21st CENTURY
案例型规划教材

21世纪全国高职高专计算机案例型规划教材

# 计算机网络安全案例教程

主 编 陈 昶 杨艳春

北京大学出版社
PEKING UNIVERSITY PRESS

21 世纪全国高职高专计算机案例型规划教材

# 计算机网络安全案例教程

主　编　陈　昶　杨艳春
参　编　冯　亮　胡宝芳
　　刘素芳　张　宏

北京大学出版社
PEKING UNIVERSITY PRESS

## 内 容 简 介

本书从网络安全的概述引入，从网络安全的角度出发，全面介绍网络安全的基本理论以及网络安全方面的管理、配置和维护。全书共分为 11 章，主要内容包括计算机网络安全概述、黑客常用的系统攻击方法、网络防病毒、数据加密、防火墙技术、入侵检测技术、Windows 2000 的安全、Web 的安全性、虚拟专用网（VPN）技术、数据库系统安全、实验指导及综合实训，各章节内容都包括引例、教学目标、教学要求、正文、本章小结、练习题。

本书注重实用性，实例丰富典型，实验内容和案例融合在课程内容中，将理论知识与实践操作很好地结合起来，最后一章的“实验指导及综合实训”注重培养实践操作能力，并作为全书内容的一个综合实训。

本书可作为高职高专计算机、电子商务等相关专业学生的教材，也可作为技术参考书或培训教材。

**图书在版编目(CIP)数据**

计算机网络安全案例教程/陈昶，杨艳春主编. —北京：北京大学出版社，2008.8

(21 世纪全国高职高专计算机案例型规划教材)

ISBN 978-7-301-14084-0

Ⅰ. 计… Ⅱ. ①陈… ②杨… Ⅲ. 计算机网络—安全技术—高等学校：技术学校—教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2008)第 109901 号

**书　　名**：计算机网络安全案例教程

**著作责任者**：陈　昶　杨艳春　主编

**策 划 编 辑**：李彦红　王显超

**责 任 编 辑**：王显超

**标 准 书 号**：ISBN 978-7-301-14084-0/TP・0966

**出　版　者**：北京大学出版社

**地　　址**：北京市海淀区成府路 205 号　100871

**网　　址**：http://www.pup.cn　http://www.pup6.com

**电　　话**：邮购部 62752015　发行部 62750672　编辑部 62750667　出版部 62754962

**电 子 邮 箱**：pup_6@163.com

**印　刷　者**：北京宏伟双华印刷有限公司

**发　行　者**：北京大学出版社

**经　销　者**：新华书店

787mm×1092mm　16 开本　18.5 印张　420 千字

2008 年 8 月第 1 版　2008 年 8 月第 1 次印刷

**定　　价**：30.00 元

# 21世纪全国高职高专计算机案例型规划教材
# 专家编写指导委员会

# 信息技术的案例型教材建设

## (代丛书序)

刘瑞挺/文

北京大学出版社第六事业部在2005年组织编写了两套计算机教材，一套是《21世纪全国高职高专计算机系列实用规划教材》，截至2008年6月已经出版了80多种；另一套是《21世纪全国应用型本科计算机系列实用规划教材》，至今已出版了50多种。这些教材出版后，在全国高校引起热烈反响，可谓初战告捷。这使北京大学出版社的计算机教材市场规模迅速扩大，编辑队伍茁壮成长，经济效益明显增强，与各类高校师生的关系更加密切。

2007年10月北京大学出版社第六事业部在北京召开了“21世纪全国高职高专计算机案例型教材建设和教学研讨会”，2008年1月又在北京召开了“21世纪全国应用型本科计算机案例型教材建设和教学研讨会”。这两次会议为编写案例型教材做了深入的探讨和具体的部署，制定了详细的编写目的、丛书特色、内容要求和风格规范。在内容上强调面向应用、能力驱动、精选案例、严把质量；在风格上力求文字精练、脉络清晰、图表明快、版式新颖。这两次会议吹响了提高教材质量第二战役的进军号。

案例型教材真能提高教学的质量吗？

是的。著名法国哲学家、数学家勒内·笛卡儿(Rene Descartes，1596—1650)说得好：“由一个例子的考察，我们可以抽出一条规律。(From the consideration of an example we can form a rule.)”事实上，他发明的直角坐标系，正是通过生活实例而得到的灵感。据说是在1619年夏天，笛卡儿因病住进医院。中午他躺在病床上，苦苦思索一个数学问题时，忽然看到天花板上有一只苍蝇飞来飞去。当时天花板是用木条做成正方形的格子。笛卡儿发现，要说出这只苍蝇在天花板上的位置，只需说出苍蝇在天花板上的第几行和第几列。当苍蝇落在第四行、第五列的那个正方形时，可以用(4，5)来表示这个位置……由此他联想到可用类似的办法来描述一个点在平面上的位置。他高兴地跳下床，喊着“我找到了，找到了”，然而不小心把国际象棋撒了一地。当他的目光落到棋盘上时，又兴奋地一拍大腿：“对，对，就是这个图”。笛卡儿锲而不舍的毅力，苦思冥想的钻研，使他开创了解析几何的新纪元。千百年来，代数与几何，井水不犯河水。17世纪后，数学突飞猛进的发展，在很大程度上归功于笛卡儿坐标系和解析几何学的创立。

这个故事，听起来与阿基米德在浴池洗澡而发现浮力原理，牛顿在苹果树下遇到苹果落到头上而发现万有引力定律，确有异曲同工之妙。这就证明，一个好的例子往往能激发灵感，由特殊到一般，联想出普遍的规律，即所谓的“一叶知秋”、“见微知著”的意思。

回顾计算机发明的历史，每一台机器、每一颗芯片、每一种操作系统、每一类编程语言、每一个算法、每一套软件、每一款外部设备，无不像闪光的珍珠串在一起。每个案例都闪烁着智慧的火花，是创新思想不竭的源泉。在计算机科学技术领域，这样的案例就像大海岸边的贝壳，俯拾皆是。

事实上，案例研究(Case Study)是现代科学广泛使用的一种方法。Case包含的意义很广：包括Example例子，Instance事例、示例，Actual State实际状况，Circumstance情况、事件、境遇，甚至Project项目、工程等。

我们知道在计算机的科学术语中，很多是直接来自日常生活的。例如 Computer 一词早在 1646 年就出现于古代英文字典中，但当时它的意义不是“计算机”而是“计算工人”，即专门从事简单计算的工人。同理，Printer 当时也是“印刷工人”而不是“打印机”。正是由于这些“计算工人”和“印刷工人”常出现计算错误和印刷错误，才激发查尔斯·巴贝奇(Charles Babbage，1791—1871)设计了差分机和分析机，这是最早的专用计算机和通用计算机。这位英国剑桥大学数学教授、机械设计专家、经济学家和哲学家是国际公认的“计算机之父”。

20 世纪 40 年代，人们还用 Calculator 表示计算机器。到电子计算机出现后，才用 Computer 表示计算机。此外，硬件(Hardware)和软件(Software)来自销售人员。总线(Bus)就是公共汽车或大巴，故障和排除故障源自格瑞斯·霍普(Grace Hopper，1906—1992)发现的“飞蛾子”(Bug)和“抓蛾子”或“抓虫子”(Debug)。其他如鼠标、菜单……不胜枚举。至于哲学家进餐问题，理发师睡觉问题更是操作系统文化中脍炙人口的经典。

以计算机为核心的信息技术，从一开始就与应用紧密结合。例如，ENIAC 用于弹道曲线的计算，ARPANET 用于资源共享以及核战争时的可靠通信。即使是非常抽象的图灵机模型，也受到二战时图灵博士破译纳粹密码工作的影响。

在信息技术中，既有许多成功的案例，也有不少失败的案例；既有先成功而后失败的案例，也有先失败而后成功的案例。好好研究它们的成功经验和失败教训，对于编写案例型教材有重要的意义。

我国正在实现中华民族的伟大复兴，教育是民族振兴的基石。改革开放 30 年来，我国高等教育在数量上、规模上已有相当的发展。当前的重要任务是提高培养人才的质量，必须从学科知识的灌输转变为素质与能力的培养。应当指出，大学课堂在高新技术的武装下，利用 PPT 进行的“高速灌输”、“翻页宣科”有愈演愈烈的趋势，我们不能容忍用“技术”绑架教学，而是让教学工作乘信息技术的东风自由地飞翔。

本系列教材的编写，以学生就业所需的专业知识和操作技能为着眼点，在适度的基础知识与理论体系覆盖下，突出应用型、技能型教学的实用性和可操作性，强化案例教学。本套教材将会有机融入大量最新的示例、实例以及操作性较强的案例，力求提高教材的趣味性和实用性，打破传统教材自身知识框架的封闭性，强化实际操作的训练，使本系列教材做到“教师易教，学生乐学，技能实用”。有了广阔的应用背景，再造计算机案例型教材就有了基础。

我相信北京大学出版社在全国各地高校教师的积极支持下，精心设计，严格把关，一定能够建设出一批符合计算机应用型人才培养模式的、以案例型为创新点和兴奋点的精品教材，并且通过一体化设计、实现多种媒体有机结合的立体化教材，为各门计算机课程配齐电子教案、学习指导、习题解答、课程设计等辅导资料。让我们用锲而不舍的毅力，勤奋好学的钻研，向着共同的目标努力吧！

**刘瑞挺教授** 本系列教材编写指导委员会主任、全国高等院校计算机基础教育研究会副会长、中国计算机学会普及工作委员会顾问、教育部考试中心全国计算机应用技术证书考试委员会副主任、全国计算机等级考试顾问。曾任教育部理科计算机科学教学指导委员会委员、中国计算机学会教育培训委员会副主任。PC Magazine《个人电脑》总编辑、CHIP《新电脑》总顾问、清华大学《计算机教育》总策划。

# 前　言

目前，随着网络用户数的飞速增长，互联网在不断改变人们的工作、学习、生活及娱乐方式，给人们带来了极大的便利。但是，随着互联网的普及、互联网技术的不断更新发展，网络用户人数的增多使得人们面临另外一个困境：私人数据、重要的企业资源以及政府机密等信息被暴露在公共网络空间中，而互联网的开放性使得这些重要的信息很容易被获取。这些信息若是被黑客们通过不同类型的攻击而非法获取，后果将不堪设想。另一方面，计算机病毒的种类和数量也在迅猛增长，并借助网络传播的速度越来越快，危害面越来越广，其破坏也越来越大，早年的 CIH 病毒和不久前的“熊猫烧香”病毒，危害性大，影响面广。计算机网络病毒不仅严重影响当前的信息化建设与工作，而且威胁到信息化长远战略。因此，无论从个人角度还是企事业单位角度来说，网络安全越来越受到重视，而要加强网络安全，正是需要大量的熟悉网络安全方面的建设、配置与维护的技术人员。本书旨在介绍网络安全的各方面理论、黑客攻击及系统漏洞的原理及防范措施，并结合实验培养网络安全方面的人才。

根据高职高专院校的教学思想以及培养目标，通过调研社会上目前对网络安全方面人才的需求及技术要求，并结合作者多年从事网络管理、服务器安装及安全配置的经验，组织编写了这本教材。本书突出了网络安全管理与维护的培养目标，并参考了国际上权威的微软认证的课程。

本书是网络安全的入门教材。通过本书的学习，可以使学生了解网络安全的基本框架，网络安全的基本理论，以及计算机网络安全方面的管理、配置和维护，为学生今后进行网络管理、维护以及安全技术服务奠定基础。

本书注重实践的培养，将实验内容融合在平时授课的内容中，使理论联系实际。本书的内容按如下的思路进行安排。

在网络安全中，“攻与防”一直是矛盾的焦点，只有了解攻击的原理、方法，才能够更好地进行防范，攻与防的技术需要了解，但是在讲解攻的方面之前，要先给学生强调思想道德方面的教育，这点希望教师在授课时一定要注意，同时本书在讲解攻的方面时掌握一个度，以避免带来不好的影响。本书的重点是强调安全防范方面，因此本书首先讲述网络安全概论，强调网络安全方面的法律知识，再介绍黑客的原理、常用工具以及病毒的危害。本书的第 1 章为计算机网络安全概述，第 2 章介绍黑客常用的系统攻击方法，第 3 章介绍网络防病毒。

数据加密是信息安全的基础，也是网络安全和日常网络使用中必不可少的一部分，许多产品、操作系统中都有各种各样的加密技术存在，数据加密在信息安全中的地位非常重要。目前网络安全技术主要有防病毒、防火墙、入侵检测（IDS）、VPN 技术。因此本书第 4 章介绍数据加密技术，第 5 章介绍防火墙技术，第 6 章介绍入侵检测技术。

操作系统是最经常使用的平台，因此非常有必要介绍操作系统的安全性、安全配置与

管理以及 IIS 的安全。本书第 7 章介绍 Windows 2000 的安全，第 8 章介绍 Web 的安全性。

对于企业在网络安全应用方面，VPN 技术和数据库系统安全都应用很广泛。因此本书第 9 章介绍 VPN 技术，第 10 章介绍数据库系统安全，第 11 章为各章实验内容及综合实训。综合实训将全书实践内容进行综合，不仅能温故而知新，也希望读者通过综合实训能对网络安全技术方面的知识融会贯通。

本书共 11 章，课程的总体学时为 64～72 学时，各学校可以根据本校的教学大纲和实验条件对讲授内容、授课课时与实验课时进行适当的调整。

本书由系统分析师陈昶组织编写及统稿。其中第 1、2、3 章由杨艳春编写，第 4、5、9、11 章由陈昶编写，第 6 章由张宏编写，第 7 章由胡宝芳编写，第 8 章由刘素芳编写，第 10 章由冯亮编写。

本书提供了课后选择题、填空题的参考答案，书中提到的一些工具软件在 Internet 上都可以下载，并且为了教师教学方便，订购本教材的教师可以登录出版社网站下载电子教案。

由于计算机网络安全技术发展迅速，加上时间仓促，书中不妥之处在所难免，恳请广大读者批评指正。编者邮箱为 cc@mitu.cn。

编　者

2008 年 5 月

# 目　录


**第 1 章　计算机网络安全概述** ..... 1

1.1 信息安全简介 ..... 2
1.1.1 信息安全的发展历程 ..... 2
1.1.2 信息安全的 3 个最基本的原则 ..... 3
1.1.3 信息安全的知识体系 ..... 3
1.2 网络安全简介 ..... 4
1.2.1 网络安全的定义 ..... 4
1.2.2 网络安全案例 ..... 5
1.2.3 网络安全所涉及的内容 ..... 6
1.2.4 网络安全的特征 ..... 6
1.3 研究网络安全的必要性 ..... 7
1.4 网络安全相关法规 ..... 7
1.4.1 网络安全的相关政策法规 ..... 7
1.4.2 关于保密和网络安全管理的相关法规条例(摘录) ..... 8
本章小结 ..... 10
练习题 ..... 11

**第 2 章　黑客常用的系统攻击方法** ..... 12

2.1 黑客概述 ..... 13
2.1.1 黑客与骇客 ..... 13
2.1.2 著名黑客 ..... 14
2.1.3 黑客守则 ..... 16
2.1.4 黑客行为的发展趋势 ..... 16
2.2 网络扫描工具原理与使用 ..... 16
2.2.1 ping ..... 17
2.2.2 X-Scan ..... 18
2.2.3 nessus ..... 20
2.2.4 nmap ..... 21
2.3 网络监听原理与工具 ..... 21
2.3.1 网络监听的原理 ..... 21
2.3.2 网络监听工具 ..... 22
2.3.3 网络监听的防范 ..... 27
2.4 木马 ..... 28
2.4.1 什么是木马 ..... 28
2.4.2 木马的种类 ..... 28
2.4.3 木马系统的组成 ..... 29
2.4.4 木马攻击原理 ..... 29
2.4.5 木马的清除 ..... 34
2.5 拒绝服务攻击 ..... 35
2.5.1 DoS ..... 35
2.5.2 DDoS ..... 36
2.5.3 DRDoS ..... 38
2.6 缓冲区溢出 ..... 39
2.6.1 缓冲区溢出的概念和原理 ..... 39
2.6.2 缓冲区溢出漏洞攻击方式 ..... 39
2.6.3 缓冲区溢出的防患 ..... 40
本章小结 ..... 41
练习题 ..... 42

**第 3 章　网络防病毒** ..... 44

3.1 计算机病毒的基本概念 ..... 45
3.1.1 计算机病毒的由来 ..... 45
3.1.2 计算机病毒的定义 ..... 46
3.2 计算机病毒的特征 ..... 46
3.3 计算机病毒的分类 ..... 48
3.3.1 按照计算机病毒存在的媒体进行分类 ..... 48
3.3.2 按照计算机病毒传染的方法进行分类 ..... 48
3.3.3 按照病毒破坏的能力进行分类 ..... 49
3.3.4 按照病毒特有的算法进行分类 ..... 49
3.3.5 按照病毒名进行分类 ..... 50

3.4 计算机病毒的防治 ..... 53
3.4.1 常用的防御措施 ..... 53
3.4.2 常见的清除病毒的方法 ..... 54
3.5 防病毒软件 ..... 57
3.5.1 奇虎 360 安全卫士 ..... 57
3.5.2 卡巴斯基反病毒软件 ..... 59
3.6 网络病毒实例 ..... 65
3.6.1 ARP 病毒 ..... 65
3.6.2 “熊猫烧香”病毒 ..... 68
3.6.3 机器狗 ..... 69
3.6.4 磁碟机 ..... 70
本章小结 ..... 71
练习题 ..... 72
第 4 章 数据加密 ..... 74
4.1 概述 ..... 75
4.1.1 密码学的有关概念 ..... 76
4.1.2 传统的加密技术 ..... 76
4.1.3 换位密码技术 ..... 78
4.2 对称加密算法 ..... 79
4.2.1 DES 算法及其基本思想 ..... 79
4.2.2 DES 算法的安全性分析 ..... 88
4.3 公开密钥算法 ..... 89
4.3.1 RSA 算法及其基本思想 ..... 89
4.3.2 RSA 算法的安全性分析 ..... 90
4.4 数据加密技术的应用 ..... 91
4.4.1 报文鉴别和 MD5 算法 ..... 91
4.4.2 数字认证 ..... 92
4.4.3 安全技术协议 ..... 96
4.5 PGP 加密解密软件的使用 ..... 99
4.5.1 PGP 系统的基本工作原理 ..... 99
4.5.2 PGP 软件的安装和使用 ..... 101
本章小结 ..... 104
练习题 ..... 105
第 5 章 防火墙技术 ..... 107
5.1 防火墙的概述 ..... 109
5.1.1 防火墙的定义 ..... 109
5.1.2 防火墙的功能 ..... 110
5.1.3 防火墙的发展过程 ..... 111
5.2 防火墙实现技术原理 ..... 112
5.2.1 包过滤防火墙技术 ..... 112
5.2.2 代理防火墙技术 ..... 114
5.2.3 动态包过滤防火墙技术 ..... 115
5.2.4 自适应代理防火墙技术 ..... 116
5.3 防火墙体系结构 ..... 116
5.3.1 双重宿主主机体系结构 ..... 116
5.3.2 被屏蔽主机体系结构 ..... 117
5.3.3 被屏蔽子网体系结构 ..... 118
5.4 防火墙的应用 ..... 120
5.4.1 个人版防火墙的应用 ..... 120
5.4.2 代理服务器的应用 ..... 124
5.5 防火墙的性能和选购防火墙的注意事项 ..... 127
5.5.1 防火墙的性能 ..... 127
5.5.2 选购防火墙的注意事项 ..... 130
本章小结 ..... 132
练习题 ..... 132
第 6 章 入侵检测技术 ..... 135
6.1 入侵检测的概念与作用 ..... 136
6.1.1 入侵检测的相关概念 ..... 137
6.1.2 入侵检测的分类 ..... 138
6.1.3 入侵检测的作用 ..... 139
6.2 入侵检测原理 ..... 140
6.2.1 工作原理 ..... 140
6.2.2 系统模型 ..... 142
6.3 入侵检测的应用 ..... 143
6.3.1 IDS 的应用 ..... 143
6.3.2 IDS 的分析方式 ..... 144
6.3.3 IDS 部署实例 ..... 144
6.3.4 Snort 简介 ..... 145
6.3.5 发展趋势 ..... 150
本章小结 ..... 150
练习题 ..... 151

第 7 章　Windows 2000 的安全 ..... 152
7.1　Windows 2000 的安全特性 ..... 153
7.1.1　Windows 2000 产品的组成 ..... 153
7.1.2　Windows 2000 的安全机制 ..... 154
7.1.3　Windows 2000 的安全体系 ..... 155
7.2　Windows 2000 的安全配置 ..... 158
7.2.1　安全策略配置 ..... 158
7.2.2　文件保护 ..... 163
7.2.3　其他安全设置 ..... 166
7.3　Windows 2000 常用的系统进程和服务 ..... 169
7.3.1　Windows 2000 系统进程 ..... 169
7.3.2　Windows 2000 常用服务 ..... 172
7.4　Windows 2000 注册表 ..... 174
7.4.1　注册表的管理 ..... 174
7.4.2　注册表的键 ..... 175
7.4.3　直接修改注册表使系统更加安全的几个应用 ..... 177
本章小结 ..... 178
练习题 ..... 179
第 8 章　Web 的安全性 ..... 180
8.1　Web 安全性概述 ..... 182
8.1.1　Internet 安全隐患 ..... 182
8.1.2　Web 安全问题 ..... 183
8.2　Web 服务器的安全性 ..... 183
8.2.1　Web 服务器 3 层模式 ..... 183
8.2.2　Web 服务器存在的漏洞 ..... 183
8.2.3　Web 服务器的安全设置 ..... 184
8.3　脚本语言的安全性、SQL 注入 ..... 187
8.3.1　CGI 程序的安全性 ..... 187
8.3.2　SQL 注入 ..... 188
8.4　旁注 Web 综合检测程序 ..... 195
8.5　Web 浏览器的安全性 ..... 196
8.5.1　浏览器本身的漏洞 ..... 196
8.5.2　ActiveX 的安全漏洞 ..... 198
8.5.3　Cookie 的安全性设置 ..... 201
本章小结 ..... 203
练习题 ..... 203
第 9 章　VPN 技术 ..... 205
9.1　VPN 技术的概述 ..... 207
9.1.1　VPN 的概念 ..... 207
9.1.2　VPN 的基本功能 ..... 207
9.2　VPN 协议 ..... 209
9.2.1　VPN 安全技术 ..... 209
9.2.2　VPN 的隧道协议 ..... 209
9.2.3　IPSecVPN 系统的组成 ..... 213
9.3　VPN 的类型 ..... 215
9.3.1　按 VPN 的应用方式分类 ..... 215
9.3.2　按 VPN 的应用平台分类 ..... 215
9.3.3　按 VPN 的协议分类 ..... 216
9.3.4　按 VPN 的服务类型分类 ..... 216
9.3.5　按 VPN 的部署模式分类 ..... 217
9.4　SSL VPN 简介 ..... 217
9.4.1　SSL VPN 的安全技术 ..... 218
9.4.2　SSL VPN 的功能与特点 ..... 218
9.4.3　SSL VPN 的工作原理 ..... 219
9.4.4　SSL VPN 的应用模式及特点 ..... 219
9.5　VPN 应用 ..... 221
9.5.1　Microsoft 的解决方案 ..... 221
9.5.2　Windows 2003 服务器端配置 ..... 221
9.5.3　VPN 客户端连接配置 ..... 223
本章小结 ..... 225
练习题 ..... 226
第 10 章　数据库系统安全 ..... 228
10.1　数据库安全概述 ..... 230
10.1.1　数据库安全的概念 ..... 230
10.1.2　计算机系统安全模型 ..... 230
10.2　数据库安全技术 ..... 231
10.2.1　用户标识与鉴别 ..... 232
10.2.2　存取控制 ..... 233

10.2.3 数据加密 ..... 236
10.3 并发控制、封锁和可串行化 ..... 237
10.3.1 并发控制 ..... 237
10.3.2 封锁 ..... 238
10.3.3 活锁与死锁 ..... 240
10.3.4 可串行性 ..... 242
10.4 数据库备份与恢复 ..... 243
10.4.1 事务 ..... 243
10.4.2 数据库的备份 ..... 244
10.4.3 数据库恢复 ..... 246
10.5 数据库系统安全保护实例 ..... 247
10.5.1 数据库完全备份 ..... 247
10.5.2 数据库还原 ..... 248
本章小结 ..... 250
练习题 ..... 251
**第 11 章 实验指导及综合实训** ..... 252
11.1 实验指导 ..... 253
实验一 使用 sniffer 分析网络协议 ..... 253
实验二 扫描工具的使用及常用的网络命令 ..... 254
实验三 木马程序 ..... 254
实验四 DoS 与 DDoS 攻击 ..... 255
实验五 杀毒软件的安装及使用 ..... 255
实验六 上网访问各防病毒网站及“奇虎 360 安全卫士”的应用 ..... 256
实验七 病毒清除的综合应用 ..... 256
实验八 RSA 及 MD5 算法应用 ..... 257
实验九 PGP 软件的应用 ..... 257
实验十 天网防火墙的应用 ..... 258
实验十一 入侵检测系统 ..... 259
实验十二 Windows 2000 安全性配置 ..... 262
实验十三 Windows 2000 服务程序 ..... 264
实验十四 Web 程序安全性及 SQL 注入 ..... 266
实验十五 VPN 网络配置及应用 ..... 268
实验十六 数据库安全配置及备份与恢复 ..... 268
11.2 综合实训 ..... 271
**部分习题参考答案** ..... 279
**参考文献** ..... 281

# 第1章 计算机网络安全概述

**教学目标：**

通过本章的学习，学生应掌握信息安全的定义和基本原则；了解信息安全的发展历程；掌握网络安全的定义；掌握网络安全所涉及的内容；了解网络安全的相关法规。

**教学要求：**

| 知识要点 | 能力要求 | 相关知识 |
| --- | --- | --- |
| 信息安全与网络安全的关系 | 掌握 | 信息安全的定义，基本原则；网络安全的定义 |
| 网络安全所涉及的内容 | 掌握 | 网络攻击、网络防御、网络扫描、网络监听等 |
| 网络安全的相关法规 | 了解 | 国内外与网络安全相关的各项规定 |

**引例**

在使用网络的过程中可能会遇到下面几种现象。

(1) 一天下午下着大雨，突然一声巨响，学校的几部电话被雷电击坏，一台交换机也被击坏了，导致学校电话几小时不能与外界联系，几天不能访问因特网。

(2) 你有一台计算机，平时用来上上网，玩玩游戏，偶尔也敲点公文进去，你朋友有时也来你这里玩玩游戏什么的，有一天，你的朋友突然告诉你，他有你的上网账号和密码，你相信吗?

(3) 有一天你打开计算机进行工作，开始非常正常，但是过了一会，你忽然发现，刚刚保存好的文件突然不见了，或者计算机好像被人操纵了，接着系统突然崩溃了，这时，你明白究竟发生了什么事吗?

(4) 你打开邮箱，看到邮箱被塞满了垃圾邮件，使得邮箱空间所剩无几，更为糟糕的是如果你感到好奇，打开其中一封邮件时，计算机所安装的防病毒软件马上检测到你的计算机已经感染了病毒。

(5) 有一天，你的同学告诉你，在校园网中从他的计算机上能够查看到你计算机中的一些文件夹。

这些问题说明网络及网络上的信息面临着各种威胁，在方便与外界联系的背后存在着许多不安全因素。

案例思考题:

1. 试列举你所见过的或在你的周围发生的关于网络安全方面的问题。
2. 如何解决引例中所列举的这些问题?

## 1.1 信息安全简介

信息安全(InfoSec)是一门交叉学科，涉及多方面的理论和应用知识，除了数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学。

### 1.1.1 信息安全的发展历程

信息安全在其发展过程中经历了 3 个阶段。

1. 通信安全阶段

早在 20 世纪初期，通信技术还不发达，面对电话、电报、传真等信息交换过程中存在的安全问题，人们强调的主要是信息的保密性，对安全理论和技术的研究也只侧重于密码学，这一阶段的信息安全可以简单称为通信安全，即 COMSEC(Communication Security)。

2. 信息安全阶段

20 世纪 80 年代后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机和网络技术的应用进入了实用化和规模化阶段，人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的信息安全阶段，即 INFOSEC(Information Security)。

3. 信息保障阶段

20 世纪 90 年代开始，由于互联网技术的飞速发展，信息无论是对内还是对外都得到

了极大开放，由此产生的信息安全问题跨越了时间和空间，信息安全的焦点已经不仅仅是传统的保密性、完整性和可用性 3 个原则了，并衍生出了诸如抗否定性、可控性、真实性等其他原则，信息安全也转化为从整体角度考虑其体系建设的信息保障阶段，即 IA(Information Assurance)。信息保障的核心思想是对系统或数据的 4 个方面的要求：保护(Protect)、检测(Detect)、反应(React)和恢复(Restore)，即 PDRR，其结构如图 1.1 所示。

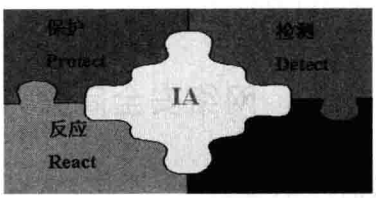


图 1.1　信息保障结构图

### 1.1.2　信息安全的 3 个最基本的原则

信息安全的 3 个最基本原则是保密性、完整性和可用性，即 C.I.A 三元组，如图 1.2 所示。

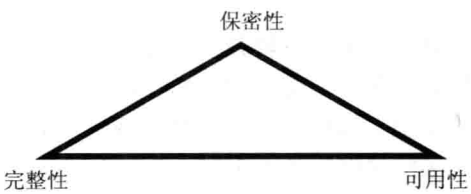


图 1.2　C.I.A 三元组

1. 保密性

保密性(Confidentiality)即保护信息的内容免遭有意的、无意的或未授权的泄漏。有许多方法可以损害保密性，如有意泄露公司的私有信息或滥用网络特权。

2. 完整性

完整性(Integrity)即确保未授权的人员或过程不能修改数据；已授权的人员或过程未经授权不能修改数据；数据的内部与外部相一致。

3. 可用性

可用性(Availability)即确保相关人员能够可靠地、及时地访问数据或其他计算机资源，即保证当需要时系统能启动和运行。

目前信息安全还有抗否定性原则，确保信息的不可抵赖性；可控性原则确保能控制信息的传播及内容等。另外，在电子商务领域还有另一种说法，网络安全的 4 大要素为：保密性、完整性、不可否认性、交易者身份确定性。

### 1.1.3　信息安全的知识体系

国际信息系统安全认证协会$(ISC)^2$ 组织世界信息安全专家编写了信息安全公共知识体系(Common Body of Knowledge，CBK)，总结了信息安全所涉及的 10 个最关键的知识领域，

这是目前最为系统和完整的信息安全行业体系标准，涵盖了安全管理、访问控制、网络安全、密码学、安全架构与模型、操作安全、应用和系统开发、灾难恢复、物理安全和法律伦理 10 个领域的问题。

网络安全是信息安全的一个重要领域，通过防止、检测和纠错的网络通信安全技术来维护网上信息的保密性、完整性、可用性。本教材主要围绕网络安全展开，在接下来的一节中首先对什么是网络安全进行简单的介绍。

## 1.2 网络安全简介

Internet 被设计成一个开放的网络，对任何一个具有网络连接和 ISP 账号的人都是开放的，因此它本身并没有多少能力保证网络上所传输信息的安全性，从安全角度看，Internet 天生就是不安全的。每个 Internet 用户都面临着一个新的挑战，即如何在允许被授权的人在使用它的同时保护敏感信息。

### 1.2.1 网络安全的定义

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。通常所说的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破坏、更改、泄露，系统连续、可靠、正常地运行，保持网络服务不中断。

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。网络安全的具体含义会随着“角度”的变化而变化。比如可以下面几个角度来讲。

1. 从用户(个人、企业等)的角度讲

用户希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私，对未授权的内容进行访问和破坏。

2. 从网络运行和管理者角度讲

管理者希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和控制等威胁，制止和防御网络黑客的攻击。

3. 从安全保密部门角度讲

安全保密部门希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，对社会产生危害，给国家造成巨大损失。

4. 从社会教育和意识形态角度讲

从社会教育和意识形态角度讲，网络上不健康的内容，会对社会的稳定和人类的发展

造成阻碍，因此必须对其进行控制。

### 1.2.2　网络安全案例

1. 国外典型的网络安全案例

1996 年初，据美国旧金山的计算机安全协会与联邦调查局的一次联合调查统计，有 53% 的企业受到过计算机病毒的侵害，42% 的企业的计算机系统在过去的 12 个月中被非法使用过。五角大楼的一个研究小组称美国一年中遭受的攻击就达 25 万次之多。

1996 年 12 月 29 日，黑客侵入美国空军的全球网网站并将其主页肆意改动，其中有关空军介绍、新闻发布等内容被替换成一段简短的黄色录像，且声称美国政府所说的一切都是谎言，迫使美国国防部一度关闭了其他 80 多个军方网站。

2002 年 2 月，Yahoo 网站、Amazon.com 和 ZDNet 遭遇分布式拒绝服务攻击。

2005 年，英国一名受雇于人的黑客贾斯明·辛，以 DoS 企图彻底弄垮对手的在线销售网点。他用计算机病毒控制上千台计算机，组成了傀儡网络，向两家在线销售体育服装的公司网站发起拒绝服务攻击，并窃取信息。

2005 年，韩国一个未满 17 岁的少年，使用“黑客软件”获取他人的密码之后，从受害人银行账户中转走 5000 万韩元(约 5 万美元)。

2007 年 6 月 21 日，美国国防部长亲口证实，五角大楼的一个非保密电子邮件系统一天前遭黑客入侵，迫使国防部 1500 个邮件账户被脱机停用，以至于美国众议员兰吉在国土安全委员会听证会上忧心忡忡地说：“这说明什么？这意味着恐怖分子或其他国家能入侵美国国土安全部的数据库，篡改姓名以便让他们能进入我国，而我们甚至根本不晓得他们已经得逞！”

2007 年 6 月 22 日，正当全球无数哈利·波特迷热切企盼着《哈利·波特》系列小说的大结局面市时，一名计算机黑客突然对外宣称，他已经成功闯入了出版商的计算机系统盗走了文稿，并且将部分内容贴上了因特网。

2007 年 9 月 2 日，美国宣布，美国政府招聘人员的专用网站遭黑客入侵，大约 14.6 万名用户的数据被盗取，以至于该网站随即被迫关闭。

2. 我国典型的网络安全案例

1996 年 2 月，刚开通不久的 CHINANET 受到攻击，且攻击得逞。

1997 年初，北京某 ISP 被黑客成功侵入，并在清华大学“水木清华”BBS 网站的“黑客与解密”讨论区张贴有关如何免费通过该 ISP 进入 Internet 的文章。

1997 年 4 月 23 日，美国德克萨斯州内查德逊地区西南贝尔互联网络公司的某个 PPP 用户侵入中国互联网络信息中心的服务器，破译该系统的 shutdown 账户，并把中国互联网信息中心的主页换成了一个笑嘻嘻的骷髅头。

1996 年初，CHINANET 受到某高校的一个研究生的攻击。

1996 年秋，北京某 ISP 和它的用户发生了一些矛盾，此用户便攻击该 ISP 的服务器，致使服务中断了数小时。

2003 年，冲击波(Blaster)至少攻击了全球 80%的 Windows 用户。