务、配置和初始化）、身份鉴别威胁（口令圈套、口令破解、算法考虑不周、编辑口令）、线缆连接威胁（窃听、拨号进入、冒名顶替）、有害程序（病毒、代码炸弹、特洛伊木马）。

当然，计算机网络安全涉及的不仅是技术问题，也跟社会和法律相关。要解决信息网络的安全问题，必须采取技术和立法等多种手段进行综合治理。

本书作为高职高专教材，在编写时采用通俗易懂的语言，围绕计算机网络所涉及的安全问题，讲述了各种相关的安全技术，各章内容如下：

第 1 章介绍了计算机网络基础，包括计算机网络的简介、网络的体系结构、和网络协议等。

第 2 章介绍了网络安全概述，包括黑客文化、网络安全简介、网络安全面临的威胁及体系结构等。

第 3 章介绍了物理安全技术，包括物理安全概述、环境安全、电源系统安全、设备安全等。

第 4 章介绍了网络攻防技术，包括网络安全的威胁、黑客信息获取的手段、常见的攻击方法等。

第 5 章介绍了密码学技术，包括密码学概述、古典密码学、对称秘钥密码体制和公钥密码体制等。

第 6 章介绍了数字身份认证，包括消息认证、数字签名、身份认证、数字证书等。

第 7 章介绍了防火墙技术，包括防火墙概述、防火墙体系结构、防火墙技术及防火墙配置实例等。

第 8 章介绍了病毒防治技术，包括病毒的基本知识、木马技术、网络病毒及反病毒技术等。

第 9 章介绍了入侵检测技术，包括入侵检测技术的概念、技术及性能等。

第 10 章介绍了虚拟专网技术，包括虚拟专网的概念、分类及安全等。

第 11 章介绍了操作系统的安全，包括操作系统概述、windows 系统的安全、Unix 系统的安全等。

第 12 章介绍了无线网络的安全，包括无线网络的协议标准、体系架构以及无线网络的攻击手段和防护技术等。

第 13 章介绍了网络设备的安全，包括交换机、路由器设备的安全技术等。

本书具体编写分工为第 1 章由重庆三峡职业学院唐磊编写；第 2 章、第 5 章、第 6 章、第 7 章、第 8 章、第 10 章、第 11 章和第 12 章由重庆城市管理职业学院教师李芳编写；第 3 章、第 9 章由重庆城市管理职业学院教师罗勇和海南职业技术学院教师张智编写；第 4 章由重庆城市管理职业学院教师李芳和重庆电子工程职业学院教师梁雪梅编写；第 13 章由重庆城市管理职业学院教师张文科和李芳编写。此外重庆城市管理职业学院老师姜继勤、程书红，重庆皓大通信技术有限公司的工程师杨超也参与了本书的编写工作，本书由李芳统稿。

本书在编写过程中得到了高等职业学校提升专业服务产业发展能力项目软件技术专业项目组的大力支持，同时参考了大量书籍和网站，在此对软件项目组、本书的编著者及网站的作者表示衷心的感谢。

由于编者水平有限，书中错误和疏漏之处在所难免，望各位专家和读者批评指正。

编　者

2017 年 6 月 10 日

目 录

1　计算机网络基础

【引导案例】

2001 年 9 月 11 日，美国遭到恐怖分子袭击，当电话、电报等传统通信系统几乎都被摧毁时，电子邮件使人们与远方的亲人仍可互通信息。可以说，在这次袭击中，当人类的许多现代文明都面临危险时，只有计算机网络以最顽强的生命力担负起了为人类信息交流的使命。根据 2012 年 12 月中国互联网络信息中心发布的第 31 次中国互联网网络发展状况统计报告，我国网民总人数大约为 56 400 万人，人均每周上网时长达 20.5 小时，互联网普及率 42.1%。

计算机网络已经成为人们获取信息的一个重要渠道。计算机网络给大家的工作、学习和生活带来了革命性变化。随着各种网络应用的发展，人们的工作效率得以提高；随着远程教育的发展，人们的学习变得更加方便，终生教育成为可能；随着网络游戏、虚拟社区等新兴应用的发展，人们的生活增加了许多乐趣。计算机网络推动了整个人类社会文明的发展。

1.1　计算机网络概述

1.1.1　计算机网络概念

1. 计算机网络定义

计算机网络就是为了实现信息共享而利用通信线路连接起来的两台或多台相互独立计算机的集合。这并不是最权威的定义，只是计算机网络定义中的一种。随着网络技术的发展以及网络应用范围的扩展，计算机网络的概念也在发展。不同的书中对计算机网络的定义也各不相同。关键不是记住计算机网络的定义，而是通过对概念的正确理解把握它的内涵，而理解计算机网络需要把握以下两点：

（1）组成计算机网络的计算机要求是独立的。每台计算机核心的基本部件，如处理器、系统总线等要求存在并且是独立的。有的计算机系统不满足这一要求，在 1980 年前后，许多图书馆采用了图书查询系统，采用一台小型机带几十台查询终端的体系结构，如图 1.1 所示。这种系统不是计算机网络，因为整个系统中除了有一台主机具有处理器外，其他的终端都只有输入/输出设备，而不是完整、独立的计算机，所以该系统属于具有一台主机的计算机系统，而不是计算机网络。

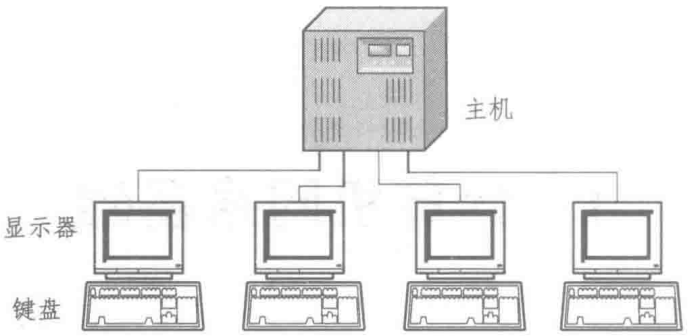

图 1.1 图书查询系统

（2）计算机网络通信的目的是实现信息共享。有的计算机系统数据通信的目的不是为了实现信息共享，而是为了实现分布式处理等，这种计算机系统也不是计算机网络。如在多处理机系统中，在各个处理器之间虽然也存在数据通信，但数据通信的目的是为了实现多个处理器协同处理一个更大的任务，保证每个处理器都能完成自己的一部分任务而不至于发生调度混乱。因此，一个多处理机系统，如双 CPU 的计算机系统不是计算机网络。在科学计算、天气预报等领域广泛应用的多处理机系统可以看做是处理能力很强的计算机，而不是计算机网络。判断计算机系统是不是计算机网络的一个必要标准，就是系统是否以实现信息共享作为数据通信的目的。当然，并不是说所有分布式处理的系统都不是计算机网络，一个计算机网络也可以实现分布式处理，如有的网络操作系统（Windows Server 2003、Linux 等）支持集群的功能，可以实现在网络环境中的多台计算机之间的负载平衡，具有分布式处理的能力。因此对于一个系统是否属于计算机网络，可从以上两个方面加以分析。

2. 计算机网络的服务

为什么要把多台计算机连成一个计算机网络呢？换句话说，计算机网络主要为用户提供了哪些服务？这个问题的答案可以概括为以下四个方面：

（1）资源共享。资源包括硬件、软件和数据。硬件为处理器、存储设备和输入/输出设备等，可以通过计算机网络实现这些硬件的共享，如打印机、硬盘空间等。软件包括操作系统、应用软件和驱动程序等，可以通过计算机网络实现这些软件的共享，如多用户的网络操作系统、应用程序服务器等。在后面的章节中会介绍利用 Windows Server 2003 的远程桌面服务进行应用程序的共享，在一台服务器上安装的应用程序可以在其他的计算机上直接使用。数据包括用户文件、配置文件和数据文件等，可以通过计算机网络实现这些数据的共享，如通过网络邻居复制文件、网络数据库等。通过资源共享可使资源发挥最大作用，同时节省成本、提高效率。

（2）数据传输。这里的数据指的是数字、文字、声音、图像、视频信号等媒体所存储信息的计算机表示。在计算机世界里，一切事物都可以用 0 和 1 这两个数字表示出来。计算机网络使得各种媒体信息通过一条通信线路从甲地传送到乙地。数据传输是计算机网络各种功能的基础，有了数据传输，才会有资源共享，才会有其他的功能。

（3）协调负载。在有多台计算机的环境中，这些计算机需要处理的任务可能不同，经常有忙闲不均的现象。有了计算机网络，可以通过网络调度来协调工作，把“忙”的计算机上的部分工作交给“闲”的计算机去做，还可以把庞大的科学计算或信息处理题目交给几台联网的计算机协调配合来完成。分布式信息处理、分布式数据库等只有依靠计算机网络才能实现协调负

载，提高效率。在有些科研领域，只有借助计算机网络的协调负载才能使一些计算处理任务的繁重工作得以完成。

（4）提供服务。有了计算机网络，才有了现在风靡全球的电子邮件、网络电话、网络会议、电子商务等，它们给人们的生活、学习和娱乐带来了极大方便。有了网络，使得实时控制系统有了备用和安全保证，使得军事设施在遭到敌方打击时指挥系统保持畅通无阻。最大的计算机网络——因特网就是冷战时期的产物，用它能够解决可靠性问题，并为计算机用户带来极大便利。随着网络新技术层出不穷，不断有新的服务使人们从中受益。

以上介绍的是计算机网络的一般功能，只是一个描述性的介绍，所有计算机网络的功能都会是以上四种功能中的一种或几种。具体的计算机网络可能各有不同的功能，如有的网络能够实现打印机共享，有的网络可以实现电子邮件服务等。

3. 计算机网络的组成

一般而论，计算机网络结构包括三部分：若干个主机，它们为用户提供服务；一个通信子网，它主要由结点交换机和连接这些结点的通信链路所组成；一系列的协议，这些协议是为在主机和主机之间或主机和子网中各结点之间的通信而采用的，它是通信双方事先约定好的和必须遵守的规则。为了便于分析，按照数据通信和数据处理的功能，一般从逻辑上将网络分为通信子网和资源子网两个部分。典型的计算机网络结构如图 1.2 所示。

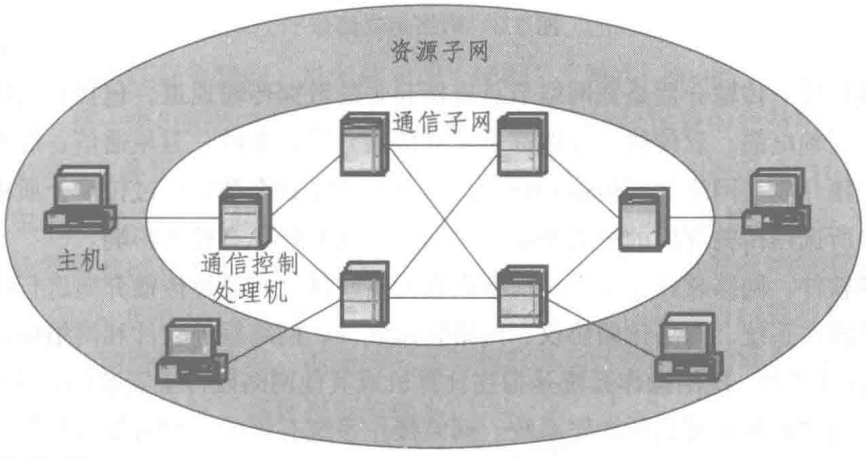

图 1.2　典型计算机网络结构

尽管现在的计算机网络很多，但不同的计算机网络都有一个共同的特点，那就是它们都由三部分组成，即网络硬件、传输介质和网络软件，如图 1.3 所示。

（1）网络硬件。网络硬件是构成网络的节点，包括计算机和网络互联设备。作为网络硬件的计算机可以是服务器，也可以是工作站。网络互联设备包括集线器、交换机和路由器等。有的网络硬件（如计算机）只有一个网络接口；有的网络硬件（如各种网络互联设备）可能有几个、几十个甚至更多的网络接口，如集线器、交换机和大多数路由器等。路由器这种特殊的网络互联设备，在网络中可以有一个网络接口，也可以有多个网络接口用以连接网络，这是由路由器在网络中的功能决定的。路由器用于连接多个网络，如果一台路由器用于连接多个物理网络，那么它需要有多个物理网络接口；如果一台路由器用于连接多个逻辑网络，那么，它可以让多个逻辑接口共用一个物理接口。

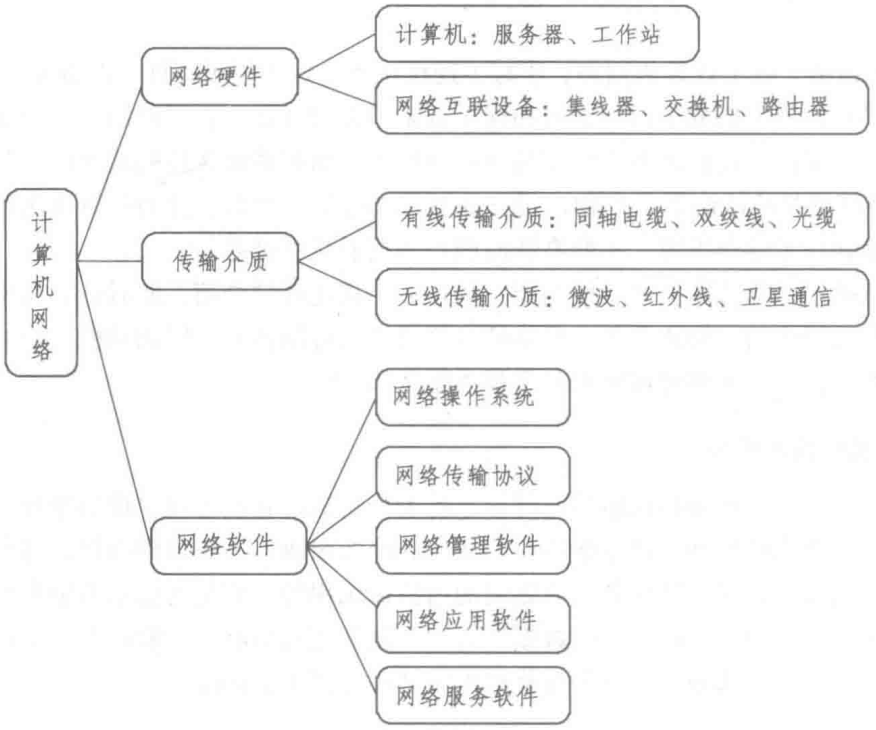

图 1.3 网络组成部分

（2）传输介质。传输介质是把网络节点连接起来的数据传输通道，包括有线传输介质和无线传输介质。同轴电缆、双绞线、光缆都是有线传输介质；微波、卫星通信、红外线都是无线传输介质。传输介质是网络数据传输的通道，所有的网络数据都要经过传输介质进行传输。因此，一个网络所选用传输介质的种类和质量对网络性能的好坏有较大影响。

（3）网络软件。网络软件是负责实现数据在网络硬件之间通过传输介质进行传输的软件系统。包括网络操作系统、网络传输协议、网络管理软件、网络服务软件和网络应用软件。

① 网络操作系统。网络操作系统是指在计算机或其他网络硬件上安装的，用于管理本地及网络资源和它们之间相互通信的操作系统。网络操作系统有集中式和对等式两种。集中式网络操作系统安装在网络服务器上，集中管理网络资源；对等式网络操作系统平等地安装在所有网络节点上，没有服务器。最典型的对等式网络操作系统是 Windows 98，常见的集中式网络操作系统有 Windows 2000/2003、Windows XP、Linux、Netware 和各种 UNIX（Solaris、AIX、HP UNIX、FreeBSD 等）。其中 Windows 系列的操作系统比较适合个人用户的 PC 机和中小型网络的服务器，UNIX 比较适合作为大型的因特网服务器。本书后面会具体地介绍 Windows 2003 操作系统在网络方面的应用。Linux 是 UNIX 操作系统在 PC 机上的实现，因其免费开放的特性，研究使用的用户比较多，许多网络管理人员都是从使用 Linux 开始的。而且，Linux 还可以作为经济实用的企业服务器操作系统。

② 网络传输协议。协议指两个或两个以上实体为了开展某项活动，经过协商后达成的一致意见。网络传输协议就是连入网络的计算机必须共同遵守的一组规则和约定，它可以保证数据