高职高专计算机类专业“十二五”规划教材

计算机网络安全与应用

JISUANJI WANGLUO ANQUAN YU YINGYONG

陈学平 主 编
李 明 副主编

化学工业出版社

高职高专计算机类专业“十二五”规划教材

计算机网络安全与应用

陈学平　主编
李　明　副主编

化学工业出版社
·北京·

本书从网络系统安全管理和应用的角度出发，重点介绍网络安全技术及其应用，各章在介绍网络安全技术后均配以相应的实践内容或应用实例，体现培养读者网络安全及管理技术的应用能力和实践操作技能的特色。本书对原理、技术难点的介绍适度，将理论知识和实际应用紧密地结合在一起，典型实例的应用性和可操作性强；章末配有练习题，便于学生学习和实践，内容安排合理，重点突出，文字简明，语言通俗易懂。

本书可作为普通高校计算机、通信、信息安全等专业的应用型本科、高职高专或成人教育学生的网络安全实践教材，也可作为网络管理人员、网络工程技术人员和信息安全管理人员的参考书。

图书在版编目（CIP）数据

计算机网络安全与应用/陈学平主编. —北京：化学工业出版社，2011.12
高职高专计算机类专业“十二五”规划教材
ISBN 978-7-122-12555-2

Ⅰ. 计… Ⅱ. 陈… Ⅲ. 计算机网络-安全技术-高等职业教育-教材 Ⅳ. TG393.08

中国版本图书馆 CIP 数据核字（2011）第 209077 号

责任编辑：王听讲　　文字编辑：吴开亮
责任校对：陈　静　　装帧设计：刘丽华

出版发行：化学工业出版社（北京市东城区青年湖南街 13 号　邮政编码 100011）
印　　装：大厂聚鑫印刷有限责任公司
787mm×1092mm　1/16　印张 18¼　字数　472　千字　　2012 年 1 月北京第 1 版第 1 次印刷

购书咨询：010-64518888（传真：010-64519686）　售后服务：010-64518899
网　　址：http: // www. cip. com. cn
凡购买本书，如有缺损质量问题，本社销售中心负责调换。

定　　价：35.00 元

前　言

本书注重实践技能的培养，以实验为依托，深入浅出地讲解理论知识，因此既可作为高职高专院校计算机及相关专业的教材，也可作为计算机网络安全类的技术参考书或培训教材。

本书从实战出发，以应用为目的，防范网络入侵为重点，是一本系统性、实战性、应用性较强的网络安全教程。本书摒弃了传统网络安全课程理论过多、实用性不强的缺点，紧密跟踪网络安全领域最新问题和技术运用，从应用的角度，系统讲述了网络安全所涉及的理论及技术。以阶段能力培养为目的，每个能力阶段为一个章节，通过实战演练，学生将具备综合运用所学的技术进行网络信息安全方面的实际工作能力。

本书首先系统介绍和分析了网络安全的定义、标准、模型，以及常见的网络安全威胁，然后从网络管理与安全防护入手，详细讲述和分析了入侵检测、数据加密、身份验证、防火墙以及无线网安全等多方面的理论与技术，同时结合现场工程应用，有机地将网络安全管理技术与主流系统软硬件结合，突出实践能力培养。本书安排了多个实验，便于读者亲身体验企业网络安全管理与防护的实际应用。

本书内容系统全面，结构清晰，注重实用性和应用性，主要特色如下。

1．本书力求做到理论与实践相结合，课程内容与实验相结合。通过实验，让读者加深对网络安全理论知识的理解，掌握网络安全管理的技能，以期达到活学活用的目的。

2．本书是一本内容丰富、特色鲜明、实用性强的信息安全理实一体化教材。本书包含了主流网络安全测试仪器的操作和使用，同时安排了无线网络安全的实训内容，对于丰富读者的网络安全实践经验，提高读者的网络安全管理水平，具有非常重要的意义。

3．本书每个实验都要求填写实训报告，便于读者对实验过程和结果进行分析和总结，并对所提出的问题进行深入思考。

4．本书从企业网络安全应用和专业角度出发，立足于“看得懂、学得会、用得上”，重点突出最新网络安全技术的可操作性和实用性，强化读者的网络安全防护能力。

我们将为使用本书的教师免费提供电子教案，需要者可以到化学工业出版社教学资源网站 http://www.cipedu.com.cn 免费下载使用。

本书由重庆电子工程职业学院陈学平担任主编，重庆电子工程职业学院李明担任副主编，陈学平编写了全书大纲，并统稿。本书第 1～3 章由李明编写，第 4 章由河南省漯河市漯河职业技术学院吴雪毅编写，第 5 章由洛阳市第一职业中等专业学校于志博编写，第 6 章由吉林电子信息职业技术学院战忠丽编写，第 7～13 章由陈学平编写。

本书在编写和出版过程中得到了化学工业出版社的支持与帮助，也得到了编者家人的支持，在此一并表示感谢。

编　者

2011 年 9 月

目 录

第 1 章 网络安全概论 …… 1
1.1 计算机网络安全的定义及内容 …… 1
1.1.1 计算机网络安全的定义 …… 1
1.1.2 典型安全问题 …… 2
1.2 网络信息安全目标 …… 3
1.3 网络信息安全基本功能 …… 4
1.4 网络安全的内容 …… 4
1.5 网络信息安全基本技术 …… 4
1.6 计算机网络安全的主要威胁及隐患 …… 6
1.6.1 网络安全的主要威胁 …… 6
1.6.2 计算机网络安全的技术隐患 …… 7
1.7 网络安全的现状及发展趋势 …… 9
1.7.1 网络安全现状 …… 9
1.7.2 网络安全的新趋势 …… 9
1.8 网络安全产品 …… 9
1.8.1 目前国内市场的主要网络安全产品厂商 …… 9
1.8.2 网络安全市场态势 …… 11
本章小结 …… 12
练习 …… 12
第 2 章 安全的基本元素 …… 13
2.1 引言 …… 13
2.2 安全的基本元素 …… 13
2.3 安全策略 …… 13
2.3.1 系统分类 …… 14
2.3.2 如何判断系统的安全级别 …… 14
2.3.3 资源优先级划分 …… 15
2.3.4 指定危险因数 …… 15
2.3.5 定义可接受和不可接受活动 …… 15
2.3.6 定义教育标准 …… 16
2.3.7 谁负责管理策略 …… 16
2.4 加密 …… 17
2.5 认证 …… 17
2.6 特殊的认证技术 …… 18
2.7 访问控制 …… 19
2.7.1 访问控制列表 …… 19
2.7.2 执行控制列表 …… 20
2.8 审计 …… 20
2.8.1 被动式和主动式审计 …… 20
2.8.2 安全的权衡考虑和缺点 …… 20
本章小结 …… 20
练习 …… 20
第 3 章 应用加密 …… 21
3.1 引言 …… 21
3.2 加密服务 …… 21
3.3 加密强度 …… 21
3.4 建立信任关系 …… 22
3.5 对称加密 …… 23
3.6 对称加密算法 …… 23
3.6.1 数据加密标准 …… 23
3.6.2 Triple DES …… 24
3.6.3 RSA 安全公司的对称算法 …… 24
3.6.4 Blowfish and Twofish …… 24
3.6.5 Skiack and MARS …… 25
3.6.6 高级加密标准 …… 25
3.7 非对称加密 …… 25
3.8 Hash 加密 …… 25
3.8.1 Hash 算法 …… 25
3.8.2 安全 Hash 算法（SHA） …… 26
3.9 签名 …… 26
3.10 应用加密的执行过程 …… 27
3.10.1 电子邮件加密 …… 27
3.10.2 PGP 加密电子邮件的过程 …… 31
3.10.3 PGP 加密分析 …… 31
3.10.4 PGP 在 E-mail 中的应用 …… 35
3.10.5 文件加密和 Web 服务器加密 …… 35
3.11 虚拟专用网络（VPN）协议 …… 36
3.11.1 PPTP 与 IPSec 在安全性上的比较 …… 36
3.11.2 保护与服务 …… 37
3.12 公钥体系结构（PKI） …… 37
3.12.1 PKI 标准 …… 37
3.12.2 PKI 术语 …… 37
本章小结 …… 38
练习 …… 38
第 4 章 网络攻击原理与常用方法 …… 39
4.1 网络攻击概述 …… 39
4.1.1 网络攻击概念 …… 39
4.1.2 网络攻击技术发展演变 …… 40
4.2 网络攻击一般过程 …… 41
4.2.1 隐藏攻击源 …… 41
4.2.2 收集攻击目标信息 …… 42
4.2.3 挖掘漏洞信息 …… 42

4.2.4 获取目标访问权限 …… 43
4.2.5 隐蔽攻击行为 …… 43
4.2.6 实施攻击 …… 43
4.2.7 开辟后门 …… 44
4.2.8 清除攻击痕迹 …… 44
4.3 网络攻击常见技术方法 …… 44
4.3.1 端口扫描 …… 44
4.3.2 口令破解 …… 45
4.3.3 缓冲区溢出 …… 46
4.3.4 网络蠕虫 …… 46
4.3.5 网站假冒 …… 47
4.3.6 拒绝服务 …… 47
4.3.7 网络嗅探 …… 48
4.3.8 SQL 注入攻击 …… 49
4.3.9 社交工程方法 …… 49
4.3.10 电子监听技术 …… 49
4.3.11 会话劫持 …… 49
4.3.12 漏洞扫描 …… 49
4.3.13 代理技术 …… 50
4.3.14 数据加密技术 …… 50
4.4 扫描类软件 …… 50
4.4.1 黑客常用软件 …… 50
4.4.2 远程监控类软件 …… 51
4.4.3 系统攻击和密码破解 …… 51
4.4.4 监听类软件 …… 52
4.5 网络攻击案例 …… 52
4.5.1 Nmap 扫描 …… 52
4.5.2 DDoS 攻击 …… 54
4.5.3 W32.Blaster.Worm …… 54
4.5.4 网络嗅探攻击 …… 55
本章小结 …… 55
练习 …… 55
第 5 章 操作系统的安全机制 …… 56
5.1 操作系统安全概述 …… 56
5.1.1 操作系统的安全控制 …… 56
5.1.2 存储器的保护 …… 57
5.1.3 操作系统的安全模型 …… 58
5.1.4 安全操作系统的设计原则 …… 59
5.2 Windows 2003 的安全机制 …… 59
5.2.1 身份验证机制 …… 59
5.2.2 访问控制机制 …… 60
5.2.3 审核策略机制 …… 60
5.2.4 IP 安全策略机制 …… 60
5.2.5 防火墙机制 …… 61
5.3 常见服务的安全机制 …… 61
5.3.1 加密机制 …… 61
5.3.2 访问控制机制 …… 61
5.3.3 数据完整性机制 …… 61
5.3.4 数字签名机制 …… 62
5.3.5 交换鉴别机制 …… 62
5.3.6 公证机制 …… 62
5.3.7 流量填充机制 …… 62
5.3.8 路由控制机制 …… 62
5.4 Windows 操作系统安全配置 …… 63
5.4.1 基本知识 …… 63
5.4.2 中级设置 …… 65
5.4.3 高级设置 …… 70
5.4.4 Windows 操作系统安装注意事项 …… 79
本章小结 …… 80
练习 …… 80
第 6 章 访问控制与防火墙技术 …… 81
6.1 访问控制 …… 81
6.1.1 访问控制的定义 …… 81
6.1.2 基本目标 …… 81
6.1.3 访问控制的作用 …… 81
6.1.4 主体、客体和授权 …… 81
6.1.5 访问控制模型基本组成 …… 82
6.1.6 访问控制策略 …… 82
6.1.7 访问控制机制 …… 84
6.1.8 其他的访问控制 …… 84
6.2 防火墙 …… 84
6.2.1 防火墙的定义 …… 85
6.2.2 防火墙的位置 …… 86
6.2.3 防火墙的理论特性和实际功能 …… 88
6.2.4 防火墙的规则 …… 94
6.2.5 防火墙的分类 …… 96
6.2.6 防火墙的好处 …… 99
6.2.7 防火墙的不足 …… 99
6.2.8 相关标准 …… 102
6.2.9 防火墙的功能要求 …… 105
本章小结 …… 107
练习 …… 107
第 7 章 入侵检测技术 …… 108
7.1 入侵检测概述 …… 108
7.2 入侵检测技术 …… 109
7.2.1 误用入侵检测 …… 109
7.2.2 异常入侵检测 …… 109
7.3 入侵检测产品 …… 110
7.3.1 安氏领信 LinkTrust …… 110
7.3.2 Enterasys Networks 公司 Dragon Sensor …… 111
7.3.3 启明星辰天阗入侵检测系统 …… 111
7.3.4 中科网威天眼入侵检测系统 …… 111
7.3.5 中联绿盟冰之眼入侵检测系统 …… 111

7.4 入侵检测产品的选择 …… 112
本章小结 …… 113
练习 …… 113
第 8 章 计算机病毒及预防 …… 114
8.1 计算机病毒及特性 …… 114
8.1.1 什么是计算机病毒 …… 114
8.1.2 计算机病毒的特性 …… 114
8.2 计算机病毒的类型及其危害 …… 115
8.2.1 计算机病毒的类型 …… 115
8.2.2 计算机网络传播病毒 …… 116
8.2.3 计算机病毒对系统的危害 …… 116
8.3 计算机病毒的结构及其作用机制 …… 117
8.3.1 计算机病毒的结构 …… 117
8.3.2 计算机病毒作用机制 …… 118
8.4 计算机病毒的攻击 …… 118
8.4.1 ARP 攻击 …… 118
8.4.2 内网 IP 欺骗 …… 119
8.4.3 内网攻击 …… 119
8.4.4 外网流量攻击 …… 119
8.5 计算机病毒的危害 …… 119
8.5.1 病毒激发对计算机数据信息的直接破坏作用 …… 119
8.5.2 占用磁盘空间和对信息的破坏 …… 120
8.5.3 抢占系统资源 …… 120
8.5.4 影响计算机运行速度 …… 120
8.5.5 计算机病毒错误与不可预见的危害 …… 120
8.5.6 计算机病毒的兼容性对系统运行的影响 …… 121
8.5.7 计算机病毒给用户造成严重的心理压力 …… 121
8.6 计算机病毒的防治 …… 121
8.6.1 发现病毒 …… 121
8.6.2 简单杀灭病毒 …… 125
8.7 计算机安全简单攻略 …… 125
8.8 几种常见病毒的发现与防治 …… 127
8.8.1 文件共享 …… 127
8.8.2 U 盘病毒 …… 127
8.8.3 木马病毒 …… 130
8.8.4 蠕虫病毒 …… 130
8.8.5 QQ 病毒 …… 132
8.8.6 网页病毒 …… 132
8.8.7 ARP 病毒 …… 133
8.8.8 磁碟机病毒 …… 134
8.9 几种常见的杀毒软件简介 …… 135
本章小结 …… 136
练习 …… 137
第 9 章 黑客攻击及其防范 …… 138
9.1 黑客及其危害 …… 138
9.1.1 认识黑客 …… 138
9.1.2 黑客类型 …… 139
9.1.3 黑客产生的社会原因 …… 140
9.1.4 黑客行为的危害 …… 140
9.2 黑客活动特点及其常用的手段 …… 144
9.2.1 黑客的行为特征 …… 144
9.2.2 黑客犯罪的特点 …… 145
9.2.3 黑客攻击的过程 …… 145
9.2.4 黑客的攻击方式 …… 146
9.2.5 黑客常用的攻击手段 …… 147
9.3 黑客的防范 …… 151
9.3.1 使用高安全级别的操作系统 …… 151
9.3.2 限制系统功能 …… 152
9.3.3 发现系统漏洞并及时堵住系统漏洞 …… 152
9.3.4 身份认证 …… 152
9.3.5 防火墙技术 …… 153
9.3.6 数据加密技术 …… 154
9.3.7 计算机病毒防治 …… 155
9.3.8 攻击检测技术 …… 155
9.3.9 核心软件国产化 …… 157
9.3.10 加强内部管理 …… 157
9.3.11 备份、清除与物理安全 …… 158
9.3.12 区别对待黑客 …… 158
本章小结 …… 160
练习 …… 160
第 10 章 嗅探器 …… 161
10.1 嗅探器原理及危害 …… 161
10.1.1 广播式网络原理 …… 161
10.1.2 点对点式网络原理 …… 162
10.1.3 网卡原理 …… 162
10.1.4 网络数据包原理 …… 162
10.1.5 嗅探器的 HUB 原理 …… 163
10.1.6 嗅探器的危害 …… 164
10.1.7 嗅探器关心的内容 …… 164
10.2 几款简单嗅探器 …… 165
10.2.1 小巧玲珑的 X-Sniffer …… 165
10.2.2 ARPSniffer 的使用方法 …… 165
10.3 Sniffer PRO …… 167
10.3.1 Sniffer 软件简介 …… 167
10.3.2 功能简介 …… 167
10.3.3 报文捕获解析 …… 167
10.3.4 报文放送 …… 171
10.3.5 网络监视功能 …… 172
10.3.6 数据报文解码详解 …… 174

10.4 嗅探器的发现 …… 184
10.5 嗅探器的防范 …… 184
本章小结 …… 185
练习 …… 185
第 11 章 无线局域网安全 …… 186
11.1 无线局域网的安全技术 …… 186
11.2 无线局域网安全防范措施 …… 187
11.3 无线路由器的安全设置 …… 188
11.3.1 无线路由器的初始设置 …… 188
11.3.2 无线路由器的安全设置 …… 193
本章小结 …… 202
练习 …… 202
第 12 章 信息安全风险管理与评估 …… 203
12.1 风险管理概述 …… 203
12.2 风险管理的过程 …… 203
12.2.1 风险识别 …… 204
12.2.2 风险分析 …… 204
12.2.3 风险计划 …… 205
12.2.4 风险跟踪 …… 205
12.2.5 风险应对 …… 205
12.3 风险评估概述 …… 205
12.3.1 风险评估简介 …… 205
12.3.2 主要风险评估方法 …… 207
12.4 国内外风险评估标准 …… 208
12.4.1 美国信息安全评估标准 …… 209
12.4.2 我国信息安全评估标准 …… 209
本章小结 …… 210
练习 …… 210
第 13 章 实验 …… 211
13.1 实验 1——PGP 邮件加密实验 …… 211
13.1.1 实验目的 …… 211
13.1.2 实验要求 …… 211
13.1.3 实验原理 …… 211
13.1.4 实验步骤 …… 213
13.2 实验 2——网络扫描实验 …… 226
13.2.1 实验目的 …… 226
13.2.2 实验环境 …… 226
13.2.3 实验原理 …… 227
13.2.4 实验步骤 …… 227
13.2.5 思考 …… 230
13.3 实验 3——网络端口扫描 …… 230
13.3.1 实验目的 …… 230
13.3.2 实验原理 …… 230
13.3.3 实验环境 …… 232
13.3.4 实验内容和步骤 …… 232
13.3.5 实验心得体会 …… 236
13.4 实验 4——网络嗅探实验 …… 236
13.4.1 实验目的 …… 236
13.4.2 实验要求 …… 236
13.4.3 实验仪器设备和材料清单 …… 236
13.4.4 实验内容 …… 236
13.4.5 实验步骤 …… 236
13.4.6 思考题 …… 239
13.5 实验 5——数据库的安全性 …… 240
13.5.1 实验目的 …… 240
13.6 实验 6——Windows 网络安全和管理配置实验 …… 248
13.6.1 实验目的 …… 248
13.6.2 实验内容和步骤 …… 248
13.6.3 实验要求 …… 248
13.6.4 相关知识 …… 248
13.7 实验 7——LC5 帐户口令破解 …… 251
13.7.1 实验目的 …… 251
13.7.2 实验环境 …… 251
13.7.3 实例 …… 251
13.8 实验 8——拒绝服务攻击的实现 …… 257
13.8.1 实验目的 …… 257
13.8.2 实验内容 …… 257
13.9 实验 9——数据恢复 …… 258
13.9.1 实验类型 …… 258
13.9.2 实验目的 …… 258
13.9.3 实验描述 …… 258
13.9.4 实验要求 …… 258
13.9.5 相关知识 …… 259
13.9.6 实验设备 …… 260
13.9.7 实验步骤 …… 260
13.9.8 实验思考 …… 262
13.10 实验 10——ISA 防火墙的配置 …… 262
13.10.1 实验目的 …… 262
13.10.2 实验内容 …… 263
13.10.3 实验设备 …… 263
13.10.4 实验原理 …… 263
13.10.5 实验步骤 …… 271
13.10.6 实验结果 …… 275
13.11 实验 11——使用 Sniffer 工具分析以太网帧和 IP 数据报 …… 275
13.11.1 实验目的 …… 275
13.11.2 实验原理 …… 275
13.11.3 实验环境 …… 276
13.11.4 实验内容和步骤 …… 276
13.11.5 实验结论 …… 280
参考文献 …… 281

第 1 章　网络安全概论

【本章要点】

① 了解网络信息安全现状和问题。
② 理解网络信息安全基本属性概念。
③ 理解网络信息安全基本功能。
④ 掌握网络信息安全基本技术。
⑤ 掌握典型网络信息安全威胁。
⑥ 掌握网络安全管控概念、方法与流程。
⑦ 能够从互联网上收集到网络安全信息，特别是漏洞信息。

网络技术和其他信息技术正在改变传统的生产、经营和生活方式，成为新的经济增长点。

信息网络国际化、社会化、开放化、个人化的特点，使国家的“信息边疆”不断延伸，甚至延伸到了每一个上网者个人。国际上围绕信息的获取、使用和控制的竞争愈演愈烈，网络安全正在成为维护国家安全、保持社会稳定、影响长远利益的一个焦点。作为一个亟待解决的重大关键问题，网络信息安全不但是发挥信息革命带来的高效率、高效益的有力保证，而且是对抗信息霸权主义、抵御信息侵略的重要屏障。网络信息安全保障能力是 21 世纪综合国力、经济竞争实力和生存能力的重要组成部分，是 21 世纪世界各国奋力攀登的制高点。

网络信息安全领域是一个综合、交叉的学科领域，它综合利用数学、物理、生化、信息技术和计算机技术等诸多学科的长期知识积累和最新发展成果，提出了系统的（而不是个别的）、完整的（而不是零碎的）、协同的（而不是孤立的）解决信息安全的方案。同时，它的研究和发展又将刺激、推动和促进相关学科的研究和发展。

网络信息安全的概念在 20 世纪经历了一个漫长的历史阶段，20 世纪 90 年代以来得到了深化，从信息的保密性（保证信息不泄漏给未经授权的人）拓展到信息的完整性（防止信息被未经授权的篡改，保证真实的信息从真实的信源无失真地到达真实的信宿）、信息的可用性（保证信息及信息系统确实为授权使用者所用，防止由于计算机病毒或其他人为因素造成的系统拒绝服务，或为敌手可用）、信息的可控性（对信息及信息系统实施安全监控管理）、信息的不可否认性（保证信息行为人不能否认自己的行为）等。信息安全需要“攻、防、测、控、管、评”等多方面的基础理论和实施技术。

1.1　计算机网络安全的定义及内容

1.1.1　计算机网络安全的定义

网络安全从其本质上来讲就是网络上的信息安全。它涉及的领域相当广泛。这是因为在目前的公用通信网络中存在各种各样的安全漏洞和威胁。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，都是网络安全所要研究的领域。下面给出网络安全的一个通用定义。

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，不因偶然或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

从用户（个人、企业等）的角度来说，他们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、抵赖等手段对用户的利益和隐私造成损害和侵犯，同时也希望当用户的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。

从网络运行和管理者的角度来说，他们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非法控制等威胁，制止和防御网络“黑客”的攻击。

对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免其通过网络泄露，避免由于这类信息的泄密对社会产生危害，对国家造成巨大的经济损失。

从社会教育和意识形态角度来讲，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，必须对其进行控制。

因此，网络安全在不同的环境和应用会得到不同的解释。

① 运行系统安全　即保证信息处理和传输系统的安全。包括计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的安全性考虑，硬件系统的可靠安全运行，计算机操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。它侧重于保证系统正常的运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁泄漏产生信息泄露，干扰他人（或受他人干扰），本质上是保护系统的合法操作和正常运行。

② 网络上系统信息的安全　包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密。

③ 网络上信息传播的安全　即信息传播后果的安全。包括信息过滤，不良信息的过滤等。它侧重于防止和控制非法、有害的信息进行传播后的后果，避免公用通信网络上大量自由传输的信息失控，本质上是维护道德、法律或国家利益。

④ 网络上信息内容的安全　即我们讨论的狭义的“信息安全”。它侧重于保护信息的保密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为，本质上是保护用户的利益和隐私。

显而易见，网络安全与其所保护的信息对象有关，本质是在信息的安全期内保证其在网络上流动时或者静态存放时不被非授权用户非法访问，但授权用户却可以访问。显然，网络安全、信息安全和系统安全的研究领域是相互交叉和紧密相连的。下面给出本书所研究和讨论的网络安全的含义。

网络安全的含义是通过各种计算机、网络、密码技术和信息安全技术，保护在公用通信网络中传输、交换和存储的信息的机密性、完整性和真实性，并对信息的传播及内容具有控制能力。网络安全的结构层次包括：物理安全、安全控制和安全服务。

1.1.2　典型安全问题

分析当前的网络安全，主要有 10 个方面的问题急需要解决，分别叙述如下。

① 信息应用系统与网络日益紧密，人们对网络依赖性增强，因而对网络安全影响范围日益扩大，建立可信的网络信息环境成为一个迫切的需求。

② 网络系统中安全漏洞日益增多，不仅技术上有漏洞，而且管理上也有漏洞。

③ 恶意代码危害性高。恶意代码通过网络途径广泛扩散，其影响越来越大。

④ 网络攻击技术日趋复杂，而攻击操作易于实施，攻击工具广为流行。

⑤ 网络安全建设缺乏规范操作，常常采取“亡羊补牢”的做法，导致信息安全共享难度增加，留下安全隐患。

⑥ 网络系统存在种类繁多的安全认证方式，一方面使得用户使用不方便，另一方面增加了安全管理工作难度。

⑦ 国内信息化技术严重依赖国外，从硬件到软件都不同程度地受制于人。

⑧ 网络系统中软硬件产品单一，易造成大规模网络安全事件发生，特别是网络蠕虫安全事件。

⑨ 网络安全建设涉及人员众多，安全和易用性难以平衡。

⑩ 网络安全管理问题依然是一个难题，主要如下。

- 用户信息安全防范意识。例如选取弱口令，使得从远程直接控制主机。
- 网络服务配置不当，开放过多网络服务。例如，网络边界没有过滤掉恶意数据包或切断网络连接，允许外部网络的主机直接 ping 内部网主机，允许建立空连接。
- 安装有漏洞的软件包。
- 默认配置。例如网络设备的口令直接使用厂家默认配置。
- 网络系统中软件不打补丁或补丁不全。
- 网络安全敏感信息泄露。例如 DNS 服务信息泄露。
- 网络安全防范缺乏体系。
- 网络信息资产不明，缺乏分类分级处理。
- 网络安全管理信息单一，缺乏统一分析与管理平台。
- 重技术，轻管理。例如没有明确的安全管理策略、安全组织、安全规范。

1.2　网络信息安全目标

网络信息安全目标就是保证网络系统资源的 5 个基本安全属性得以实现，即机密性、完整性、可用性、抗抵赖性、可控性。通俗地说，安全的目标就是实现网络信息的可用、可控、可信。

1．机密性

网络机密性是指网上资源不泄露给非授权的用户、实体或程序，能够防止网上用户非授权获取网上资源。例如网络系统上传递的信息有些属于重要安全信息，若一旦攻击者通过监听手段获取到，就有可能危及网络系统整体安全，例如网络管理帐号口令信息泄露将会导致网络设备失控。

2．完整性

完整性是指网上信息或系统未经授权不能进行更改的特性。例如，网上电子邮件信息在存储或传输过程中保持不被删除、修改、伪造、插入等。

3．可用性

可用性是指授权的网上用户能够按照系统所提供的途径访问网上资源。例如，网站服务能够防止拒绝服务攻击。

4．抗抵赖性

抗抵赖性是指防止网上实体否认其已经发生的网上行为。这一特性保证了网上信息的来源及信息发布者的真实可信。例如，通过网络审计，可以记录访问者在网络系统中的活动。

5．可控性

可控性是指网络具有可管理性，能够根据授权对网络进行监测和控制，使得管理者有效

地控制网络用户的行为和网上信息的传播。

1.3 网络信息安全基本功能

要实现网络安全的5个基本目标，应具备防御、监测、应急、恢复这几个基本功能。下面分别简要叙述。

1．网络安全防御

网络安全防御是指采取各种手段和措施，使得网络系统具备阻止、抵御各种已知网络威胁的功能。

2．网络安全监测

网络安全监测是指采取各种手段和措施，检测、发现各种已知或未知的网络威胁的功能。

3．网络安全应急

网络安全应急是指采取各种手段和措施，针对网络系统中的突发事件，具备及时响应、处置网络攻击威胁的功能。

4．网络安全恢复

网络安全恢复是指采取各种手段和措施，针对已经发生的网络灾害事件，具备恢复网络系统运行的功能。

1.4 网络安全的内容

网络安全的内容大致上包括：网络实体安全、软件安全、数据安全和网络安全管理4个方面，如图1-1所示。

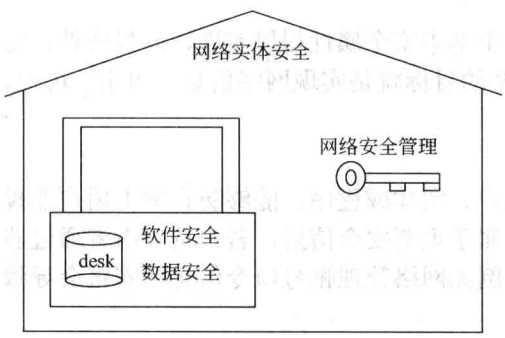

图1-1 网络安全的内容

1．网络实体安全

如计算机机房的物理条件、物理环境及设施的安全，计算机硬件、附属设备及网络传输线路的安装及配置等。

2．软件安全

如保护网络系统不被非法侵入，系统软件与应用软件不被非法复制、不受病毒的侵害等。

3．网络中的数据安全

如保护网络信息数据的安全、数据库系统的安全，保护其不被非法存取，保证其完整、一致等。

4．网络安全管理

如运行时突发事件的安全处理等，包括采取计算机安全技术，建立安全管理制度，开展安全审计，进行风险分析等内容。

1.5 网络信息安全基本技术

1．网络物理安全

物理安全也称实体安全，是指包括环境、设备和记录介质在内的所有支持网络系统运行的硬件的总体安全，是网络系统安全、可靠、不间断运行的基本保证。物理安全需求主要

如下。

① 环境安全　对系统所在环境的安全保护，如区域保护和灾难保护。

② 设备安全　网络物理实体做到防范各种灾害，如防火、防雷、防水。物理实体能够抵抗各种物理临近攻击。

③ 存储介质安全　包括存储数据的安全及存储介质本身的安全。

2．网络认证

网络认证是实现网络资源访问控制的前提和依据，是有效保护网络管理对象重要的技术方法。网络认证的作用是标识鉴别网络资源访问者的身份的真实性，防止用户假冒身份访问网络资源。

3．网络访问控制

网络访问控制是有效保护网络管理对象，使其免受威胁的关键技术方法。其目标主要有两个。

① 限制非法用户获取或使用网络资源。

② 防止合法用户滥用权限，越权访问网络资源。

在网络系统中，存在着各种价值的网络资源。这些网络资源一旦受到危害，都将不同程度地影响到网络系统安全。通过对这些网上资源访问控制，可以限制其所受到的威胁，从而保障网络正常运行。例如，在因特网中，采用防火墙可以阻止来自外部网的不必要的访问请求，从而可以避免内部网受到潜在的攻击威胁。

4．网络安全保密

在网络系统中，承载着各种各样的信息，这些信息泄露将会造成不同程度的安全影响，特别是网上用户个人信息、网络管理控制信息。网络安全保密的目的就是防止非授权的用户访问网上信息或网络设备。为此，重要的网络物理实体能够采用辐射干扰机技术，防止电磁辐射泄露机密信息。

5．网络安全监测

网络系统面临着不同级别威胁，网络安全运行是一项复杂工作。网络安全监测的作用在于发现综合网系统的入侵活动和检查安全保护措施的有效性，以便及时报警给网络安全管理员，对入侵者采取有效措施，阻止危害扩散和调整安全策略。

6．网络漏洞评估

网络系统存在的安全漏洞和操作系统的安全漏洞等，是黑客等入侵者攻击屡屡得手的重要原因。入侵者通常都是通过一些程序来探测网络系统中存在的安全漏洞，然后通过发现的安全漏洞，采取相应技术进行攻击。因此，网络系统中应需配备弱点或漏洞扫描系统，用以检测网络中是否存在安全漏洞，以便网络安全管理员根据漏洞检测报告，制定合适的漏洞管理方法。

7．恶意代码防护

网络是病毒、木马等恶意代码传播最好、最快的途径之一。恶意代码可以通过网上文件下载、电子邮件、网页、文件共享等传播方式进入个人计算机或服务器。由于恶意代码危害性极大并且传播极为迅速，网络中一旦有一台主机感染恶意代码，则恶意代码就完全有可能在极短的时间内迅速扩散，传播到网络上的其他主机，可能造成信息泄露、文件丢失、计算机死机等严重后果。因此，防范恶意代码是网络系统的必不可少的安全需求。

8．应急响应

网络系统所遇到的安全威胁往往难以预测，虽然采取一些网络安全防范措施，但是由于人为或技术上的缺陷，网络安全事件仍然不可避免地会发生。既然网络安全事件不能完全消

除，则必须采取一些措施来保障在出现意外情况下，恢复网络系统的正常运转。

9．网络安全体系

网络安全的实现不仅取决于某项技术，而是依赖于一个网络信息安全体系的建立，包括安全组织机构、安全制度、安全管理流程、安全人员意识等。通过安全体系的建立，可以最大程度上实现网络的整体安全，满足企事业单位的安全发展要求。

1.6 计算机网络安全的主要威胁及隐患

1.6.1 网络安全的主要威胁

计算机网络的发展，使信息共享应用日益广泛与深入。但是信息在公共通信网络上存储、共享和传输，会被非法窃听、截取、篡改或毁坏而导致不可估量的损失。尤其是银行系统、商业系统、管理部门、政府或军事领域对公共通信网络中存储与传输的数据安全问题更为关注。如果因为安全因素使得信息不敢放进 Internet 这样的公共网络，那么办公效率及资源的利用率都会受到影响，甚至使人们丧失了对 Internet 及信息高速公路的信赖。

事物总是辨证的：一方面，网络提供了资源的共享性、用户使用的方便性，通过分布式处理提高了系统效率和可靠性，并且还具有了扩充性；另一方面，正是这些特点增加了网络受攻击的可能性。计算机网络所面临的威胁包括对网络中信息的威胁和对网络中设备的威胁。

影响计算机网络的因素很多，有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；还可能是外来黑客对网络系统资源的非法使用等。

人为的无意失误，如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的帐号随意转借给他人或与别人共享都会对网络安全带来威胁。

人为的恶意攻击，是计算机面临的最大威胁。敌手的攻击和计算机犯罪就属于这一类。此类攻击又可以分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一种是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄露。

网络软件的漏洞和“后门”。网络软件不可能是百分之百无缺陷和无漏洞的。然而，这些漏洞和缺陷恰恰是黑客经常攻击的首选目标。黑客攻入网络内部的事件大部分就是因为安全措施不完善所招致的。另外，软件的“后门”都是软件公司的设计编程人员为了方便而设置的，一般不为外人所知，但一旦“后门”打开，其造成的后果将不堪设想。

总的说来，网络安全的主要威胁来自以下几个方面。

① 自然灾害、意外事故。

② 计算机犯罪。

③ 人为行为，例如使用不当，安全意识差等。

④“黑客”行为。黑客的入侵或侵扰，例如非法访问、拒绝服务、计算机病毒、非法链接等。

⑤ 内部泄密。

⑥ 外部泄密。

⑦ 信息丢失。

⑧ 电子谍报，例如信息流量分析、信息窃取等。

⑨ 信息战。

⑩ 网络协议中的缺陷，例如 TCP/IP 协议的安全问题等。

1.6.2　计算机网络安全的技术隐患

计算机网络的安全隐患是多方面的。从网络组成结构上分，有计算机信息系统的，有通信设备、设施的；从内容上分，有技术上的和管理上的。从技术上来看，主要有以下几个方面。

1．网络系统软件自身的安全问题

网络系统软件的自身安全与否直接关系到网络的安全，网络系统软件的安全功能较少或不全，以及系统设计时的疏忽或考虑不周而留下的“破绽”都等于给危害网络安全的人和事留下许多“后门”。例如，美国微软公司就经常针对已发现的系统“破绽”发布“补丁”程序。同时，在同一系统软件中，低版本的往往比高版本的在安全性能方面差了许多，所以在服务器上要注意尽量使用高版本的操作系统，并应使用系统软件所能提供的最高安全级别。

另外，值得注意的是操作系统的许多默认值都已被黑客们盯上了，往往被用来作为侵入网络的突破口，所以应尽量避免使用系统默认值。此外，还要注意的有以下几点。

① 操作系统的体系结构造成其本身是不安全的，这也是计算机系统不安全的根本原因之一。操作系统的程序是可以动态连接的，包括 I/O 的驱动程序与系统服务，都可以采用打“补丁”的方式进行动态连接。许多 Unix 操作系统的版本的升级、开发都是采用打“补丁”的方式进行的。这种方法既然厂商可以使用，那么黑客也可以使用，同时这种动态连接也成为计算机病毒产生的好环境。

② 操作系统的一些功能，例如支持在网络上传输文件的功能，包括可以执行的文件映象，即在网络上加载程序等，必然带来一些不安全因素。

③ 操作系统不安全的另一原因在于它可以创建进程，甚至支持在网络的节点上进行远程进程的创建与激活，更重要的是被创建的进程可以继承创建进程的权力。这一点与可在网络上加载程序结合起来就构成了可以在远端服务器上安装“间谍”软件的条件。若再加上把这种间谍软件以打补丁的方式“打”在一个合法的用户上，尤其“打”在一个特权用户上，系统进程与作业监视程序就都无法监测这些黑客和间谍软件的存在。

④ 操作系统运行时一些系统进程总在等待一些条件的出现，一旦有满足要求的条件出现，程序便继续运行下去，这都是黑客可以利用的。

⑤ 操作系统要安排无口令入口，这原本是为系统开发人员提供的便捷入口，但它也是黑客的通道。另外，操作系统还有隐蔽信道。

⑥ Internet 和 Intranet 使用的 TCP/IP（传输控制协议/网际协议）以及 FIP（文件传输协议）、E-mail（电子邮件）、RPC（远程程序通信规则）、NFS（网络文件系统）等都包含许多不安全的因素，存在着许多漏洞。

2．网络系统中数据库的安全设计问题

网络中的信息数据是存放在计算机数据库中的，供不同的用户来共享。数据库存在着不安全性和危险性，因为在数据库系统中存放着大量重要的信息资源，在用户共享资源时可能会出现以下现象：授权用户超出了他们的访问权限进行更改活动，非法用户绕过安全内核窃取信息资源等。因此提出了数据库安全问题，也就是要保证数据的安全可靠和正确有效。对数据库数据的保护主要是针对数据的安全性、完整性和并发控制三方面。

数据的安全性就是保证数据库不被故意地破坏和非法地存取。数据的完整性是防止数据库中存在不符合语义的数据，以及防止由于错误信息的输入、输出而造成无效操作和错误结果。并发控制即数据库是一个共享资源，在多个用户程序并行地存取数据库时，就可能会产生多个用户程序并发地存取同一数据的情况，若不进行并发控制就会使取出和存入的数据不正确，破坏数据库的一致性。

所以在数据库设计时，必须考虑到这些问题。通常可采取一系列的安全策略和安全机制，其中主要是解决存取控制问题。可是对数据的存取控制还不足以对数据库用户进行约束，所以还要增加作业授权控制，把作业授权控制结合到安全策略中，并用自主性和强制性的存取控制来处理用户对数据的访问。而作业授权控制是处理用户对作业以及作业对数据的访问，这种作业授权控制既提供了高可靠性，又提供了应用的灵活性。

下面以著名的数据库 Oracle 和 Fox 或 dBASE 为例来说明。Oracle 数据库系统是一个非常有影响的分布式数据库系统，它不仅有国内广泛使用的微机版本，而且还支持许多不同的操作系统。Oracle 数据库系统体系非常庞大，在此，仅以 Oracle forNetWare 为例来说明其良好的自身保护机制。Oracle 是通过保护数据库的数据单元表（table 来保护信息资源不被其他程序进行非授权访问，从而达到保护自身的目的。Oracle 的 table 存储方式是由若干 table 组合在一起，以一个大文件的形式存放在 Novell 网络服务器的 Oracle 目录内的。这个文件的结构和加密方法对外均不公开，因而，其他用户程序是无法破解这些 table 信息的，而且 Oracle 对外也不提供访问的接口。相比之下，Fox 或 dBASE 的自身保护机制就差得多，甚至可以说没有一点自身保护机制。众所周知，Fox 或 dBASE 的 table 存放在以 DBF 结尾的文件里，而结构完全是公开的。存放在 DBF 文件内的信息没有任何加密处理，非授权用户可以不通过 Fox 规定的方式访问 DBF 文件，因而很容易受到外来程序的攻击。这一点希望能引起所有基于 Fox 或 dBASE 建造的网络信息系统，尤其是金融、财务系统的管理人员的注意，对其每天都要运行的系统的安全性给予高度重视。

3．传输线路安全与质量问题

尽管在同轴电缆、微波或卫星通信中要窃听其中指定一路的信息是很困难的，但是从安全的角度来说，没有绝对安全的通信线路。

同时，无论采用何种传输线路，当线路的通信质量不好时，将直接影响联网效果，严重的时候甚至导致网络中断。例如，市内电话线路，主要电气指标有直流电气性能指标（环阻、绝缘电阻）、交流特性（线路衰耗、线路衰耗交流频率特征）、交流特性阻抗等，当通信线路中断，计算机网络也就中断，这还比较明显。而当线路时通时断、线路衰耗大或杂音严重时，问题就不那么明显，但是对通信网络的影响却是相当大，可能会严重地危害通信数据的完整性。为保证好的通信质量和网络效果，就必须要有合格的传输线路，如在干线电缆中，应尽量挑选最好的线作为计算机联网专线，以得到最佳的效果。

4．其他威胁网络安全的典型因素

其他威胁网络安全的典型因素主要有以下几方面。

① 计算机黑客（将在后面的章节专门介绍）。

② 内部人员作案。有的员工可能会利用工作机会报复，此外如果系统管理员也成了黑客那就更危险了。

③ 窃听。同轴电缆、双绞线、光纤或无线方式引入了新的物理安全暴露点，被动方式如搭线窃听或主动方式的如无线仿冒。利用计算机通信设备天然存在的电磁泄漏进行窃取活动，也是一个重要的安全隐患。

④ 部分对整体的安全威胁，任一单一组件的失密都可能造成整个网络的安全失败。

⑤ 程序共享造成的冲突，共享同一程序可能会造成死锁、信息失效或文件不正确的开关状态。

⑥ 对互联网而言，可能有更多潜在的威胁，即使各网均能独立安全运行，联网之后，也会发生互相侵害的后果。

⑦ 计算机病毒。由于网络的设计目标是资源共享，使得网络是计算机病毒滋生和传播

的理想家园。

1.7　网络安全的现状及发展趋势

1.7.1　网络安全现状

随着信息化建设进展，网络已经成为支撑许多行业开展业务的基础平台，网络安全将直接影响到业务的正常运转，甚至关系到国家安全和社会稳定。目前，网络面临着不同动机的威胁者，承受着不同类型的攻击。信息泄露、恶意代码、垃圾邮件、网络恐怖主义等都将影响到网络安全。多协议、多系统、多应用、多用户组成的网络环境，其复杂性高，存在难以避免的安全脆弱性。据 SecurityFocus 公司的漏洞统计数据表明，绝大部分操作系统存在安全漏洞。由于管理、软件工程难度等问题，新的脆弱性不断地被引入到网络环境中，所有这些安全脆弱点都将可能成为攻击切入点，攻击者可以利用这些脆弱点入侵系统，窃取信息。1998 年 2 月，黑客利用 SolarSunrise 弱点入侵美国国防部网络，受害的计算机数超过 500 台，而攻击者只是采用了中等复杂工具。现在的网络安全事件日趋增多。

1.7.2　网络安全的新趋势

2011 年的网络安全会出现哪些新变化、新趋势呢?下面是五条有关 2011 年安全趋势的预言，每条预言都很给力。

① 能够精确制导并跨国摧毁关键物理设施的类“超级工厂病毒”。

今年出现的超级工厂病毒，让人们见识了病毒在网络战争里的威力。

② 僵尸网络之间的战争升级。

黑吃黑其实并不仅仅出现在现实社会里，各类僵尸网络之间，由于黑色产业链下经济利益的冲突，互相火并爆发黑道大战不可避免。

③ 被病毒感染后更加凶悍的木马、蠕虫程序。

病毒+木马的时代下，病毒与木马、蠕虫也在融合，融合后的新木马、蠕虫将更加强悍。

④ 社交网站成为黑客传播病毒的乐园。

社交网站在互联网上建立起了虚拟的人类社会，鱼龙混杂下，社交网站也成为黑客传播病毒的温床与乐园。

⑤ 无所不在、缺乏防范的智能手机将成为 IT 经理们的恶梦。

智能手机给人们带来愈来愈多的便利，也给黑客带来越来越多入侵的机遇，IT 经理们将面临新的噩梦。

1.8　网络安全产品

目前，国内网络安全产品主要是以硬件为主，其中包括防火墙、入侵检测系统、防病毒网关、VPN、物理隔离卡等产品，其中以防火墙、入侵检测系统、VPN 应用得最为广泛。对于大多数用户而言，他们目前需求的已经不再是单一的产品，而是从系统需求分析到产品的专业化整体解决方案。

1.8.1　目前国内市场的主要网络安全产品厂商

1．NetScreen 网络安全技术公司

NetScreen 公司总部设在美国 Santa Clara 市，是一家专业开发基于 ASIC 的互联网安全系