新版

21世纪

高职高专系列教材

计算机网络安全与应用

◎张兆信　赵永葆　赵尔丹　等编著

提供电子教案的增值服务

机械工业出版社
CHINA MACHINE PRESS

21世纪高职高专系列教材

计算机网络安全与应用

张兆信　赵永葆　赵尔丹　等编著

机械工业出版社

本书介绍了计算机网络安全的基础知识、硬件实体的防护安全、加密技术、备份技术、防火墙技术、计算机操作系统的安全与配置，以及计算机病毒和黑客技术。

本书是本着“理论知识以够用为度，重在实践应用”的原则，以“理论＋工具＋分析实施”为主要形式编写的。主要章节都配合内容提供了应用工具及分析实施的相关实例，每章都配有习题或实训。

本书适合用作高职高专计算机专业、网络专业及相近专业的教材，也可供有关工程人员和自学者使用。

图书在版编目（CIP）数据

计算机网络安全与应用/张兆信等编著. —北京：机械工业出版社，2005.2
（21世纪高职高专系列教材）
ISBN 7-111-16135-1

Ⅰ.计… Ⅱ.张… 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（2005）第010438号

机械工业出版社（北京市百万庄大街22号　邮政编码100037）
策　　划：胡毓坚
责任编辑：李利健
责任印制：杨　曦

北京蓝海印刷有限公司印刷·新华书店北京发行所发行

2005年3月第1版·第1次印刷
787mm×1092mm $^{1}/_{16}$·13印张·321千字
0001-5000册
定价：19.00元

21世纪高职高专计算机专业系列教材
编委会成员名单

出 版 说 明

根据教育部《关于以就业为导向深化高等职业教育改革的若干意见》中提出的高等职业院校必须把培养学生动手能力、实践能力和可持续发展能力放在突出的地位，促进学生技能的培养，以及教材内容要紧密结合生产实际，并注意及时跟踪先进技术的发展等指导精神，机械工业出版社组织全国40余所院校的骨干教师对在2001年出版的“面向21世纪高职高专系列教材”进行了修订。

在几年的教学实践中，本系列教材获得了较高的评价。因此，在修订过程中，各编委会保持了第1版教材“定位准确、注重能力、内容创新、结构合理和叙述通俗”的编写特色。同时，针对教育部提出的高等职业教育的学制将由三年逐步过渡为两年，以及强调以能力培养为主的精神，制定出了本次教材修订的原则：跟上我国信息产业飞速发展的节拍，适应信息行业相关岗位群对第一线技术应用型操作人员能力的要求，针对两年制兼顾三年制，理论以“必须、够用”为原则，增加实训的比重，并且制作了内容丰富而且实用的电子教案，实现了教材的立体化。

针对课程的不同性质，修订过程中采取了不同的处理办法。核心基础课的教材在保持扎实的理论基础的同时，增加实训和习题；实践性较强的课程强调理论与实训紧密结合；涉及实用技术的课程则在教材中引入了最新的知识、技术、工艺和方法。此外，在修订过程中，还进行了将几门课程整合在一起的尝试。所有这些都充分地体现了修订版教材求真务实、循序渐进和勇于创新的精神。在修订现有教材的同时，为了顺应高职高专教学改革的不断深入，以及新技术新工艺的不断涌现和发展，机械工业出版社及教材编委会在对高职高专院校的专业设置和课程设置进行了深入的研究后，还准备出版一批适应社会发展的急需教材。

信息技术以前所未有的速度飞快地向前发展，信息技术已经成为经济发展的关键手段，作为与之相关的教材要抓住发展的机遇，找准自身的定位，形成鲜明的特色，夯实人才培养的基础。为此，担任本系列教材修订任务的教师，将努力把最新的教学实践经验融于教材的编写之中，并以可贵的探索精神推进本系列教材的更新。由于高职高专教育正在不断的发展中，加之我们的水平和经验有限，在教材的编审中难免出现问题和错误，恳请使用这套教材的师生提出宝贵的意见和建议，以利我们今后不断改进，为我国的高职高专教育事业作出积极的贡献。

机械工业出版社

前　言

本书是根据教育部的高职高专从三年制逐步过渡为二年制，将培养方向由技术应用型向技能型转变的要求而编写的。作者均是多年从事网络安全教学和网络安全设计及实践，并有丰富的高职高专教学经验的教师。

本书以网络安全为重点，兼顾基础理论，以“理论＋工具＋分析实施”的形式，由浅入深，以通俗的语言和丰富的实例使读者能快速掌握教材内容。在编写过程中，本书作者参阅了大量最新资料，使本书内容能及时反映最新的技术发展。对于所用的一些软件，为了读者便于查找，都给出了相关网站。本课程建议授课学时为 40 学时，实验学时为 20 学时。

本书共分为 8 章，第 1 章介绍计算机网络安全的基础知识，包括计算机网络安全的含义及安全等级、计算机网络系统的脆弱性及安全威胁、计算机网络安全的体系结构等；第 2 章介绍硬件实体的防护安全，包括物理实体和计算机硬件的防护以及机房的防护；第 3 章介绍加密技术，包括对称加密和非对称加密以及具体应用等；第 4 章介绍备份技术，包括备份的层次与备份方法、克隆利器——Ghost、WinRAR 的使用、网络备份方案的设计等；第 5 章介绍防火墙技术，包括防火墙的分类、防火墙的选择和使用、防火墙的发展趋势、防火墙产品实例等；第 6 章介绍计算机操作系统的安全与配置，包括 Windows 95/98/Me 的安全性、Windows NT/2000/XP 的安全基础、UNIX 系统的安全性、Linux 系统的安全性；第 7 章介绍计算机病毒，包括计算机病毒的分类、计算机病毒的工作原理、反病毒技术、常见计算机病毒介绍、常用杀毒软件等；第 8 章介绍黑客技术，包括黑客攻击的步骤与防范、端口扫描与安全防范、拒绝服务攻击与防范、网络监听与防范、木马与安全防范等。每章后附有与内容紧密结合的习题或实训。本书还配有电子教案，选用本教材的学校可在机械工业出版社网站（http://www.cmpbook.com）上获取，或通过电子邮件与作者联系，作者的 E-mail:fvzzx@sohu.com。

本书由张兆信、赵永葆、赵尔丹等编著，其中，第 1～3 章由张兆信、张炳辉编写，第 4、5、8 章由赵永葆编写，第 6、7 章由赵尔丹、张照枫编写，全书由张兆信统稿。

由于作者水平有限，书中出现的错误和不妥之处，敬请读者批评、指正。

编　者

目　录

出版说明
前言
第 1 章　计算机网络安全概述 …… 1
1.1　计算机网络安全事件 …… 1
1.2　计算机网络安全的含义及安全等级 …… 2
1.3　计算机网络系统的脆弱性及安全威胁 …… 4
1.4　计算机网络安全的体系结构 …… 6
1.5　计算机网络安全的设计 …… 8
1.6　习题 …… 9
第 2 章　计算机网络系统的硬件防护技术 …… 10
2.1　影响实体安全的主要因素 …… 10
2.2　计算机的安全维护 …… 11
2.3　计算机机房的建设与安全防护 … 12
2.4　实训 …… 14
2.5　习题 …… 14
第 3 章　加密技术 …… 15
3.1　加密概述 …… 15
3.2　传统加密方法(对称密码) …… 16
3.2.1　数据加密标准(DES) …… 17
3.2.2　其他对称分组密码 …… 23
3.3　公钥加密(非对称密码) …… 23
3.3.1　RSA 公钥加密 …… 24
3.3.2　DH(Diffie-Hellman)公钥加密 …… 24
3.4　公钥基础设施 PKI (Public Key Infrastructure) …… 25
3.4.1　数字签名 …… 25
3.4.2　认证及身份验证 …… 26
3.5　Kerberos 身份认证系统 …… 28
3.6　PGP(Ptetty Good Privacy)加密系统 …… 29
3.7　加密技术的应用 …… 34
3.7.1　Word 文件加密解密 …… 34
3.7.2　Foxmail 加密解密 …… 36
3.7.3　WinRAR 加密解密技术 …… 41
3.8　使用加密工具加密 …… 44
3.8.1　ABI-Coder 的应用 …… 44
3.8.2　电子邮件加密工具 A-lock 的应用 …… 46
3.9　计算机网络加密技术 …… 48
3.9.1　链路加密 …… 49
3.9.2　节点加密 …… 49
3.9.3　端-端加密 …… 49
3.10　实训 …… 49
3.11　习题 …… 50
第 4 章　备份技术 …… 51
4.1　备份技术概述 …… 51
4.1.1　备份的概念 …… 51
4.1.2　备份数据的类型 …… 52
4.1.3　备份的方式 …… 53
4.1.4　备份采用的存储设备 …… 55
4.1.5　网络备份 …… 57
4.2　备份的层次与备份方法 …… 58
4.2.1　备份的层次 …… 58
4.2.2　硬件级备份 …… 59
4.2.3　软件级备份技术 …… 62
4.3　Windows 2000 中的备份与恢复 …… 64
4.3.1　Windows 2000 中备份的作用 …… 64
4.3.2　Windows 2000 中的备份方法 …… 64
4.3.3　Windows 2000 中文件(夹)的备份 …… 65
4.3.4　Windows 2000 中其他重要数据的备份 …… 66
4.4　克隆利器——Ghost …… 67
4.4.1　Ghost 介绍 …… 67
4.4.2　Ghost 备份硬盘上的数据 …… 67
4.4.3　Ghost 使用注意事项 …… 70
4.5　WinRAR 的使用 …… 70
4.5.1　WinRAR 介绍 …… 70

4.5.2 WinRAR 压缩文件 …… 70
4.5.3 WinRAR 解压文件 …… 71
4.6 网络备份方案的设计 …… 72
4.6.1 备份软件 …… 72
4.6.2 日常备份制度 …… 73
4.6.3 灾难恢复措施 …… 75
4.7 实训 …… 75
4.8 习题 …… 76
第 5 章 防火墙技术 …… 77
5.1 防火墙概述 …… 77
5.1.1 防火墙概念 …… 77
5.1.2 防火墙的功能 …… 78
5.1.3 防火墙的局限性 …… 79
5.2 防火墙的分类 …… 80
5.2.1 网络层防火墙 …… 80
5.2.2 应用层网关 …… 82
5.2.3 复合型防火墙 …… 83
5.3 防火墙的选择和使用 …… 84
5.3.1 防火墙的选择原则 …… 84
5.3.2 防火墙的使用误区 …… 86
5.4 防火墙的发展趋势 …… 87
5.5 防火墙产品实例 …… 88
5.5.1 联想网御 2000 …… 88
5.5.2 天网防火墙 …… 91
5.6 实训 …… 97
5.7 习题 …… 97
第 6 章 计算机操作系统的安全与配置 …… 98
6.1 Windows 95/98/Me 的安全性 …… 98
6.1.1 Windows 98 的登录机制 …… 98
6.1.2 Windows 98 的屏幕保护机制 …… 99
6.1.3 利用注册表提高 Windows 98 系统的安全 …… 100
6.2 Windows NT/2000/XP 的安全基础 …… 107
6.2.1 Windows 2000 的安全基础概念 … 107
6.2.2 用户账号的管理 …… 108
6.2.3 组的管理 …… 111
6.2.4 Windows 2000 的安全模型 …… 113
6.2.5 Windows 2000 的安全机制 …… 115
6.2.6 Windows 2000 的安全性 …… 117
6.2.7 Windows 2000 安全访问控制 … 118
6.2.8 在 Windows 2000 系统中监视和优化性能 …… 120
6.2.9 Windows NT/2000/XP 的安全措施 …… 124
6.3 UNIX 系统的安全性 …… 126
6.3.1 UNIX 操作系统简介 …… 126
6.3.2 UNIX 系统的安全性 …… 127
6.4 Linux 系统的安全性 …… 129
6.4.1 Linux 操作系统简介 …… 129
6.4.2 Linux 系统的常用命令 …… 130
6.4.3 Linux 系统的网络安全 …… 131
6.5 实训 …… 134
6.6 习题 …… 135
第 7 章 计算机病毒 …… 136
7.1 计算机病毒概述 …… 136
7.1.1 计算机病毒的定义 …… 136
7.1.2 计算机病毒的发展历史 …… 136
7.1.3 计算机病毒的危害 …… 137
7.1.4 计算机病毒的特征 …… 138
7.2 计算机病毒的分类 …… 139
7.3 计算机病毒的工作原理 …… 142
7.3.1 计算机病毒的结构 …… 142
7.3.2 引导型病毒的工作原理 …… 142
7.3.3 文件型病毒的工作原理 …… 143
7.4 反计算机病毒技术 …… 144
7.4.1 反计算机病毒技术的发展 …… 145
7.4.2 病毒防治的常用方法 …… 145
7.4.3 Windows 病毒防范技术 …… 146
7.5 常见计算机病毒介绍 …… 149
7.5.1 CIH 病毒 …… 149
7.5.2 Word 宏病毒 …… 151
7.5.3 红色代码病毒 …… 153
7.5.4 尼姆达病毒 …… 154
7.5.5 硬盘杀手病毒 …… 156
7.5.6 冲击波病毒防范技术 …… 157
7.5.7 振荡波病毒防范技术 …… 160
7.6 常用杀毒软件 …… 161
7.6.1 瑞星杀毒软件 …… 161
7.6.2 江民杀毒软件 …… 166
7.6.3 Norton AntiVirus 杀毒软件 …… 170

7.7 实训 …… 179
7.8 习题 …… 179
第 8 章 黑客的攻击与防范 …… 180
8.1 关于黑客 …… 180
8.2 黑客攻击的步骤与防范 …… 181
8.2.1 黑客攻击的步骤 …… 181
8.2.2 防范黑客原则 …… 181
8.3 端口扫描与安全防范 …… 182
8.3.1 端口的概念 …… 182
8.3.2 端口的分类 …… 182
8.3.3 端口扫描 …… 183
8.3.4 端口扫描的安全防范 …… 184
8.4 拒绝服务攻击与防范 …… 185
8.4.1 拒绝服务攻击的概念 …… 185
8.4.2 分布式拒绝服务攻击——DDoS …… 186
8.4.3 拒绝服务攻击的防范 …… 188
8.5 网络监听与防范 …… 189
8.5.1 网络监听的工作原理 …… 189
8.5.2 网络监听的检测和防范 …… 190
8.6 木马与安全防范 …… 191
8.6.1 木马的概念 …… 191
8.6.2 木马的种类 …… 193
8.6.3 木马工具——冰河 …… 193
8.6.4 木马的防范 …… 195
8.6.5 木马的清除 …… 196
8.7 邮件炸弹 …… 197
8.7.1 邮件炸弹的概念 …… 197
8.7.2 预防邮件炸弹 …… 198
8.8 实训 …… 199
8.9 习题 …… 199
参考文献 …… 200

第1章　计算机网络安全概述

本章要点

- 计算机网络安全事件
- 计算机网络安全的含义及安全等级
- 计算机网络系统的脆弱性及安全威胁
- 计算机网络安全的体系结构
- 计算机网络安全的设计

1.1　计算机网络安全事件

随着网络技术的发展和普及，全球信息化已成为人类社会发展的大趋势。网络的快速发展使得网上资源越来越丰富，许多诸如电子商务、电子政务、电子税务、电子海关、网上银行、网络防伪等新兴业务也迅速兴起，又由于 Internet 的国际化、社会化、开放化、个人化的特点，使网络安全问题变得越来越重要，计算机网络犯罪所造成的经济损失令人吃惊，而且在许多情况下网络侵入造成的损失远远不能用经济损失来衡量。下面是来自公开媒体的一些典型安全事件。

Pakistan 病毒：巴锡特（Basit）和阿姆杰德（Amjad）两兄弟是巴基斯坦的拉合尔（Lahore）人，经营着一家 IBM-PC 机及其兼容机的小商店。1986 年初，他们编写了 Pakistan 病毒，即 C-Brain 病毒，业界都公认这是真正具备完整特征的电脑病毒始祖。他们的目的主要是为了防止他们的软件被任意盗拷，只要有人盗拷他们的软件，C-Brain 就会发作，将盗拷者的硬盘剩余空间给吃掉。

1988 年美国典型计算机病毒入侵计算机网络的事件：1988 年 11 月 2 日，美国 6000 多台计算机被病毒感染，造成 Internet 不能正常运行。这次非常典型的计算机病毒入侵计算机网络的事件，迫使美国政府立即作出反应，国防部也成立了计算机应急行动小组。这次事件中遭受攻击的有 5 个计算机中心和 12 个地区结点，它们连接着政府、大学、研究所和拥有政府合同的 250000 台计算机。这次病毒事件使计算机系统遭受的直接经济损失就达 9600 万美元。这个病毒程序的设计者是罗伯特·莫里斯（Robert T.Morris），当年 23 岁，在康乃尔（Cornell）大学攻读研究生学位。

黑客侵入美国军方及美国航空航天局网络的典型事件：1996 年 12 月，黑客侵入美国空军的全球网网址并将其主页肆意改动，迫使美国国防部一度关闭了其他 80 多个军方网址。2002 年 11 月 12 日，美国联邦政府对一名英国计算机管理员提起起诉，指控他非法侵入了美军和美国航空航天局的 92 处计算机网络，其中在侵入新泽西州一处海军设施的网络时，导致该设施系统陷入崩溃状态。

考生答卷被删事件：2002 年，江苏省普通高中信息技术等级考试，由于“黑客”入侵，有近

万名考生答卷被删,造成了非常恶劣的后果。之后“黑客”以破坏网上考试的罪名被判刑6个月。

17岁黑客害了11万台电脑:17岁的犯罪嫌疑人池勇是黑龙江省七台河市一所高级中学的在校生,他自己经营了一个“混客帝国”网站,从事病毒攻击、盗取数据、非法交易等危害网络安全的行为,据其个人主页上的计数器统计,仅从2001年12月17日到2002年1月27日,即网络安全人员开始对其跟踪侦查到将其捕获的短短42天时间里,就有超过11万名各地电脑用户因登录“混客帝国”而遭受严重损失。池勇在审讯过程中还承认自己盗取的QQ号就有5000多个。

互联网的“9·11”—— 蠕虫王病毒:2003年1月25日,互联网遭遇到全球性的病毒攻击。受此病毒袭击,在中国80%以上的网民不能上网,很多企业的服务器被此病毒感染导致网络瘫痪。在美国、泰国、日本、韩国、马来西亚、菲律宾和印度等国家的互联网也受到严重影响。这个病毒名叫Win32.SQLExp.Worm,病毒体极其短小,却具有极强的传播性,它利用Microsoft SQL Server的漏洞进行传播,由于Microsoft SQL Server在世界范围内普及度极广,因此,此次病毒攻击导致全球范围内的互联网瘫痪。此次蠕虫发作,对人们的震撼不亚于美国的恐怖袭击“9·11”事件。这是继红色代码、尼姆达、求职信病毒后又一起极速病毒传播的案例。“蠕虫王病毒”的发作致使全世界范围内的损失额保守估计可高达12亿美元。

“冲击波”病毒肆虐全球:2003年8月11日,一种名为“冲击波”(WORM_MSBlast.A)的新型蠕虫病毒开始在国内互联网和部分专用信息网络上传播。该病毒运行时会扫描网络,寻找操作系统为Windows 2000/XP的计算机,然后通过RPC漏洞进行感染,该病毒会操纵135、4444、69端口,危害系统。受到感染的计算机中的Word、Excel、Powerpoint等文件无法正常运行,弹出找不到链接文件的对话框,“粘贴”等一些功能无法正常使用,计算机出现反复重新启动等现象,并且该病毒传播速度快、波及范围广,对计算机的正常使用和网络运行造成严重影响。

上述事件只是网络安全事件中极典型的几例,有媒体报道,实际上,中国95%与Internet相连的网络管理中心都遭到过境内外黑客的攻击或侵入。而美国由于网络安全事故造成的经济损失在2000年就达3.78亿美元,2001年则达到4.56亿美元。国外的一项研究表明,15年来,每年在信息安全方面的预算上涨17倍,但实际花费却增长了120倍,可是这些花费的收效却甚微。所以,网络安全的问题已成为当今世界极其重要的问题。

1.2 计算机网络安全的含义及安全等级

上述事例一定已使读者对计算机网络安全有了一个初步的了解,但是计算机网络安全的真正含义是什么呢?从不同的角度来说,网络安全具有不同的含义,从运行管理角度考虑是要求网络正常、可靠、连续地运行。从国家、社会的角度是要过滤有害信息。

但就一般用户而言,所希望的就是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,避免他人利用不法手段对用户信息的损害和侵犯。总的来说,网络安全是指网络系统的硬件、软件及其系统中的数据的安全。

实际上,网络安全所涉及的领域是相当广泛的,因为对计算机网络安全的威胁来自各个方面,有自然因素,也有人为因素。自然因素有地震、火灾、空气污染和设备故障等,而人为因素

有无意和有意之分，无意的比如误操作造成的数据丢失；有意的如诸多的黑客侵入。

衡量网络安全的指标主要有保密性、完整性、可用性、可控性与可审查性。

- 保密性：即防泄密，确保信息不泄露给未授权的实体或进程。
- 完整性：主要是防篡改，只有得到允许的人才能修改实体或进程，并且能够判别出实体或进程是否已被修改。
- 可用性：防中断，只有得到授权的实体才可获得服务，攻击者不能占用所有的资源，阻碍授权者的工作。
- 可控性：可控性主要指信息的传播及内容具有控制能力。使用授权机制，控制信息的传播范围和内容，必要时能恢复密钥，实现对网络资源及信息的可控性。
- 可审查性：对出现的安全问题提供调查的依据和手段。

网络安全的目标是确保网络系统的信息安全。网络信息主要包括两个方面：信息存储安全和信息传输安全。信息存储安全是指信息在静态存放状态下的安全，而信息传输安全主要是指在动态传输过程中的安全。信息传输安全尤其需要防护的是截获、伪造、篡改、中断和重发。

换种说法，网络安全的目的是使用访问控制机制使非授权用户“进不来”；使用授权机制使不该拿走的信息“拿不走”；使用加密机制使信息即使不慎被拿走了，未授权实体或进程也“看不懂”；使用数据完整鉴别机制使未授权者对数据“改不了”；使用审记、监控、防抵赖机制使得攻击者、破坏者、抵赖者“逃不脱”。

随着计算机安全问题的被重视，1983 年，美国国防部提出一套《可信计算机评估标准》，又称“桔皮书”，它将计算机的安全等级划分为四大类——D、C、B、A，共 7 个小类——D、C1、C2、B1、B2、B3 和 A1。

- D 类：最低保护。无账户，可任意访问文件，没有安全功能。拥有这个级别的操作系统是完全不可信的。
- C1 类：选择性安全保护。系统能够把用户和数据隔开，用户根据需要采用系统提供的访问控制措施来保护自己的数据，系统中必有一个防止破坏的区域，其中包含安全功能。C1 级保护的不足之处在于用户可直接访问操作系统的根用户。C1 级不能控制进入系统的用户的访问级别，所以用户可以将系统中的数据任意移走，可以控制系统配置，获取比系统管理员允许的更高权限。
- C2 类：受控的访问控制。控制粒度更细，使得允许或拒绝任何用户访问单个文件成为可能。系统必须对所有的注册，以及文件的打开、建立和删除进行记录。审计跟踪必须追踪到每个用户对每个目标的访问。使用附加身份认证就可以让一个 C2 级系统用户在不是超级用户的情况下有权执行系统管理工作。还有就是用户权限可以以个人为单位对某一程序所在目录进行访问，如果其他程序或数据在同一目录下，那么用户也将自动得到访问这些信息的权限。
- B1 类：有标签的安全保护。系统中的每个对象都有一个敏感性标签，而每个用户都有一个许可级别。许可级别定义了用户可处理的敏感性标签。系统中的每个文件都按内容分类并标有敏感性标签，任何对用户许可级别和成员分类的更改都受到严格控制，即使是文件所有者，也不能随意改变文件许可权限。B1 级计算机系统安全措施由操作系统决定，政府机构和防御承包商们是 B1 级计算机系统的主要拥有者。

- B2 类:结构化安全保护。系统的设计和实现要经过彻底的测试和审查。系统应结构化为明确而独立的模块,遵循最小特权原则。必须对所有目标和实体实施访问控制。政策要有专职人员负责实施,要进行隐蔽信道分析。系统必须维护一个保护域,保护系统的完整性,防止外部干扰。它是提供较高安全级别的对象与较低级别的对象相通的第一个级别。
- B3 类:安全域机制。系统的安全功能足够小,以利于广泛测试。必须满足参考监视器的需求,以传递所有的主体到客体的访问。要有安全管理员、安全硬件装置、审计机制扩展到用信号通知安全相关事件,还要求有恢复规程,系统高度抗侵扰。该级别也要求用户通过一条可信任的途径连接到系统上。
- A1 类:核实保护。这是当前桔皮书中的最高级别。它包含了一个严格的设计、控制和验证过程。与前面提到的各级别一样,这一级别包含了较低级别的所有特性。设计必须是从数学角度上经过验证的,而且必须进行秘密通道和可信任分布的分析。

近 20 年来,人们一直在努力发展安全标准,并将安全功能与安全保障分离,制定了复杂而详细的条款。但真正实用,并且在实践中相对易于掌握的还是 TCSEC 及其改进版本。在现实中,安全技术人员也一直将 TCSEC 的 7 级安全划分当作默认标准。

我国的《计算机信息系统安全保护等级划分准则》也已经正式颁布,并于 2001 年 1 月 1 日起实施。该准则将信息系统安全分为 5 个等级:

- 自主保护级:相当于 C1 级。
- 系统审计保护级:相当于 C2 级。
- 安全标记保护级:相当于 B1 级,属于强制保护。
- 结构化保护级:相当于 B2 级。
- 访问验证保护级:相当于 B3～A1 级。

实际应用中,主要考核的安全指标有身份认证、访问控制、数据完整性、安全审计、隐蔽信道分析等。

1.3 计算机网络系统的脆弱性及安全威胁

计算机网络系统的脆弱性通常包括计算机系统本身的脆弱性、通信设施的脆弱性和数据库安全的脆弱性。操作系统的不安全性、网络通信协议的缺陷、网络软件和网络服务的漏洞、数据库数据容易丢失以及通信硬件的不安全性等都会给危害网络安全的人和事留下许多后门。

从前面介绍的安全等级可以看到,有的操作系统属于 D 级,这一级别的操作系统根本就没有安全防护措施,如 Windows 95 等,它们根本不能用于安全性要求高的服务器,即使可用于服务器的 Windows NT 和 UNIX 等因设计时的疏忽和考虑不周仍然存在许多安全漏洞,使入侵者有机可乘。可以说,操作系统的不安全性是计算机系统不安全的根本原因。

一是操作系统的程序支持程序与数据的动态连接,包括 I/O 的驱动程序与系统服务都可以用打"补丁"的方式进行动态连接。UNIX 操作系统的某些版本升级、开发也是用打"补丁"的方式进行的。既然厂商可以使用这种方法,"黑客"同样也可以使用,它当然也就成了计算机病毒产生的好环境。

另外，操作系统的一些功能，比如，支持在网络上传输文件的功能，在带来许多方便的同时必然也带来不安全的因素，而且这种矛盾很难解决。

操作系统不安全性的另一原因还在于它可以创建进程，更重要的是被创建的进程可以继承创建进程的权力，这一点同网络上加载程序结合就可以在远端服务器上安装“间谍”软件。

操作系统运行时，一些系统进程总是等待一些条件出现，一旦满足条件，程序就继续运行下去，黑客也可以利用这样的软件为进程创造条件，使系统程序的运行方向偏离正常轨道。

还有，操作系统安排有无口令入口，这原是为系统开发人员提供的便捷入口，但也可能成为黑客的通道；另外，操作系统还有隐蔽通道，“黑客”一旦测得，便可控制他人的操作系统。

网络通信协议和网络软件也都包含有许多不安全的因素，存在许多漏洞，比如 TCP/IP（传输控制协议/网络协议）在包监视、泄露、地址欺骗、序列号攻击、路由攻击、拒绝服务、鉴别攻击等方面存在漏洞；应用层比如 FTP（文件传输协议）、E-mail（电子邮件）、RPC（远程程序通信协议）、NFS（网络文件系统）等也同样有许多安全隐患。

计算机系统硬件和通信设施极易遭受到自然环境因素的影响（如：温度、湿度、灰尘度和电磁场等的影响）以及自然灾害（如：洪水、地震等）的物理破坏，一旦出现硬件故障则必然造成通信中断。

通信设施的人为破坏包括故意损坏和非故意损坏。一旦信息进入通信线路，就存在被他人获取或破坏的可能。通过无源线路窃听，“黑客”可以获取网络中的信息内容；通过有源线路窃听，破坏者可以对信息流内容进行伪造或删除，甚至可以模仿合法用户破坏信息传输；信息进入通信线路还容易受到电磁辐射和串音的干扰，这些都可对传输的信号造成严重的破坏。

另外，数据库系统因为其共享性、独立性、一致性、完整性和可访问性等诸多优点，已成为计算机系统存储数据的主要形式，但由于它的应用在安全方面考虑较少，容易造成存储数据的丢失、泄漏和破坏。

以上种种问题都是网络系统的脆弱性所在，而在这些问题中有些是难以避免的。网络系统存在诸多弱点，黑客的攻击手段却在不断提高，这就对本来十分脆弱的网络系统造成了严重的安全威胁。

安全威胁这种对安全的潜在侵害在网络系统中主要表现在以下方面：

- 非授权访问：没有预先经过同意，就使用网络或计算机资源，如有意避开系统访问控制机制，对网络设备及资源进行非正常的使用，或擅自扩大权限，越权访问信息。如假冒、身份攻击、非法用户进入网络系统进行违法操作等都属于非授权访问。
- 泄漏信息：指敏感数据在有意或无意中被泄漏出去或丢失，通常包括信息在传输中丢失或泄漏，信息在存储介质中丢失或泄漏。如黑客通过各种手段截获用户的口令、账号等。
- 破坏信息：以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用。
- 拒绝服务：通过不断对网络服务系统进行干扰，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。典型的拒绝服务有资源耗尽和资源过载。最早的拒绝服务攻击是“电子邮件炸弹”，它能使用户在短时间内收到大量电子邮件，使用户系统不能处理正常业务，严重时会使系统崩溃、网络瘫痪。
- 计算机病毒：通过网络传播计算机病毒，破坏性巨大，而且很难防范。

上述威胁有内部威胁和外部威胁。内部威胁如系统的合法用户以非授权方式访问系统，多数已知的计算机犯罪都和系统安全遭受损害的内部攻击有密切的关系。外部威胁的实施也称远程攻击。外部攻击可以使用的办法有搭线(主动的与被动的)、截取辐射、冒充是系统的授权用户或系统的组成部分、对鉴别或访问控制机制设置旁路等。

1.4 计算机网络安全的体系结构

因为网络软、硬件都可能存在安全漏洞，不可能十全十美，无懈可击，又有各种威胁的存在，使得网络安全事件频频发生，要想使网络尽可能的安全可靠，损失尽可能小，这就使得人们必须利用其他的手段来维护这个网络体系，即依据一定的安全策略建立一个网络安全防护体系。

安全策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则。实现网络的安全，不但要靠先进的技术，也要靠严格的管理、法律约束和安全教育。当前制定的网络安全策略主要包括五个方面的策略：物理安全策略、访问控制策略、防火墙控制、信息加密策略和网络安全管理策略。

由于网络安全不仅仅是一个纯技术问题，单凭技术因素是不可能确保网络安全的，因此，网络安全问题涉及法律、管理和技术等多方面的因素。网络安全体系是由网络安全法律体系、网络安全管理体系和网络安全技术体系组成，这三者是相辅相成的。

网络技术安全包括物理安全、网络安全和信息安全。

(1) 物理安全

物理安全是指用装置和应用程序来保护计算机和存储介质的安全，主要包括环境安全、设备安全和媒体安全。

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。

要保障区域安全，应设立电子监控，而要在灾难发生时使损失尽可能小，则应设立灾难的预警、应急处理和恢复机制。

2) 设备安全：主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。

- 防盗　要求门窗上锁，并可在安全等级较高的场地安装报警器。
- 防毁　即要防火、防水。要求设备外壳要有接地保护，以防在有电泄漏时起火对设备造成毁坏。
- 防电磁信息辐射泄漏　常用方法有屏蔽、滤波、隔离、接地、选用低辐射设备和加装干扰装置。将计算机和辅助设备用屏蔽材料封闭起来，既可防止屏蔽体内的泄漏源产生的电磁波泄漏到外部空间，又可阻止外来电磁波进入屏蔽体；信号线上加装合适的滤波器可以阻断传导泄漏的通路；把需要重点防护的设备从系统中分离出来，可切断其与其他设备间电磁泄漏的通路；良好的接地可以给杂散电磁能量一个通向大地的低阻回路，从而在一定程度上分流可能经电源线和信号线传输出去的杂散电磁能量。
- 防止线路截获　首先是预防，当然还需用检测仪器进行探测、定位，然后实施对抗。
- 电源保护　要求使用 UPS、纹波抑制器等。

3) 媒体安全：包括媒体数据的安全及媒体本身的安全。

媒体本身的安全要求媒体安全保管，比如防盗、防毁、防霉等。媒体数据安全要求防复制、防消磁、防丢失等。

(2) 网络安全

网络安全是指主机、服务器安全，网络运行安全，局域网安全以及子网安全。要实现网络安全，需要内外网隔离、内部网不与网络安全域隔离、及时进行网络安全检测、对计算机网络进行审计和监控，同时更重要的是网络反病毒和网络系统备份。

- 在内部网与外部网之间设置防火墙，用以实现内外网的隔离与访问控制，这是保护内网安全的最主要、最有效、最经济的措施之一。
- 内部网的不同网段之间的敏感性和受信任度不同，在它们之间设置防火墙可以限制局部网络安全问题对全局网络造成的影响。
- 用网络安全检测工具对网络系统定期进行安全性分析，发现并修正存在的弱点和漏洞可以及时发现网络中最薄弱的环节，以最大限度地保证网络系统的安全。
- 审计是记录用户使用计算机网络系统进行所有活动的过程，对于确定是否有网络系统攻击情况，审计信息对于确定问题和攻击源很重要。另外，对安全事件的不断收集、积累和分析，可以对某些站点和用户进行审计跟踪。
- 在网络环境下，由于计算机病毒的威胁和破坏是不可估量的，反病毒的实现可通过对网络服务器中的文件进行频繁扫描和监控，在工作站上对网络目录和文件设置访问权限等。
- 备份不仅在网络系统硬件故障或人为失误时起到保护作用，在入侵者非授权访问或对网络进行攻击破坏数据完整性时也起到保护作用。更重要的是，它是系统灾难恢复的前提之一。

(3) 信息安全

信息安全就是要保证数据的机密性、完整性、抗否认性和可用性。网络上的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，计算机病毒防治和数据加密等。

从加强安全管理的角度出发，可以认为，网络安全首先是管理问题，然后才是技术问题。

系统的安全管理在行政安排上一般基于以下三个原则：

- 多人负责原则：每一项与系统安全有关的工作进行时都必须有两人或多人在场。
- 任期有限原则：安全管理的职务最好不要长期由某个人担任，这样可以防止某些人利用长期的工作机会，从事有损他人利益的活动而不容易被发现。
- 职责分离原则：进行信息处理系统工作的人员不要打听、了解或参与本人业务范围以外的与安全有关的事情。

遵守以上原则并不困难，而是难在要始终坚持。

网络安全管理要做的具体工作包括：

- 根据工作的重要程度，确定系统的安全等级；根据确定的安全等级，确定安全管理范围；根据安全管理范围，分别进行安全管理。比如对安全等级较高的系统实施分区控制等。
- 制定严格的安全制度，如机房出入管理制度、设备管理制度、软件管理制度、备份制度等。
- 制定严格的操作规程，遵循职责分离和多人多责的原则，各司其职，各负其责，做到事事

有人管，人人不越权。

- 制定完备的系统维护制度，对系统维护前应报主管部门批准，维护时要详细记录故障原因、维护内容、系统维护前后的状况等。
- 制定应急恢复措施，以便在紧急情况下尽快恢复系统，使其正常运行。
- 加强人员管理，对调离人员要求其有安全保密义务，并及时收回其相关证件和钥匙，工作人员调离时还要及时调整相应的授权并修改相关口令。

1.5 计算机网络安全的设计

有些用户在系统与网络安全保障上，把关注点仅仅放在选择防火墙产品上，实际上这是很片面的。网络安全是整体的、动态的，它的整体性是指安全系统既包括安全设备，又包括管理手段，动态性则是说随着环境和时间的变化，系统的安全性有可能不同。所以，防火墙并不能实现全部要素，要选择具有不同安全功能的设备系统和管理措施有机地结合。

在进行网络系统安全方案规划设计时，应遵循以下原则：

(1) 需求、风险、代价平衡分析的原则

对任一网络，绝对安全是难以达到的。对一个网络的投入与产出要相匹配，所以要对网络系统进行实际的研究(包括任务、性能、结构、可靠性、可维护性等)，并对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，然后制定规范和措施，确定系统的安全策略。

(2) 一致性原则

一致性原则是指网络系统的安全问题与整个网络的工作周期要同时存在，制定的安全体系结构也必须与网络的安全需求相一致。在网络建设的开始，比如网络系统设计及实施计划时，就要考虑网络安全对策，这样比在网络建设好后再考虑安全措施要容易，且花费也少。

(3) 综合性、整体性原则

要用系统工程的观点方法、分析网络的安全，制定具体措施。安全措施主要包括：行政法律手段、各种管理制度以及专业技术措施。多种方法适当综合的安全措施才会是比较好的措施。

不同的网络会有不同的安全措施，但任何网络安全都应遵循整体安全性原则，要根据确定的安全策略制定出合理的网络安全体系结构。

(4) 易操作性、方便用户原则

安全措施如果过于复杂，对人的要求过高，本身就降低了安全性，因此，设计时要方便用户操作，且措施的实施不能影响系统的正常运行。

(5) 适应性及灵活性原则

随着网络性能及安全需求的变化，安全措施必须能灵活适应，而且要容易修改和升级。

(6) 动态化原则

用户的增加、网络技术的快速发展，使得安全防护也需要不断地发展，所以制定安全措施要尽可能引入更多的可变因素，使之具有良好的扩展性。

(7) 有效性和实用性原则

实用性即要能最大限度地满足实际工作要求，它是任何信息系统在建设过程中所必须考虑的一种系统性能。有效性是必须要保证系统的安全。所以，设计的系统要在保证安全的基