http://www.phei.com.cn

计算机网络安全技术及应用

邵 波 王其和 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

计算机网络安全技术及应用

邵　波　王其和　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

针对计算机网络安全问题，本书系统地介绍了网络和主机安全的基础知识，主要内容包括密码技术、数字水印技术、入侵监测技术、黑客攻击和防备技术、防火墙技术、网络管理和数据库安全。最后两章论述了网络安全在电子商务及企业反竞争情报领域的应用。

本书的特点是注重理论与实践的结合，除了理论知识的阐述外，每章后面还添加了“应用操作”，实用性强。本书适合高等学校信息管理与信息系统、电子商务等非计算机专业的学生使用。

图书在版编目（CIP）数据

计算机网络安全技术及应用 / 邵波，王其和编著. —北京：电子工业出版社，2005.11
ISBN 7-121-01856-X

Ⅰ.计… Ⅱ.①邵… ②王… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2005）第 120392 号

责任编辑：雷洪勤　　特约编辑：范　晓
印　　刷：北京市李史山胶印厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×1092　1/16　印张：19　字数：480 千字
印　　次：2005 年 11 月第 1 次印刷
印　　数：5000 册　　定价：26.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前　言

随着信息技术的飞速发展，网络及网络信息安全技术已经影响到社会的政治、经济、文化和军事等各个领域。以网络方式获取和传播信息已成为现代信息社会的重要特征之一。网络技术的成熟使得网络连接更加容易，人们在享受网络带来的便利的同时，网络的安全也日益受到威胁。安全的需求不断向社会的各个领域扩展，人们需要保护信息，使其在存储、处理或传输过程中不被非法访问或删改，以确保自己的利益不受损害。网络安全从其本质来讲就是网络上的信息安全，目前的公用通信网络中存在着各种各样的安全漏洞和威胁，其涉及的领域相当广泛。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性和可控性的相关技术和理论，都是网络安全的研究领域。

黑客攻击、病毒传播以及非法入侵等行为都向网络安全提出了挑战。网络安全是一项动态的、整体的系统工程，从技术上说，网络安全由防病毒、防火墙、入侵检测、网络监控、信息审计、通信加密、灾难恢复、安全扫描等多个安全组件组成。一个单独的组件是无法确保信息网络的安全性。针对上述情况，笔者结合多年的教学经验和工作体会撰写了本书。

计算机网络安全技术是涉及网络技术、主机技术和通信技术等多领域的一门综合性学科。随着各种网络安全问题的出现，网络安全技术的发展极为迅速。本书主要介绍网络安全的基础知识、相关的安全技术以及网络安全的应用。第 1～3 章介绍了网络技术及网络安全的基础理论，包括网络技术基础、网络安全概述及主机网络安全和访问控制安全；第 4～10 章论述了常规的网络安全技术，包括密码技术、数字水印技术、入侵监测技术、黑客攻击及防备技术、防火墙技术、数据库安全和网络安全管理；第 11～12 章阐述了网络安全在电子商务及企业反竞争情报领域的应用，包括电子商务安全和网络安全以及企业反竞争情报。

大部分网络安全方面的教材是从理论的角度论述，内容不够丰富生动。本书在每一章后面都附有应用操作，增强了读者的实际动手能力。最后两章阐述了网络安全与具体学科的结合，可为专业学生提供借鉴，也可扩展读者对网络安全应用的认识。

本书分 12 章，邵波、王其和构筑了本书的框架结构，蒋杰参加了第 5、9、10 章部分初稿的撰写；宋继伟参与了第 6、7、8 章部分初稿的撰写，其余部分由邵波、王其和撰写；最后由邵波对全书充实、修改和审定。

网络安全技术是一个不断发展的领域，还有许多问题需要进一步探索，加之作者水平有限，因此，本书还存在许多需要深入探讨和更新的内容，有待于今后进一步修订和补充。

作　者

2005.8

目　录

第 1 章　网络技术基础

随着计算机和通信技术的发展，计算机网络已成为全球信息基础设施的主要组成部分。同时，网络信息的安全和保密已成为一个至关重要且急需解决的问题。计算机网络所具有的开放性、互连性和共享性等特征使网上信息安全存在着先天不足，再加上系统软件中的安全漏洞以及所欠缺的严格管理，致使网络易受黑客、恶意软件的攻击，因此针对网络的安全所采取的措施应能全方位地针对各种不同的威胁，保障网络信息的保密性、完整性和可用性。网络安全技术的发展离不开计算机网络技术的发展，因此本章将简要介绍计算机网络技术方面的基础知识。

1.1　计算机网络概述

计算机网络是把一定地理范围内的计算机通过通信线路互连起来，并在相应通信协议和网络软件的支持下，彼此互相通信并共享资源的系统。因此，计算机网络还可以定义为“以能够相互共享资源的方式连接起来，并且各自具备独立功能的计算机系统的集合”。简单地说就是“一个互连的自主的计算机集合”，“计算机就是网络”的概念越来越被人们接受。

网络的作用是将原本独立且各自拥有部分资源的工作站（计算机）连接在一起形成网络，让资源得到最有效的运用，实现计算机之间的资源共享。因此，网络能提供资源的多少决定了一个网络的存在价值。计算机网络的规模有大有小，大的可以覆盖全球，小的可以只由一间办公室的两台或几台微机构成。通常，网络规模越大，包含的计算机越多，它所提供的网络资源就越丰富，其价值也就越高。

（1）Internet：Internet 是英文 International Network 的缩写，也就是所谓的“国际因特网”，简称为“因特网”。国际因特网可以说是世界范围内所有网络的集合，因为它不仅仅是单一的区域网络、而是由横跨全世界的各种相连的网络所组成。就技术层次而言，国际因特网是数以千计的电脑以 TCP/IP 为通信协议而连接在一起的网络。因此，Internet 可以说是分散在全球各地的资源与新通信交流媒体的总和。这样，使得任何一位连入 Internet 的用户都能获取散布在全球各地网络上的资源，并获得信息服务。

对广大网络用户而言，Internet 提供了许多服务，其中 5 种主要的服务分别是：全球资讯网（World Wide Web）、电子邮件（E-mail）、文件传输（FTP）、电子公告板（BBS）和远程登录（Telnet）。这 5 种服务各有所长，彼此间在功能上也有一些重叠。

（2）协议（Protocal）：协议就是大家必须共同遵从的一致约定。因为 Internet 由数以万计的网络与数亿台计算机组成，因此必须有一种方法保证 Internet 能够正常工作，虽然 Internet 的管理结构是松散的，但连入 Internet 的计算机必须遵从一致的约定，例如怎样建立连接，怎样互相识别等。只有遵守这个约定，计算机之间才能相互通信和交流。在现实生活中，世界上不同国家、地区的人与人之间的交谈需要使用同一种语言。如果一个人讲中文，另一个

人讲英文，那就必须找一个翻译，否则这两个人之间的信息无法沟通。计算机之间的通信过程和人与人之间的交谈过程非常相似，只是前者由计算机来控制，后者由参加交谈的人来控制。现在在 Internet 中使用的 TCP/IP 协议，就是这样的约定，它规定了计算机之间互相通信的方法。TCP/IP 协议对计算机网络中主机的寻址方式、主机的命名机制、信息的传输规则以及各种各样的服务功能均做了详细约定。TCP/IP 协议为任何一台计算机连入 Internet 提供了技术保障，任何人、任何团体都可以加入到 Internet。对用户开放、对服务提供者开放是 Internet 获得成功的重要原因。TCP/IP 协议就像是在“Internet 世界”中使用的“世界语”。只要 Internet 上的用户都使用 TCP/IP 协议，大家就能方便地进行交谈。

1.2　计算机网络的发展

计算机网络的发展过程经历了从简单到复杂、从单机到多机、从终端与计算机之间的通信发展到计算机与计算机之间的直接通信的演变过程。其发展历史按年代可以划分为 4 个阶段：

（1）20 世纪五六十年代：出现了以批处理为运行特征的主机系统和远程终端之间的数据通信为基础的第一代计算机网络。这一代计算机网络是以单个计算机为中心的远程联机系统。典型应用是由一台计算机和全美范围内 2000 多个终端组成的飞机订票系统。

（2）20 世纪六七十年代：出现了分时系统，主机运行分时操作系统，主机和主机之间、主机和远程终端之间通过前置机通信为基础的第二代计算机网络。第二代计算机网络是以多个主机通过通信线路互连起来，为用户提供服务，兴起于 20 世纪 60 年代后期，典型代表是美国国防部高级研究计划局协助开发的 DARPANET。主机之间不是直接用线路相连，而是由接口报文处理机 IMP 转接后互连的。IMP 和它们之间互连的通信线路一起负责主机间的通信任务，构成了通信子网。通信子网互连的主机负责运行程序，提供资源共享，组成了资源子网。

（3）20 世纪七八十年代：是计算机网络发展最快的阶段、网络开始商业化和实用化，通信技术和计算机技术促进、结合更加紧密，Internet 也应运而生，由此而产生了以 Internet 为基础的第三代计算机网络。第三代计算机网络是具有统一的网络体系结构并遵循国际标准的开放式和标准化的网络。ISO 在 1984 年颁布了 OSI/RM，该模型分为 7 个层次，也称为 OSI7 层模型。OSI 模型被公认为新一代计算机网络体系结构的基础，为普及局域网奠定了基础。

20 世纪 70 年代后，由于大规模集成电路出现，局域网由于投资少、方便灵活而得到了广泛的应用和迅猛的发展。

（4）20 世纪 90 年代后：局域网成为计算机网络结构的基本单元，网络间互连的要求越来越强，真正实现了以资源共享、数据通信和分布处理为目标的第四代计算机网络。第四代计算机网络从 20 世纪 80 年代末开始，局域网技术逐渐发展成熟，出现了光纤及高速网络技术、多媒体、智能网络。

1.3　计算机网络的功能及拓扑分类

1.3.1　计算机网络的功能

（1）资源共享功能：计算机网络的资源共享包括硬件资源共享和软件资源共享。硬件资源共享表现在计算机网络可以在全范围内提供信息处理设备资源、存储设备资源、输入输出设备资源等的共享，尤其是可以提供较高级和昂贵的设备，如激光打印机、大型绘图仪以及大容量外部存储器等的共享；软件资源的共享表现在允许网上的用户远程访问各种类型的数据库，并可使用各种公用的软件。

（2）分布处理功能：计算机网络的分布处理功能是指，把同一任务分配到网络中不同地理分布的结点机上协同完成。计算机网络的分布处理功能使人们可以通过计算机网络，将许多大型信息处理问题借助于分散在网络中的多台计算机协同完成，解决了单机无法完成的信息处理任务。特别是分布式数据库管理系统，它是分散存储在网络不同系统中的数据，使用起来就像集中存储和集中管理一样方便。

（3）网络服务功能：计算机网络在一定的协议软件的支持下能向网络用户提供一定的网络服务功能，如文件传输、远程文件访问、电子邮件、电子电话、虚终端、网络进程通信等。这些功能属于网络体系的应用层向用户提供的服务。随着网络技术的发展，计算机网络的各种服务功能将不断扩大和丰富。

（4）网络应用功能：计算机网络系统可以应用在不同的管理系统和信息系统，构成各种不同功能的网络应用系统。计算机网络的应用功能是在网络资源共享功能、分布式处理功能和网络服务功能的基础上，通过各种专业应用软件而实现的。

1.3.2　计算机网络的拓扑与分类

1. 计算机网络的拓扑结构

（1）总线结构：总线型结构采用单根传输线（或称总线）作为公共的传输通道，所有的结点都通过相应的接口直接连接到总线上，并通过总线进行数据传输。总线型结构使用广播式传输技术，总线上的所有结点都可以发送数据到总线上，数据沿总线传播。由于所有结点共享同一公共通道，因此在任何时候只允许一个结点发送数据，数据可以被总线上的其他结点接收，并分析目的地址再决定是否真正接收该数据。以太网就是这种结构的典型代表。

（2）环状结构：环状结构是将各个网络结点通过通信线路连成一条首尾相接的闭合环。在环状结构网络中，信息按固定方向流动，或顺时针方向，或逆时针方向。令牌环就是这种结构的典型代表。

（3）星状结构：星状结构是由点到点链路与中央结点相连的各结点组成的。信息的传输是通过中央结点的存储转发技术实现的，并且只能通过中央结点与其他结点通信。星状结构是以中央结点为中心，其他各结点通过单独的线路与中央结点连接，相邻结点之间的通信必须经过中央结点。这种拓扑结构的特点是利于集中控制，中央结点就是控制中心，一般应用于分级的主从式网络。

（4）树状结构：树状结构是从总线型结构和星状结构演变而来的。各结点按一定的层次连接起来，其形状像一棵倒置的树，故取名为树状结构，在树状结构的顶端有一个根结点，它带有分支，每个分支也可以带有子分支。这种树状结构与带有几个段的总线结构的主要区别在于根的存在。当结点发送时，根接收该信号，然后再重新广播送至全网。

（5）网状结构：网状结构是指将各网络结点与通信线路互连成不规则的形状，每个结点至少与其他两个结点相连。大型因特网一般都采用网状结构，例如：中国教育科研示范网CERNET及国际因特网的主干网。另外，也可以由上述两种或两种以上的网络拓扑结构组成一种混合型拓扑结构。例如，环星状结构是FDDI网络常用的拓扑结构。

2. 计算机网络的分类

由于计算机网络覆盖的地理范围不同，它们所采用的传输技术也不同，因此形成了各自的网络技术特点和网络服务功能。按照网络覆盖的地理范围大小，计算机网络可分为局域网、广域网和城域网。

（1）局域网：局域网（Local Area Network，LAN）是将较小地理区域内的计算机或数据终端设备连接在一起的通信网络。局域网覆盖的地理范围比较小，它常用于组建一个企业、校园、楼宇和办公室内的计算机网络。

（2）广域网：广域网（Wide Area Network，WAN）是在一个广阔的地理区域内进行数据、语音、图像等信息传输的通信网络。广域网覆盖的地理区域较大，它可以覆盖一个城市、一个国家、一个洲乃至整个地球。

（3）城域网：城域网（Metropolitan Area Network，MAN）是介于局域网和广域网之间的一种高速网络，它的覆盖范围在一个城市内。城域网的设计目标是要满足几十千米范围内的大量企业、公司、机关和学校的多个局域网互连的需求，以实现大量用户之间的数据、语音、图像和视频等多种信息的传输。

通常将网络上的计算机和通信设备等称为结点。按照结点之间的关系，可将计算机网络分为客户/服务器型网络和对等型网络两种。

（1）客户/服务器型网络：在客户/服务器型网络中存在两种类型的计算机。一个是客户（又称为工作站），它是指网络中的个人用户使用的计算机，可接受服务器提供的服务；另一个是服务器，它是网络管理、存储程序和数据及提供共享资源的中心设备。网络中使用的服务器一般都是高性能计算机，而且在服务器上运行的操作系统也是适合网络服务的系统。

（2）对等型网络：对等型网络与客户/服务器型网络的最大区别就是对等型网络没有专设服务器。所有的计算机都平等地共享联网任务，它们都具有相同的能力来提供网络资源，并在其他结点上使用这些资源。每个计算机既可作为工作站，又可作为其他工作站的服务器。

1.4　OSI参考模型与TCP/IP协议

1.4.1　OSI参考模型

使网络中的两台计算机系统通信需要一致的协议，同时不同主机、不同厂商的网络互联需要统一的标准。国际标准化组织（ISO）早在20世纪70年代末就提出了开放系统互连（OSI）

参考模型。OSI 模型提出后的 30 多年来，有关网络协议设计的思想已经有了很大发展，许多现代的网络协议也不完全符合 OSI 模型，但是 OSI 的概念与思想仍然被保留了下来。

OSI/RM 只给出了计算机网络的一些原则性说明，并不是一个具体的网络。它将整个网络的功能划分成七个层次（如图 1-1 所示）。层与层之间的联系是通过各层之间的接口来进行的，上层通过接口向下层提出服务请求，而下层通过接口向上层提供服务。两个用户计算机通过网络进行通信时，除物理层之外，其余各对等层之间均不存在直接的通信关系，而是通过各对等层之间的通信协议来通信，只有两物理层之间通过传输介质进行真正的数据通信。

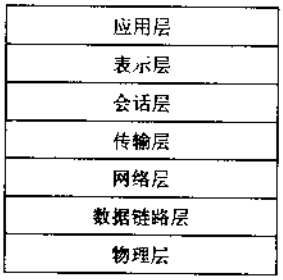

图 1-1　七层 OSI 参考模型

OSI 参考模型中各层的主要作用如下。

（1）物理层：为数据链路层提供物理连接，在其上串行传送比特流，即所传送数据的单位是比特。此外，该层中还具有确定连接设备的电气特性和物理特性等功能。

（2）数据链路层：负责在网络结点间的线路上通过检测、流量控制和重发等手段，无差错地传送以帧为单位的数据。为做到这一点，在每一帧中必须同时带有同步、地址、差错控制及流量控制等控制信息。

（3）网络层：为了将数据分组从源（源端系统）送到目的地（目标端系统），网络层将选择合适的路由和交换结点，使从源传输层传下来的分组信息能够正确无误地按照地址找到目的地，并交付给相应的传输层，即完成网络的寻址功能。

（4）传输层：传输层是高低层之间衔接的接口层。数据传输的单位是报文，当报文较长时将它分割成若干分组，然后交给网络层进行传输。传输层是计算机网络协议分层中最关键的一层，该层以上各层将不再管理信息传输问题。

（5）会话层：该层对传输的报文提供同步管理服务。在两个不同系统的互相通信的应用进程之间建立、组织和协调交互。例如，确定是双工还是半双工工作。

（6）表示层：该层的主要任务是把所传送的数据的抽象语法变换为传送语法，即把不同计算机内部的不同表示形式转换成网络通信中的标准表示形式。此外，对传送的数据加密（或解密）、正文压缩（或还原）也是表示层的任务。

（7）应用层：该层直接面向用户，是 OSI 中的最高层。它的主要任务是为用户提供应用的接口，即提供不同计算机间的文件传送、访问与管理，电子邮件的内容处理，不同计算机通过网络交互访问的虚拟终端功能等。