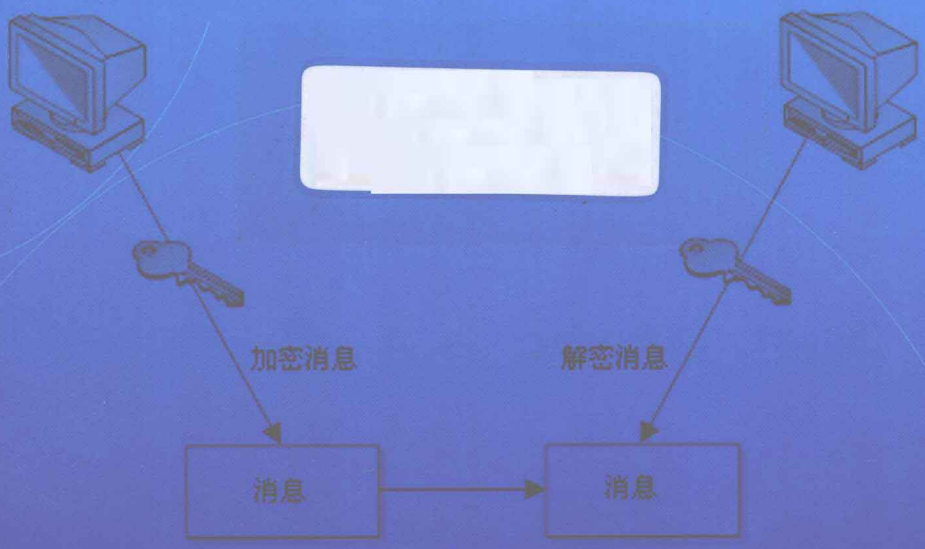
高等院校网络教育系列教材

网络安全设计

WANGLUO ANQUAN SHEJI

于九红 主编　　范贵生 副主编



華東理工大學出版社
EAST CHINA UNIVERSITY OF SCIENCE AND TECHNOLOGY PRESS

图书在版编目(CIP)数据

网络安全设计 / 于九红主编. —上海:华东理工大学出版社,2012.8
高等院校网络教育系列教材
ISBN 978-7-5628-3335-2

Ⅰ.①网… Ⅱ.①于… 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(2012)第 173143 号

高等院校网络教育系列教材

网络安全设计

主　　编 / 于九红
副 主 编 / 范贵生
责任编辑 / 纪冬梅
责任校对 / 金慧娟
封面设计 / 裘幼华
出版发行 / 华东理工大学出版社有限公司
地　　址:上海市梅陇路 130 号,200237
电　　话:(021)64250306(营销部)
(021)64250787(编辑室)
传　　真:(021)64252707
网　　址:press.ecust.edu.cn
印　　刷 / 上海崇明裕安印刷厂
开　　本 / 787 mm×1092 mm　1/16
印　　张 / 16.25
字　　数 / 394 千字
版　　次 / 2012 年 8 月第 1 版
印　　次 / 2012 年 8 月第 1 次
书　　号 / ISBN 978-7-5628-3335-2
定　　价 / 39.80 元

联系我们:电子邮箱 press@ecust.edu.cn
官方微博 e.weibo.com/ecustpress

序

网络教育是依托现代信息技术进行教育资源传播、组织教学的一种崭新形式，它突破了传统教育传递媒介上的局限性，实现了时空有限分离条件下的教与学，拓展了教育活动发生的时空范围。从1998年9月教育部正式批准清华大学等4所高校为国家现代远程教育第一批试点学校以来，我国网络教育历经了若干年发展期，目前全国已有68所普通高等学校和中央广播电视大学开展现代远程教育。网络教育的实施大大加快了我国高等教育的大众化进程，使之成为高等教育的一个重要组成部分；随着它的不断发展，也必将对我国终身教育体系的形成和学习型社会的构建起到极其重要的作用。

华东理工大学是国家“211工程”重点建设高校，是教育部批准成立的现代远程教育试点院校之一。华东理工大学网络教育学院凭借其优质的教育教学资源、良好的师资条件和社会声望，自创建以来得到了迅速的发展。但网络教育作为一种不同于传统教育的新型教育组织形式，如何有效地实现教育资源的传递，进一步提高教育教学效果，认真探索其内在的规律，是摆在我们面前的一个新的、亟待解决的课题。为此，我们与华东理工大学出版社合作，组织了一批多年来从事网络教育课程教学的教师，结合网络教育学习方式，陆续编撰出版一批包括图书、课程光盘等在内的远程教育系列教材，以期逐步建立以学科为先导的、适合网络教育学生使用的教材结构体系。

掌握学科领域的基本知识和技能，把握学科的基本知识结构，培养学生在实践中独立地发现问题和解决问题的能力是我们组织教材编写的一个主要目的。系列教材包括了计算机应用基础、大学英语等全国统考科目，也涉及了管理、法学、国际贸易、机械、化工等多学科领域。

根据网络教育学习方式的特点编写教材，既是网络教育得以持续健康发展的基础，也是一次全新的尝试。本套教材的编写凝聚了华东理工大学众多在学科研究和网络教育领域中有丰富实践经验的教师、教学策划人员的心血，希望它的出版能对广大网络教育学习者进一步提高学习效率予以帮助和启迪。

华东理工大学副校长 徐嘉东

前　言

网络安全日益成为人们关注的焦点，小至日常生活中的上网安全，大至国家军事、政治安全。信息安全是网络安全的重要概念，所谓信息安全，要从“信息”和“安全”两方面来分析。首先所谓“信息”，信息的载体可以是书，可以是人，也可以是媒体，当然目前最大的载体应该是互联网。人们在网上获取、传播、交换信息，以前所未有的速度更新信息，但这些信息的来源、真伪、可靠性以及传播过程中会不会被他人截取、篡改等问题，需要我们考虑，这就是“安全”。信息安全要做的就是保证信息的保密性、完整性和不可抵赖性。

平时我们使用计算机时担心中病毒、担心 QQ 被盗号、担心网银密码泄露等，这些都是信息安全的范畴。而在企业中，数据的备份恢复、员工的安全培训、IT 架构的实施，这些也属于信息安全。所以说信息安全所涉及的范围是整个 IT 领域，凡是与计算机相关的行业，都离不开信息安全。平时的业务不关注安全，一旦发生故障，就会使大量业务瘫痪或导致数据泄密，造成巨大的损失，而问题十之八九是出在信息安全方面。

本书主要介绍有关网络安全的各个领域，包括计算机病毒、网络攻防、密码学、数据备份及恢复等，特别对当前的热点应用——无线技术和远程访问——单独进行了详细的讲述。本书的特点是结合大量的网络安全实验，从原理和实际应用的角度深入浅出地讲解什么是网络安全，网络安全到底该如何应用，从而摒弃了传统网络安全书籍中堆砌理论和文字的做法，让不同基础的读者都能够领悟和应用网络安全的知识。特别在本书的最后一章安排了网络安全设计实验，读者可以先从这一章学起，实际动手解决日常生活中的信息安全问题，然后带着疑问阅读相关的理论知识。当然，也可以先学习理论知识，最后用实际操作融会贯通。

在此，非常感谢博士生裴新和周陆乐编写部分章节的内容，由于能力有限，书中错误和不足之处在所难免，敬请各位读者批评指正！

编　者

2012.8

目　录

第 1 章　网络安全概论

【概述】

互联网是对全世界都开放的网络，任何单位或个人都可以在互联网上方便地传输和获取各种信息。互联网这种具有开放性、共享性、国际性的特点对计算机网络安全提出了挑战。

【学习目标】

(1) 了解国内外网络安全的现状；
(2) 掌握网络基础知识，深入理解 OSI 网络 7 层模型；
(3) 了解网络安全的主要技术；
(4) 了解网络安全模型。

计算机技术的发展历史非常短，1946 年世界上第一台计算机诞生，随后的几十年时间内，计算机技术迅速崛起，到如今计算机技术可以说是如日中天、备受瞩目。

在大型机时代，只有少数人才能够接触到计算机，用户直接通过服务器访问大型机，虽然存在安全漏洞，但没有太多人有兴趣利用它们，信息安全并没有受到重视。然而，随着计算机技术的发展，成千上万个对计算机不甚精通的人有更多的机会接触到重要数据和流程，却没有建立相关的屏障和保护机制，这样很容易造成重要数据的损坏和丢失，因此用户之间需要层次型的软件，操作系统的各部分和用户有可能破坏的数据之间也同样应该有层次型的结构。这种层次型的结构一方面通过将个人与操作系统和数据文件的核心隔离开来，提高安全性，另一方面，也有益于不断增强计算机的功能。

短短几十年中，不管是在日常生活还是商业方面，人们已经极大地依赖于计算机技术。计算机被应用于公共设施、军事防御系统、金融机构和医疗设备，并应用于各种可能的商业角落。几乎所有的公司都会由于各种原因依赖于数据处理。我们对技术的依赖性和技术在我们生活中发挥的作用，使得信息安全成为一个必须面对的课题。

1.1　网络安全的现状

安全的概念非常广泛，它包含了众多彼此影响着的不同的领域。物理安全与信息安全相关，数据库安全受操作系统安全的影响，操作安全影响计算机系统的使用，灾难恢复技术

用来处理紧急情况下的系统，几乎每个安全案例都会牵涉到某种法律或责任关系。技术、硬件、人和法律条例交织在一起，形成一个安全网。当调查一个具体问题时，应该对问题进行分解，理解问题的不同部分，这样才能提出最好和最有效的解决方案。安全是一个复杂并且精彩的课题。

互联网是对全世界都开放的网络，任何单位或个人都可以在网上方便地传输和获取各种信息，互联网这种具有开放性、共享性、国际性的特点就对计算机网络安全提出了挑战。网络系统的脆弱性主要有以下几项。

网络的开放性。网络的技术是全开放的，使得网络所面临的攻击来自多方面。或是来自物理传输线路的攻击，或是来自对网络通信协议的攻击，以及对计算机软件、硬件的漏洞实施攻击。

网络的国际性。意味着对网络的攻击不仅是来自于本地网络的用户，还可以是互联网上其他国家的黑客，所以，网络安全面临着国际化的挑战。

网络的自由性。大多数的网络对用户的使用没有技术上的约束，用户可以自由地上网，发布和获取各类信息。

由于网络的开放性和安全性本身即是一对固有矛盾，无法从根本上予以调和，再加上基于网络的诸多已知和未知的人为与技术的安全隐患，网络很难实现自身的根本安全。目前，计算机信息系统的安全威胁主要来自于以下几类。

1. 计算机病毒

随着计算机网络技术的发展，计算机病毒技术也在快速地发展变化之中，而且在一定程度上走在了计算机网络安全技术的前面。有专家指出，从木马病毒的编写、传播到出售，整个病毒产业链已经完全互联网化。对数量继续暴增的计算机病毒来说，防护永远只能是一种被动措施，而计算机感染上病毒后，轻则使系统工作效率下降，重则造成系统死机或毁坏，使部分或全部数据文件丢失，甚至造成计算机主板等部件的损坏，导致硬件系统完全瘫痪。据公安部调查结果显示，计算机病毒仍然呈现出异常活跃的态势，互联网站被大量“挂马”成为病毒木马传播的主要方式。同时，目前计算机病毒、木马等绕过安全产品的探测、查杀甚至破坏安全产品的能力也增强了。可见，当前计算机系统遭受病毒感染的情况相当严重。

2. 黑客的威胁和攻击

计算机信息网络上的黑客攻击事件愈演愈烈，据《2008 瑞星中国大陆地区互联网安全报告》披露，以牟利为目的的黑客产业链已经形成并成为新的暴利产业。电脑一旦成为了“肉鸡”，黑客可以在被控制的该电脑上恣意妄为。同时，作为技术能力比较弱的中国，遭受境外黑客攻击的情况也十分严重。

3. 内部威胁

上网单位由于对内部威胁认识不足。所采取的安全防范措施不当，导致了内部网络安全事故逐年上升。不论是有意的还是偶然的，内部威胁始终是一个很大的安全隐患。如果网络的安全策略是未知的或不能执行的，用户的某些行为诸如浏览不安全的网站，点击电子邮件中的恶意链接，或者不对敏感数据加密等都将不知不觉地扮演着安全炸弹的角色。而随着人员的移动性越来越强，使用未加密的移动设备上网也大大增加了“暴露”的风险，给犯罪分子留下可乘之机。另外，一机两用甚至多用的情况普遍存在，计算机在内外网之间频繁切换使用，许多用户将在 Internet 上使用过的计算机在未经许可的情况下擅自接入内部局

域网络使用，造成病毒的传入和信息泄密。公安部调查结果显示，攻击或病毒传播源来自内部人员的比例有所增加，来自外部人员的比例有所减少，说明联网单位绝大部分考虑外部网络的攻击，而来自内部的威胁呈上升态势。

4. 网络犯罪

网络犯罪是非常容易操作的，不受时间、地点、条件限制的网络诈骗简单易行、隐蔽性强，能以较低的成本获得较高的效益。再加上网络空间的虚拟性、异地性等特征，在一定程度上刺激了网络犯罪率的增长。网络犯罪率的增长，除了给社会造成负面影响外，也造成经济损失，据有关方面统计，现在每天因全球网络犯罪导致资金流失高达数百亿、甚至上千亿美元。

5. 系统漏洞

许多网络系统都存在着这样那样的漏洞，这些漏洞有可能是系统本身所有的。如Windows NT、UNIX等都有数量不等的漏洞。另外，局域网内网络用户使用盗版软件，随处下载软件及网管的疏忽都容易造成网络系统漏洞。这不但影响了局域网的正常工作，也在很大程度上把局域网的安全置于危险之地，黑客利用这些漏洞就能进行密码探测、系统入侵等攻击。

1.2 网络基础知识

1.2.1 开放系统参考互联模型

ISO是为提供国际标准而工作的全球联盟。20世纪80年代早期，它发展了一套适用于全世界所有的供应商的协议集，以此希望确保所有供应商的产品都能跨过国家和技术的边界进行通信和交互。OSI的模型被采纳，成为大多数应用和协议所遵循的抽象框架。

OSI模型给供应商、工程师、开发者和其他人提供了重要的指导，它将网络任务、协议和服务分为不同的层。当两台计算机通过网络通信时，每一层都有它自己的任务，它的功能由对应层的服务和协议来实现。图1-1为OSI模型。

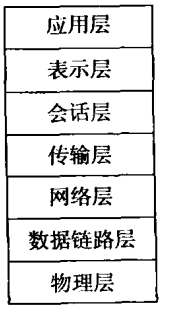


图1-1 OSI模型

网络协议是决定网络中系统如何通信的规则标准的集合。两个不同系统之所以能相互通信，是因为它们用了相同的协议，尽管它们本身有所不同。这与两个人因使用相同的语言而能相互交流的道理是一样的。

虽然计算机通信是物理的，它们也通过逻辑通道通信。特定OSI层次的协议与工作在另一台计算机的相同OSI层次的协议通信，这可以通过封装来完成。

封装过程如下：一个消息在应用层创建，通过协议栈往下传。每一层协议在消息中添加特定信息，消息尺寸在协议栈往下走的过程中变大。然后消息被送到目标计算机，通过逆转封装的过程，将消息拆开，最后送到目标计算机上的应用层。图1-2表示了OSI模型的封装过程。

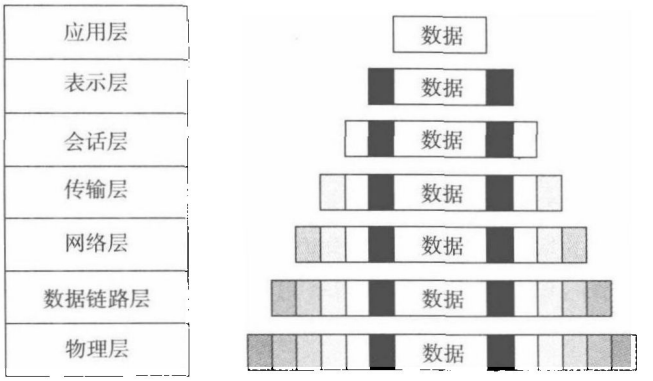


图 1-2 OSI 模型的封装过程

下面对 OSI 模型的每一层中具体的功能和协议进行详细讨论。

1. 应用层(Application Layer)

应用层是 OSI 模型中的第七层，是与用户端最近的一层，它提供文件传输、消息交换、终端会话以及更多功能。这一层不包括实际的应用，但是包括支持这些应用的协议。当应用要在网络中传送数据时，由这一层进行处理，给数据适当的格式并传到 OSI 模型的下一层(表示层)。应用层创建的数据包含了每一层所需的关键信息后，数据才会在网络中传送。

应用层的协议用于处理文件传输、虚拟终端、网络管理，并执行应用程序的网络请求。以下是应用层中的几个协议：

- 文件传输协议(FTP)；
- 普通文件传输协议(TFTP)；
- 简单网络管理协议(SNMP)；
- 简单邮件传输协议(SMTP)；
- 超文本传输协议(HTTP)；
- 远程登录协议(Telnet)。

图 1-3 表示了应用程序如何通过应用程序接口(API)与下面的协议通信。

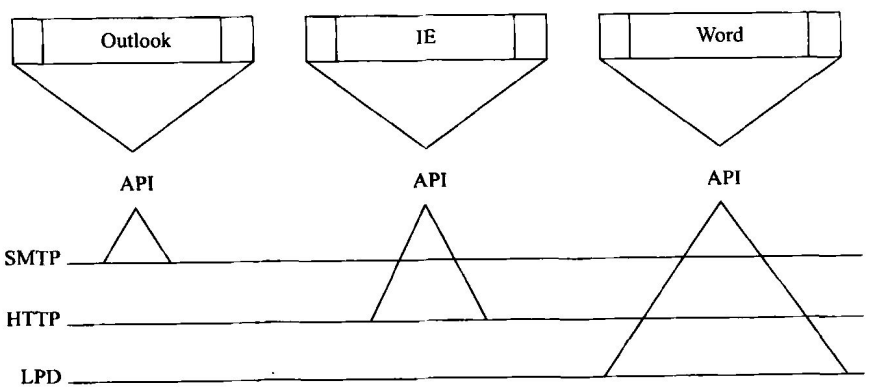


图 1-3 应用发送请求到 API

图 1-3 中，Outlook 利用 SMTP 协议收发邮件，对邮件内容进行加密等处理；IE 使用 HTTP 协议对上网用户实现即时响应；行式打印机后台程序（Line Printer Daemon，LPD）用来处理 Word 文档，应用层的协议通过 API 接口实现应用程序的功能。

2. 表示层（Presentation Layer）

表示层是 OSI 模型中的第六层，它从应用层协议接收信息，然后将信息变成所有遵守 OSI 模型的计算机都能理解的格式。这一层提供了一种能被末端系统正确处理的用一个结构表示数据的方式。表示层不管数据的含义，只关心数据的格式和语法。它像一个翻译机那样工作，将应用程序使用的格式翻译成能在网络上用于消息传递的标准格式。表示层也处理数据的压缩和加密。如果应用层的一个程序请求在将某个文件传送到网络之前，对其进行了压缩和加密，表示层就可以向目标计算机提供必要信息。这些信息包括有关加密或者所使用的压缩类型的指令，以及如何向用户正确呈现这个文件。指令被添加到数据包中，用于告知接收系统如何正确地解密或解压数据。

表示层中的服务用于处理标准格式的转译、数据压缩与解压，以及数据加密与解密。这一层中没有协议工作，只有服务。下面是表示层中的一些标准：

- 美国信息交换标准编码（ASCⅡ）；
- 扩展二进制编码十进制交换模式（EBCDIC）；
- 标签图像文件格式（TIFF）；
- 联合影像专家组（JPEG）；
- 活动图像专家组（MPEG）；
- 乐器数字接口（MIDI）。

图 1-4 为表示层如何将文件转变成不同标准的文件格式。

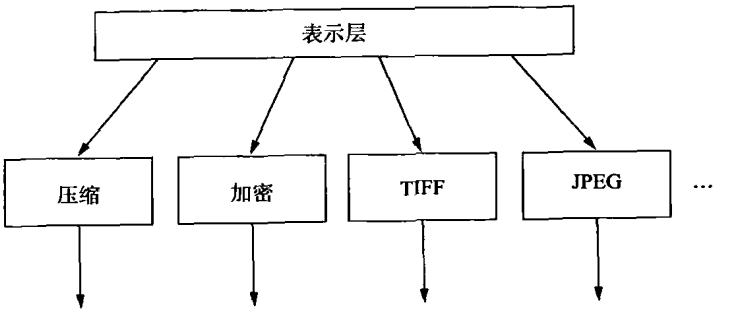


图 1-4 表示层将数据转变为不同标准的格式

3. 会话层（Session Layer）

会话层是 OSI 模型中的第五层，负责在两个应用程序之间建立连接，在传送数据的过程中保持连接并控制连接的释放。会话层的工作分为三个阶段：建立连接、数据传输、释放连接。在有些情况下还提供会话重新开始和恢复，以及完整会话的维持。会话结束时拆除路径并且使所有参数恢复到初始设置。

会话层协议在应用程序之间建立连接，进行会话控制，并协商、建立、维持或撤销通信通道。以下是会话层中的一些协议：

- 网络文件系统（NFS）；

- 结构化查询语言(SQL)；
- 远程过程调用(RPC)；
- 网络基本输入/输出系统协议(NetBIOS)。

会话层协议使得两个应用程序之间能以三种不同的模式通信：单向模式、半双工模式、全双工模式。

图 1-5 描述了一个会话的三个阶段。

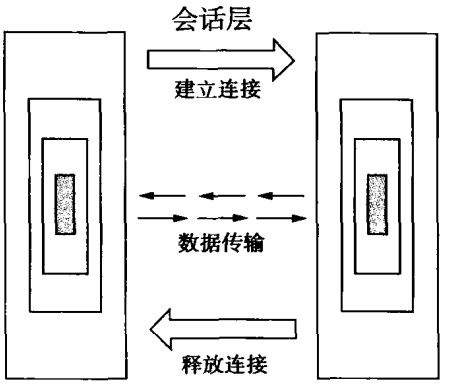


图 1-5　会话的三个阶段

4. 传输层(Transport Layer)

传输层是 OSI 模型中的第四层，负责建立两台计算机之间的连接。当两台计算机通信时，要确保一次发送信息量及数据完整性、一致性等，这有助于更可靠的数据传输、错误的检测与改正、流量控制，并优化了执行这些任务所需要的网络服务。传输层提供了端到端的数据传输服务并建立了两台通信计算机间的逻辑连接。传输层从许多不同的应用接收数据并把它们整合为一个流，以便在网络中正确地传送。

传输层的协议用于处理端对端传输和数据流分解。传输层中的协议有以下几项：

- 传输控制协议(TCP)；
- 用户数据报协议(UDP)；
- 安全套接层(SSL)；
- 序列封包交换(SPX)。

图 1-6 给出了传输层从不同应用程序中接收数据并整合为流的过程。

5. 网络层(Network Layer)

网络层是 OSI 模型中的第三层，它的主要任务是在数据包头中插入信息以便数据包被正确地编址和分配路由，并使数据通过路由到达正确的目的地。在网络中，可以有许多路由通往目标。网络层的协议必须确保数据包能走最好的路由。路由协议在这一层创建和维护它们的路由表。这些表是网络图，当一个数据包需要从一台计算机传送到另一台计算机上时，协议会检查网络表，在数据包头加入所需要的信息，然后送它上路。

网络层协议负责网际网络服务、寻址和路由。以下是网络层中的协议：

- 因特网协议(IP)；
- 因特网控制消息协议(ICMP)；