中等职业学校计算机技能型
紧缺人才培养规划教材 计算机网络技术及应用专业

计算机信息安全基础教程

韩祖德 编

www.ptpress.com.cn
免费提供
教学相关资料

人民邮电出版社
POSTS & TELECOM PRESS

中等职业学校计算机技能型紧缺人才培养规划教材

计算机网络技术及应用专业

计算机信息安全基础教程

韩祖德　编

人民邮电出版社

图书在版编目（CIP）数据

计算机信息安全基础教程 / 韩祖德编. —北京：人民邮电出版社，2005.9
中等职业学校计算机技能型紧缺人才培养规划教材
计算机网络技术及应用专业

ISBN 7-115-13293-3

Ⅰ. 计… Ⅱ. 韩… Ⅲ. 电子计算机—安全技术—专业学校—教材 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2005）第 101857 号

内 容 提 要

本书简要地介绍计算机以及计算机网络安全的基础知识和基本技术。主要内容包括：计算机信息安全的概念、密码技术、操作系统安全、 数据库安全、应用系统安全、计算机病毒及防范、防火墙、入侵检测技术及安全扫描技术等内容。本书的重点是实训，重点介绍网络的检测、安全设置和网络管理工具的使用。通过实训，读者可以具有网络检测、安全设置和管理工具的实践与使用等技能。

本书为中等职业学校计算机相关专业教材，也可作为计算机爱好者的自学用书。

中等职业学校计算机技能型紧缺人才培养规划教材

计算机网络技术及应用专业

计算机信息安全基础教程

◆ 编　　韩祖德
责任编辑　潘春燕
执行编辑　韩学义
◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销
◆ 开本：787×1092　1/16
印张：9.25
字数：215 千字　　2005 年 9 月第 1 版
印数：1－3 000 册　　2005 年 9 月北京第 1 次印刷

ISBN 7-115-13293-3/TP・4592

定价：14.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223

中等职业学校计算机技能型紧缺人才培养规划教材

编 委 会

丛书前言

实施信息化的关键在人才，在我国各行各业都需要大批的各个层次的计算机应用专业人才。在未来几年内，我国经济和社会发展对计算机应用与软件专业初级人才具有很大的需求，而这些人才的培养主要应由中等职业教育来承担。要培养具备综合职业能力和全面素质，直接在生产、服务、技术和管理等第一线工作的技能型人才，必须在课程开发上，从职业岗位技能分析入手，以教材建设推动中等职业教育教学改革，从而提高中等职业教育质量。

人民邮电出版社根据《教育部等七部门关于进一步加强职业教育工作的若干意见》的指示精神，在深入调查研究的基础上，会同企业技术专家、中等职业学校教师、职业教育教研人员按照专业的“培养目标与规格”教学要求进行整体规划设计了本套教材。本套教材以教育部办公厅、信息产业部办公厅联合颁布的“中等职业学校计算机应用与软件技术专业领域技能型紧缺人才培养培训指导方案”为依据，遵循“以全面素质为基础，以职业能力为本位；以企业需求为基本依据，以就业为导向；适应行业技术发展，体现教学内容的先进性和前瞻性；以学生为主体，体现教学组织的科学性和灵活性”等技能型紧缺人才培养培训的基本原则。

本套教材适用于中等职业学校计算机及相关专业，按计算机软件、多媒体应用技术、计算机网络技术及应用等 3 个专业组织编写。在教学内容的编排上，力求着重提高受教育者的职业能力，具备如下特色特点：

（1）在具备一定的知识系统性和知识完整性的情况下，突出中等职业教育的特点，在写作的过程中把握好“必须”和“足够”这两个“度”。

（2）任务驱动，项目教学。让学生零距离接触所学知识，拓展学生的职业技能。

（3）按照中等职业教育的教学规律和学生认知特点讲解各个知识点，选择大量与知识点紧密结合的案例。

（4）由浅及深，由易到难，循序渐进，通俗易懂，理论与案例制作相结合，实用与技巧相结合。

（5）注重培养学生的学习兴趣、独立思考能力、创造性和再学习能力。

（6）适量介绍有关业内的专业知识和案例，使学生学习后可以尽快胜任岗位工作。

为了方便教师教学，我们提供辅助教师教学的“电子教案、习题答案以及模拟考试试卷”，其中部分教材配备为老师教学而提供的多媒体素材库，并发布在人民邮电出版社网站（www.ptpress.com.cn）的下载区中。

随着中等职业教育的深入改革，编写中等职业教育教材始终是一个新课题；我们衷心希望，全国从事中等职业教育的教师与企业技术专家与我们联系，帮助我们加强中等职业教育教材建设，进一步提高教材质量。对于教材中存在的不当之处，恳请广大读者在使用过程中给我们多提宝贵意见。联系方式：zhangmengwei@ptpress.com.cn

编者的话

计算机特别是计算机网络的应用，使信息技术得以迅速发展。

信息网络技术的应用在以 Internet 为代表的全球性信息化浪潮的推动下，正日益普及和广泛，应用层次越来越深入，应用领域从传统的、小型业务系统逐渐向大型的、关键业务系统扩展，典型的如政府部门信息系统、金融业务系统、企业商务系统等。伴随着网络的普及，网络安全日益成为影响网络效能的重要因素。

目前我国计算机安全防护能力处于初级阶段，许多计算机基本处于不设防的状态。计算机的安全问题解决不好，不仅会给国家、企业和个人造成巨大的经济损失，严重的还将危及国家的安全和社会的稳定。当今的计算机技能型人才，必须具有计算机安全意识并掌握一定的计算机安全技术。

本书针对中等职业学校学生的特点进行编写，以培养学生计算机安全意识和使学生具有一定的计算机安全技术为目标。计算机信息安全技术涉及面极广，包含的内容技术含量也比较高，本书只试图对其中的基本问题进行较为通俗的介绍。

本书分为 8 章。第 1 章对计算机安全、计算机网络安全的概念以及信息安全的分类、信息安全的级别作一般性的介绍；第 2 章介绍数据加密技术的概念以及主要的加密技术；第 3 章介绍操作系统的安全并重点讨论了 Windows 2000/XP 的安全；第 4 章重点讨论数据库的安全；第 5 章介绍应用系统安全的概念，重点讨论了 Web 站点安全和 Web 客户端的安全防范；第 6 章讲述恶意代码与病毒、计算机病毒、病毒的防治；第 7 章主要介绍防火墙的基本概念以及个人防火墙的使用；第 8 章重点讲述计算机黑客、网络监听、安全扫描技术以及入侵检测等内容。

教材中对基本概念、基础知识的介绍力求简明扼要，各章相互配合又自成体系并附有习题。本书还提供了 12 个实训，从而使学生能够在实践中了解并学习计算机安全技术的应用。

本书在编写过程中得到了北京蓝波今朝科技有限公司的大力支持，在此表示真诚的感谢。由于时间仓促，水平有限，书中难免有疏漏之处，希望广大读者提出中肯的批评意见。

编者

2005 年 7 月

目　录

计算机信息安全概述

第1章

本章知识要点：计算机安全和计算机网络安全的概念；信息安全的分类和信息安全的级别。

- 信息安全和计算机安全
- 计算机网络安全的概念、网络安全的5层体系
- 信息安全的分类
- 信息安全的级别
- 安全策略的概念

从计算机发明的那一天起，直到计算机网络飞速发展的今天，安全问题一直是信息处理、存储、交换的首要问题。而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对计算机信息安全提出了更高的要求。

我们先看看几个历史上计算机安全事件及其造成的危害。

1988 年 11 月 2 日，美国康乃尔大学的研究生罗伯特·莫里斯编制了一个被称为“蠕虫”的程序，并将它放入 Internet 中，使美国军方的 MIL 网和 APPA 网中的 6000 台计算机受到感染，并致使欧洲一些连网的计算机也被感染。该行为造成的直接经济损失近亿美元。

2000 年 2 月 7 日，连续数日，来历不明的黑客对美国的“亚马逊”、“雅虎”、“微软”等众多知名网站实施大规模的网络袭击行动，使网络服务器无法运行，造成服务中断数小时。

2003 年，Slammer 病毒在 1 月 25 日发作，针对 SQL Server 数据库漏洞，光是发作的头五天，就造成全球 10 亿美元的损失。

1998 年，一连串的网络非法入侵事件改变了中国网络安全“一片空白”的历史。有媒体报道，中国 95%以上与 Internet 相连的信息中心都遭受过境内或境外黑客的侵入或攻击。

从上面的案例可以看出，计算机尤其是计算机网络必须采取多种安全措施，才能保障正常工作。

1.1 计算机安全和网络安全的概念

计算机信息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科学。

1.1.1 信息安全和计算机安全

1. 信息安全的概念

信息安全包括 5 个基本要素：保密性、完整性、可用性、可控性与可审查性。

（1）信息的保密性：指确保信息不暴露给未经授权的实体或进程。

（2）信息的完整性：指只有得到允许的人才能访问数据，并且能够判别出数据是否已被修改。

（3）信息的可用性：指得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。

（4）信息的可控性：表示控制授权范围内的信息流向及行为方式。

（5）信息的可审查性：指对出现的网络安全问题提供调查的依据和手段。

一个现代化的信息系统若不包含有效的信息安全技术措施，就不能认为是完整的和可信的。

2. 计算机安全的概念

（1）国际标准化组织（ISO）的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然或恶意的原因遭到破坏、更改和泄露。

（2）我国公安部的定义：计算机系统的硬件、软件、数据受到保护，不因偶然的或恶意的原因而遭到破坏、更改、泄露，保证系统能正常运行。

1.1.2 计算机网络安全

网络安全和单台计算机安全的目标并没有本质的区别，但对网络安全的要求要远远高于单台计算机。

1. 计算机网络安全的概念

计算机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原因而遭到破坏、更改、泄露，确保系统能连续可靠正常地运行，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，从广义的角度讲，凡是涉及到网络上信息的保密性、完整性、可用性、可控性与真实性都属于网络安全研究的范畴。

2. 网络安全的目标

网络安全的主要目标如下。

（1）网络服务的可用性：必须保证网络服务的正常使用，如可以抵御拒绝服务等攻击。

（2）网络信息的保密性：网络服务必须能够防止重要信息的泄露，要求只有在授权的情况下才能获得重要信息。

（3）网络信息的完整性：网络服务必须保证信息的内容不能被非授权者有意或无意篡改。

（4）网络信息的非否认性：要保证网络上的用户不能否认信息的发送或接收。

（5）网络运行的可控性：指网络管理的可控性，包括网络运行的物理可控性和逻辑可控性，要求能够有效地控制网络用户的行为以及信息的传播范围。

3. 网络安全的5层体系

网络安全主要涉及5个方面的问题。

（1）用户是否安全：要保证只有真正被授权的用户才能使用系统中的资源和数据。

可采取对用户进行分组管理，根据不同的安全级别将用户分成若干等级，每一等级的用户只能访问与其等级相对应的系统资源和数据。还应该具有较强的身份认证能力，确保用户的密码不会被外人获取。

（2）操作系统是否安全：主要是要避免病毒的威胁和黑客对操作系统的侵入和破坏。

（3）应用程序是否安全：要保证只有合法的用户才能对重要的数据进行操作。

主要包括：应用程序对数据的合法权限，如，上级部门的应用程序能够存取下级部门的数据，而下级部门的应用程序一般不能允许存取上级部门的数据，另外同级部门的应用程序的存取权限也应有所限制。

（4）网络是否安全：主要是网络能够得到控制，即可以控制进入网络的 IP 用户。

（5）数据是否安全：主要是保证加密数据能够处于机密状态。

1.2 信息系统安全面临的威胁

1.2.1 安全威胁的种类

1. 物理威胁

计算机硬件、存储介质和数据也是偷窃者的目标。常见的物理安全问题有：偷窃、废物搜索和间谍活动等，计算机偷窃行为所造成的损失可能远远超过计算机本身的价值。通常计算机内存储的数据的价值远远高于计算机设备本身，因此必须采取严格的防范措施，以确保计算机设备尤其是计算机内信息存储设备的安全。

2. 意外威胁

意外威胁是由于系统管理员的疏忽或用户的无知，没有预先思考或计划而引起的。例如，用户远程访问一个系统时，可能会无意中进入一个没有被先前登录的用户彻底终止的登录会话。如果先前的用户在查看一个很机密的文件，这个文件只有经过授权的用户才能打开，但是当这个用户结束自己的会话时，并没有将这个文件的查看程序关闭，那么新登录的用户就可以很容易地浏览整个文件的内容，从而造成泄密。

3. 故意威胁

故意威胁是有企图的行为的结果，是计划好的活动。威胁的范围从简单的不修改数据的文件检查，到整个系统中进行体系的改变以致造成恶意的损坏。故意威胁可以进一步分为被动威胁和主动威胁。

（1）被动威胁。这类威胁包括在网络上使用探测器读取正在发送的数据包，而不修改数据包的内容，数据的合法用户很可能不知道这种活动的存在。这种类型的活动通常不被记录。

（2）主动威胁。包括的行为有：反复的尝试访问和修改存储在操作系统中的信息；还包括生成大量的数据包来阻塞网络。

1.2.2 网络安全威胁的表现形式

目前，网络中存在的威胁主要表现为以下几个方面。

1. 非授权访问

没有预先经过同意，就使用网络或计算机资源，就是非授权访问。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使用，或擅自扩大权限，越权访问信息。它主要有以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权

方式进行访问等。

2. 信息泄漏或丢失

信息泄漏或丢失指敏感数据在有意或无意中被泄漏或丢失，它通常包括：信息在传输中丢失或泄漏；信息在存储介质中丢失或泄漏。

3. 破坏数据的完整性

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，如恶意添加、修改数据，以干扰用户的正常使用。

4. 拒绝服务攻击

不断对网络服务系统进行干扰，改变正常的作业流程，或执行无关程序使系统响应减慢甚至瘫痪，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得不到相应的服务。

5. 用网络传播病毒

通过网络传播计算机病毒，其破坏性远大于单机病毒，而且用户很难防范。

1.3 计算机安全分类和主要安全技术简介

1.3.1 计算机安全分类

根据中国国家计算机安全规范，计算机的安全大致可分为如下 3 类。

（1）实体安全：包括机房、线路和主机等的安全。

（2）网络与信息安全：包括网络的畅通、准确以及网上信息的安全。

（3）应用安全：包括程序的开发允许、I/O、数据库等的安全。

其中，网络与信息安全可分为如下 4 类。

① 基本安全类：包括访问控制、授权、认证、加密以及内容安全。

② 管理与记账类：包括安全策略的管理、实时监控、报警以及企业范围内的集中管理与记账。

③ 网络互连设备类：包括路由器、通信服务器和交换机等。

④ 连接控制类：包括负载均衡、可靠性以及流量管理等。

1.3.2 主要安全技术

从广义上讲，计算机信息安全技术主要有以下几个。

（1）主机安全技术。

（2）身份认证技术。

（3）访问控制技术。

（4）数据加密技术。

（5）防火墙技术。

（6）安全审计技术。

（7）安全管理技术。

我们应该在了解计算机信息安全技术的基础上，尽快掌握使用计算机信息安全产品的技

术，不断提高实现信息安全的能力，以适合我国信息化对信息安全的需求。

1.4 系统安全级别

1. 美国的“可信计算机系统评估准则”（TCSEC）

这个安全性级别是美国国防部制订的，共有 A、B、C、D 四级，A 级最高，D 级最低。国际上经常使用该标准来评价一个计算机系统的安全性。各个级别的主要特点如下。

（1）D 级

D 类级别是最低的安全级别，该级别的操作系统没有系统访问和数据访问限制，操作者不需任何账户均可随意进入该系统，同时可以随意访问其他用户的数据文件。因为 D 级别的系统无任何安全性防护，所以属于最不安全的系统。

例如，DOS、Windows 3.X 和 Windows 95 操作系统的安全性级别就属于 D 级。

（2）C 级

分为 C1 和 C2 两个子级别。

① C1 级：该级别也叫做选择性安全保护系统。其主要特点为：

- 所有的用户都被分组；
- 对于每个用户，必须登记后才能使用系统；
- 系统必须记录每个用户的登记；
- 系统必须对可能破坏自身的操作发出警告。

例如，标准 UNIX 和低版本的 NetWare 操作系统的安全性级别就属于 C1 级。

② C2 级：在满足 C1 条件的基础上，增加以下几条要求：

- 所有的对象都有且仅有一个物主；
- 对于每个试图访问对象的操作，都必须检验权限，对于不符合权限要求的访问，必须予以拒绝；
- 有且仅有物主和物主指定的用户可以更改权限；
- 管理员可以取得对象的所有权，但不能归还；
- 系统必须保证自身不能被管理员以外的用户改变；
- 系统必须有能力对所有的操作进行记录，并且只有管理员和由管理员指定的用户可以访问该记录。

例如，SCO UNIX 和 Windows NT 操作系统的安全性级别就属于 C2 级。

（3）B 级

分为 B1、B2、B3 三个子级别。

① B1：在满足 C2 条件的基础上，增加以下几条要求：

- 不同的组成员不能访问对方创建的对象，但管理员许可的除外；
- 管理员不能取得对象的所有权。

Windows NT 的定制版本可以达到 B 级。

② B2：在 B1 的基础上，增加以下几条要求：

- 所有的用户都被授予一个安全等级；
- 安全等级较低的用户不能访问高等级用户创建的对象。

银行的金融系统通常达到B2级。

③ B3：在满足B2的基础上，使用安装硬件的方法来加强安全。

（4）A级

A级别在B2的基础上，增加以下要求：系统的整体安全策略一经建立便不能修改。

A级安全性要求过高，目前商品化的操作系统没有达到A级要求的。

2. 中国国家标准——《计算机信息安全保护等级划分准则》

该准则将计算机信息系统安全保护等级划分为5个级别。

（1）用户自主保护级（第一级）：本级的安全保护机制通过隔离用户与数据，使用户具备自主安全保护能力，保护用户和用户组信息，避免其他用户对数据的非法读写和破坏。

（2）系统审计保护级（第二级）：具备第一级的所有安全保护功能，并实施了更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。

（3）安全标记保护级（第三级）：具备第二级的所有安全保护功能，此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；消除通过测试发现的任何错误。

（4）结构化保护级（第四级）：具备第三级的所有安全保护功能，并将安全保护机制划分成关键部分和非关键部分相结合的结构，其中关键部分直接控制访问者对访问对象的存取。本级具有相当强的抗渗透能力。

（5）访问验证保护级（第五级）：具备第四级的所有安全保护功能，还提供：支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。

1.5 安全策略的制定与实施

1.5.1 安全策略

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。安全策略模型包括了建立安全环境的三个重要组成部分，即威严的法律、先进的技术、严格的管理。

1. 法律措施

安全的基石是社会法律、法规与手段，这部分用于建立一套安全管理标准和方法。即通过建立与信息安全相关的法律、法规，使非法分子慑于法律，不敢轻举妄动。

2. 技术措施

先进的安全技术是信息安全的根本保证，用户对于自身面临的威胁进行风险评估，决定其需要的安全服务种类。选择相应的安全机制，然后集成先进的安全技术。

3. 管理措施

各网络使用机构、企业和单位应建立相宜的信息安全管理方法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。安全策略参考与制定原则如表1.1所示。

表 1.1 安全策略参考与制定原则

安全策略参考	安全策略的制定原则
网络规划安全策略	
网络管理员安全策略	适应性原则
访问服务网络安全策略	动态性原则
远程访问服务网络安全策略	简单性原则
系统用户的安全策略	系统性原则
上网用户的安全策略	最小授权原则
远程访问用户的安全策略	
直接风险控制安全策略	
自适应网络安全策略	
智能网络系统安全策略	

1.5.2 安全工作的目的

安全工作的目的就是为了在安全法律、法规、政策的支持与引导下，通过采用合适的安全技术与安全管理措施，完成以下任务。

（1）用访问控制机制，阻止非授权用户进入网络，即“进不来”，从而保证网络系统的可用性。

（2）使用授权机制，实现对用户的权限控制，即不该拿走的“拿不走”，同时结合内容审计机制，实现对网络资源及信息的可控性。

（3）使用加密机制，确保信息不暴露给未授权的实体或进程，即“看不懂”，从而实现信息的保密性。

（4）使用数据完整性鉴别机制，保证只有得到允许的人才能修改数据，而其他人“改不了”，从而保证信息的完整性。

（5）使用审计、监控、防抵赖等安全机制，使得攻击者、破坏者、抵赖者“走不脱”，并进一步对网络出现的安全问题提供调查依据和手段，实现信息安全的可审查性。

习 题

1. 什么是计算机信息安全？
2. 信息安全的 5 要素是什么？
3. 什么是计算机网络安全？
4. 简述网络安全的 5 层体系的内容。
5. 计算机信息系统面临的威胁有哪些？
6. 计算机的安全大致可分为哪几类？
7. 我国系统安全有哪些级别？
8. 安全策略由哪几部分组成？