信号与信息处理
技术丛书

传统网络与现代网络安全

刘华群 主编

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

信号与信息处理技术丛书

传统网络与现代网络安全

刘华群　主　编

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

内 容 简 介

本书共分 10 章，内容包括网络安全概述、网络安全体系结构与协议、身份认证理论与技术、访问控制原理及技术、防火墙技术与应用、统一威胁安全管理技术、无线网络技术及其安全、物联网技术及其安全、云计算与云安全、移动互联网技术与安全。本书既注重对传统网络安全技术与原理的介绍，又注重引入网络安全中的新技术和新概念，从而对于帮助读者全面了解网络安全的相关原理、技术实现及其发展前沿具有重要作用。

本书既可以作为网络信息安全或计算机专业本科生、研究生的教材，也可以作为相关领域研究人员和专业技术人员的参考用书。

图书在版编目（CIP）数据

传统网络与现代网络安全 / 刘华群主编. —北京：电子工业出版社，2014.3
（信号与信息处理技术丛书）
ISBN 978-7-121-21797-5

Ⅰ. ①传… Ⅱ. ①刘… Ⅲ. ①计算机网络—安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2013）第 261679 号

策划编辑：董亚峰
责任编辑：底 波
印 刷：北京天宇星印刷厂
装 订：三河市鹏成印业有限公司
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
开 本：787×1 092 1/16 印张：21 字数：537.6 千字
印 次：2014 年 3 月第 1 次印刷
定 价：49.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

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。

服务热线：（010）88258888。

前　言

网络安全学科对国家安全和经济建设有着极其重要的作用。近年来，随着我国国民经济和社会信息化进程的全面加快，计算机网络在政治、军事、金融、商业等部门的广泛应用，网络与信息系统的基础性、全局性作用不断增强，全社会对计算机网络的依赖越来越大。网络系统如果遭到破坏，不仅会引起社会混乱，还将带来经济损失。网络安全已经成为国家安全的重要组成部分。加快网络安全保障体系的建设、培养高素质的网络安全人才队伍，已经成为我国经济社会发展和信息安全体系建设中的一项长期性、全局性和战略性的任务。目前，世界各国都积极开展了网络安全的研究和教育。在欧美，网络安全的教育已大为普及。美国的多所大学为政府和军事部门培养了大批专门的网络安全人才。相比之下，我国的网络安全教育还略显滞后，专业教材相对匮乏。为此，我们根据自己的科学实践，以多年来的科研成果为基础，结合网络安全的教学经验，编著了本书。

本书内容全面，既涵盖网络安全的理论基础知识，又包括网络安全的实用技术和最近的科研成果。讲用结合，按照从一般到特殊的原则，每章在介绍相关理论基础知识的基础上，还将结合科研实践，对相关领域进行深入探讨。

本书在编写过程中，参考和引用了大量的产品技术资料、现有教材资料和工程文档，这些资料列在书末的参考文献中，在此谨对所有相关材料的作者表示感谢。

本书适合于不同层次的关心和喜爱网络安全的读者。每一章的中前部的理论基础知识可以帮助初级读者迅速了解和掌握该领域的基础知识和概貌，而后面深入的科研成果论述，又可以满足高级读者深入学习的需要。

编　者

反侵权盗版声明

目　录

第1章 网络安全概述

知识点

- 网络安全的定义
- 网络面临的安全威胁
- 网络出现安全威胁的原因
- 网络的安全机制

难点

- 网络安全威胁是如何产生的

要求

熟练掌握以下内容:

- 网络安全的定义
- 网络面临的各种安全威胁
- 网络的安全机制

了解以下内容:

- 产生网络安全威胁的原因

随着计算机技术和通信技术的迅速发展，计算机应用已经逐渐渗入到人类社会的各个领域中。而20世纪80年代后计算机互联网络技术的日渐成熟，更是为人类社会打开了一个前所未有的新世界。实际上，网络的快速普及与发展，客户端软件多媒体化、协同计算、资源共享、远程信息的管理、电子商务、移动商务、电子政务等都已经成为网络时代不可缺少的重要产物。如今，互联网所固有的跨时空和跨地域的特性，不仅改变了人们传统的工作方式和生活模式，而且也促进了我国的经济和社会的发展。但是，正因为互联网的开放化和个性化的特点，使得它在向人们提供各类网络信息共享和资源共享及在线通信的同时，也给自身带来了很大不安全因素。

1.1 计算机网络概述

计算机网络是随着计算机技术和通信技术相结合的产物，是用于信息传输的基础设施，而信息对于任何时代而言都是人类社会所需的重要资源。因此，保障网络的安全，从某种程度上来说，保障网络中的“信息”安全是社会稳定安全的必要条件。用于承载“信息”的网络，尤其是计算机网络，其自身的安全性是保障一切安全的基础。因此，在解释网络信息安全及其相关术语之前，首先必须明确计算机网络的相关概念。

1.1.1 计算机网络基本概念

在计算机网络发展过程的不同阶段中，人们对计算机网络提出了不同的定义。不同的定义反映当时网络技术发展的水平，人们对网络的认识程度以及研究的着眼点不同。而在本书中，我们采用如下的计算机网络概念：计算机网络就是利用通信设备和线路将地理位置不同的、功能独立的多个计算机系统互连起来，以功能完善的网络软件（即网络通信协议、信息交换方式、网络操作系统等）实现网络中资源共享和信息传递的系统。一个典型的计算机网络组成结构如图 1-1 所示。

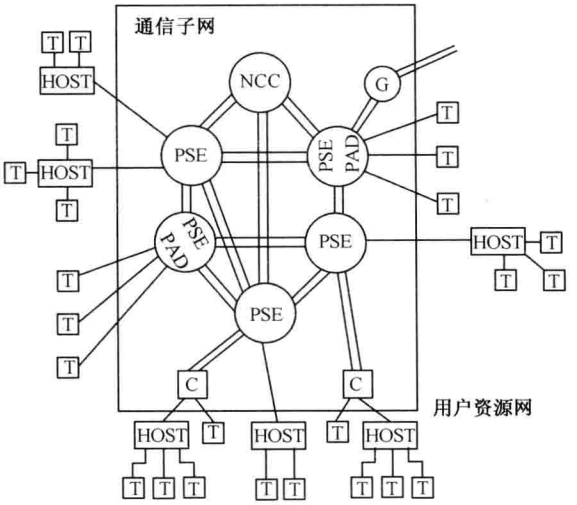

图 1-1 一个典型的计算机网络结构

其中，由主机（Host）和终端（Terminal）组成的资源子网，用于实现计算机网络中的数据处理功能；由分组交换设备 PSE、分组装 / 卸设备 PAD、集中器 C、网络控制中心 NCC、网间连接器 G 和通信链路组成的通信子网，用于实现计算机网络中的数据传输功能。

与计算机网络相类似的另外一个概念“分布式系统”，为了方便讨论，在本书中，对两者不做细致的区分。事实上，分布式系统是构建在计算机网络顶部的软件系统，软件使其具有内聚性和透明性。计算机网络和分布式系统有很多相通之处，尤其两者在硬件与底层通信协议上是基本相同的，包括拓扑结构、硬件连接和通信控制规程等。

计算机网络的基本功能及所能提供的服务，包括如下几个方面：

（1）实现包括：文件传输、IP 电话、Email、视频会议、OICQ 等数据通信。

（2）实现网络包括：软件、硬件、数据等多种类型的资源共享。

（3）可替代的资源，提供连续的高可靠服务，从而实现网络系统的高可靠性等。

1.1.2　网络拓扑结构与信息安全

网络的拓扑结构是影响计算机网络性能和安全的重要因素之一。其中，网络拓扑隐去了网络的具体物理特性（如距离、位置等）而抽象出节点之间的关系加以研究。常见的网络拓扑结构包括：总线网、星状网、环状网和分布式结构等。

1．总线网

在总线网结构中，采用单根传输线作为传输介质，也就是说，所有的计算机都连接到一条公共传输介质（或称总线）上，如图 1-2 所示。

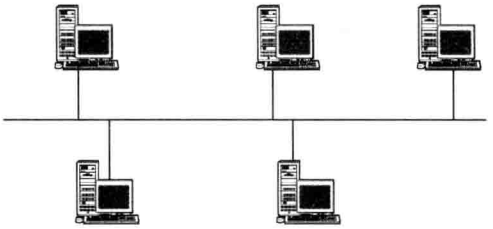

图 1-2　总线网拓扑结构

这种网络拓扑结构具有费用低、用户入网灵活、站点或某个用户失效不影响其他站点或用户通信的优点。缺点是一次仅能一个用户发送数据，其他用户必须等到获得发送权；媒体访问获取机制较复杂；维护难，分支节点故障查找难。尽管有上述一些缺点，但由于布线要求简单，扩充容易，用户失效、增删不影响全网工作，所以总线网是 LAN 技术中使用最普遍的一种。

2．星状网

星状网是以中央节点为中心，用单独的线路使中央节点与其他各站点直接相连，如图 1-3 所示。

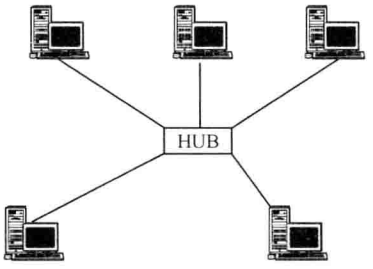

图 1-3　星状网拓扑结构

星状网因为网络用户之间的通信必须经过中心站，所以其拓扑结构便于集中控制。由于这一特点，也带来了易于维护和较安全等优点。网络用户设备因为故障而停机时也不会影响其他用户间的通信。同时星状网拓扑结构的网络延迟时间较小，传输误差较低。但这种结构非常不好的一点是：中心系统必须具有极高的可靠性，因为中心系统一旦损坏，整个系统便趋于瘫痪。对此，中心系统通常采用双机热备份，以提高系统的可靠性。

3．环状网

环状网用户都与两个相邻的网络用户相连，因而存在点到点链路，但总是以单向方式操作，如图 1-4 所示。

信息流在网中是沿着固定方向流动的，两个节点仅有一条道路，故简化了路径选择的控制。

环状网的缺点是：当环中节点过多时，网络的响应时间延长；由于环状网是封闭的，不便于扩充；同时当一个节点故障，将会造成全网瘫痪，故其可靠性低；维护难，对分支节点故障定位较难。

4．分布式结构

分布式结构的网络是将分布在不同地点的计算机通过线路互连起来的一种网络形式，如图 1-5 所示。

分布式结构的网络具有如下特点：由于采用分散控制，即使整个网络中的某个局部出现故障，也不会影响全网的操作，因而具有很高的可靠性；网络中的路径选择最短路径算法，故网上延迟时间少，传输速率高，但控制复杂，在一般局域网中不采用这种结构。

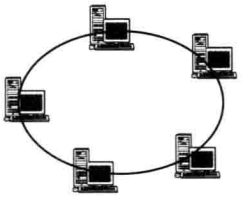

图 1-4　环状网拓扑结构

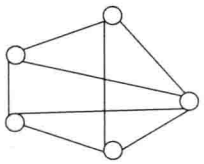

图 1-5　分布式结构

1.1.3　网络体系结构及协议

1.1.3.1　网络体系结构的定义和发展

网络体系结构作为一个抽象的概念，它定义和描述一组用于计算机及其通信设施之间互连的标准和规范的集合，遵循这组规范可以很方便地实现计算机设备之间的通信。网络体系结构就是指网络的分层、各层协议和层间接口的集合，即网络及其部件应当完成功能的定义。换句话来说，网络的体系结构相当于网络的类网，而具体的网络体系结构则相当于网络的一个具体实例。

网络体系结构是为了便于描述、设计和实现网络的整套协议而采用的。计算机网络体系结构采用分层体系结构，即将整套协议体系分成不同的层次，每一层把下面各层包扎起来，并把下一层和上一层隔开。每一层都在下层提供的服务上增加一定的功能，一起为上一层提供服务，从而使最高层能为用户提供一组完整的服务。由此可见，网络体系结构的特点可以归纳如下几点：

- 每一层都将利用它下一层的服务来向它的上一层提供服务。
- 每一层都通过协议和其他节点的同一层进行通信。这种通信通过与下一层之间的直接通信来完成。
- 第 n 层与第 $n-1$ 层之间的通信称为接口。
- 第 n 层从第 $n+1$ 层得到包含一些必要的附加信息（如目的地址等）的数据后，第 n 层把这些数据传输给目的节点的第 n 层处理，目的节点的第 n 层再把这些数据送给该节点的第 $n+1$ 层。第 n 层经常需要在数据包上附加一些信息。

- 为了得到目的节点的信息，第 n 层将传递一个数据块给第 $n-1$ 层，里面包括从第 $n+1$ 层上传来的数据以及第 n 层上附加的一些控制信息。另外，第 n 层还可以在这个数据块中加入一些其他的信息，如第 n 层与第 $n-1$ 层之间的接口信息。

1.1.3.2　通信协议

计算机网络中的数据交换必须遵守事先约定好的规则。这些规则明确规定了所交换的数据的格式以及有关的同步问题（同步含有时序的意思）。为进行网络中的数据交换而建立的规则、标准或约定即网络协议（Network Protocol），简称协议。网络协议由三个要素组成：

- 语法：用户数据与控制信息的结构和格式。
- 语义：需要发出何种控制信息以及完成的动作和做出的响应。
- 时序：对事件实现顺序的详细说明。

1.1.3.3　ISO/OSI 参考模型

世界上第一个网络体系结构 SNA（Systems Network Architecture，网络系统结构）是由美国 IBM 公司在 1974 年按照分层的方法提出的。现在 SNA 已成为世界上较广泛使用的一种网络体系结构。此后，其他公司也相继提出了自己的网络体系结构，如 Digital 公司的 DNA（Digital Network Architecture，数字网络体系结构），美国国防部提出的 TCP/IP 等。多种网络体系结构并存，其结果是若采用 IBM 的结构，就只能选用 IBM 的产品，只能与同种结构的网络互连。

1．OSI 的设计目的

OSI 的设计目的是：成为一个所有销售商都能实现的开放网络模型，以克服使用众多私有网络模型所带来的困难和低效性。OSI 是在一个备受尊敬的国际标准团体的参与下完成的，这个组织就是 ISO（国际标准化组织）。在 OSI 出现之前，计算机网络中存在众多的体系结构，其中以 IBM 公司的 SNA（系统网络体系结构）和 DEC 公司的 DNA（Digital Network Architecture）数字网络体系结构最为著名。

为了解决不同体系结构的网络的互连问题， ISO（注意不要与 OSI 搞混）于 1981 年制定了开放系统互连参考模型（Open System Interconnection Reference Model，OSI/RM）。这个模型把网络通信的工作分为 7 层，它们由低到高分别是：物理层（Physical Layer）、数据链路层（Data Link Layer）、网络层（Network Layer）、传输层（Transport Layer）、会话层（Session Layer）、表示层（Presentation Layer）和应用层（Application Layer）OSI 参考模型如图 1-6 所示。

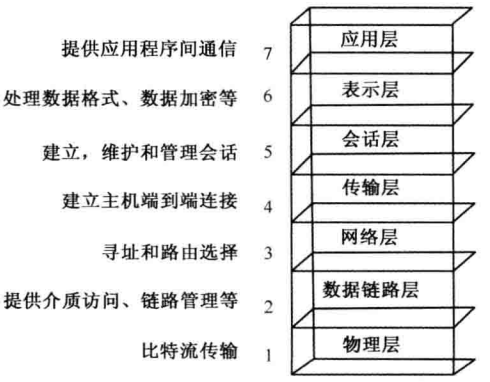

图 1-6　OSI 参考模型