21世纪高等教育规划教材

计算机安全技术

侯迎春　主编

SWJUP 西南交通大學出版社
Http://press.swjtu.edu.cn

21世纪高等教育规划教材

计算机安全技术

主　编　侯迎春
副主编　刘传领　邢文凯

西南交通大学出版社
·成　都·

内 容 简 介

计算机安全主要包括操作系统安全、数据库安全和网络安全三部分，尤其是网络安全。本书首先介绍了计算机安全的基础知识、计算机软件安全、计算机病毒，接着用了大量的篇幅介绍网络安全的相关内容，其中涉及访问控制与防火墙技术、加密与认证、网络监听与端口扫描、网络攻防、入侵检测、安全审计与系统恢复、Windows XP 的安全、数据库安全等。

本书适合作为高职高专计算机类专业及需要掌握计算机安全技术的相近专业的课程教材，配合本书的课件，也可供自学者使用。

图书在版编目(CIP)数据

计算机安全技术/侯迎春主编. —成都：西南交通大学出版社，2008.10

21 世纪高等教育规划教材

ISBN 978-7-5643-0098-2

Ⅰ.计… Ⅱ.侯… Ⅲ.电子计算机—安全技术—高等学校—教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2008)第 159181 号

21 Shiji Gaodeng Jiaoyu Guihua Jiaocai

21 世纪高等教育规划教材

Jisuanji Anquan Jishu

计算机安全技术

主 编 侯迎春

*

责任编辑 张华敏

特邀编辑 高青松 李科亮

封面设计 水木时代

西南交通大学出版社出版发行

(成都市二环路北一段 111 号 邮政编码：610031 发行部电话：028-87600564)

http://press.swjtu.edu.cn

北京广达印刷有限公司印刷

*

成品尺寸：185 mm×260 mm 印张：15

字数：399 千字

2008 年 10 月第 1 版 2008 年 10 月第 1 次印刷

ISBN 978-7-5643-0098-2

定价：28.80 元

前　言

计算机安全技术是一个涉及计算机科学、网络技术、通信技术等多种学科的边缘性综合学科。随着对计算机系统及网络安全的研究与应用的日益广泛和深入，目前从事计算机安全技术的研究、设计和教学工作的科技工作者越来越多，许多高等院校也陆续开设了这方面的课程或增设专业和研究方向。社会上对计算机安全人才，特别是动手能力较强的计算机类毕业生的需求非常迫切，这给“计算机安全技术”课程的课堂教学与实践环节提出了新的更高的要求。

本书根据应用型计算机科学与技术专业的培养目标、特点和要求，全面、系统地介绍了计算机安全与保密技术方面的知识。以计算机系统及网络安全技术实际应用为主线，将安全理论、安全工具与安全实践三方面内容有机地结合在一起，较全面地介绍了计算机系统及网络安全技术的基本概念和基础知识，突出实用性、可操作性和连贯性。

本书以作者多年来的课堂教学和实际开发应用系统的经验体会为基础，同时参考大量有关计算机安全方面的最新资料而编成。无论是学习计算机安全技术的新手，还是已有丰富经验的读者，通过阅读本书都可以加深对计算机安全技术的理解并从中受益。

全书从内容体系上分成四部分。

第一部分：包括第 1 章到第 3 章，介绍计算机系统及网络安全的基础知识。其中第 1 章介绍计算机安全的基础知识、网络安全的层次体系、网络安全标准及安全等级、对网络安全的攻击类型、网络安全机制应具有的功能以及网络安全常用的技术、计算机软件安全和计算机病毒。第 2 章介绍访问控制的有关概念，包括访问控制的概念和目标、访问控制策略和机制、授权的管理、网络访问控制组件的分布，并给出了 Windows XP 的访问控制实例。第 2 章还介绍了主流防火墙技术、防火墙技术的发展趋势、分布式防火墙技术、防火墙的工作模式、防火墙设计以及防火墙中的安全策略配置等内容。第 3 章介绍加密与认证技术，包括对称密钥加密、公开密钥密码体制和常用公钥算法、单向散列算法以及加密技术的应用，讨论认证机制和认证系统、公钥基本结构(PKI)的概念和证书服务的基础知识。

第二部分：包括第 4 章到第 7 章，介绍网络安全的攻击和防御技术，以及远程攻击与监控技术、入侵检测、安全审计和系统恢复等内容。其中第 4 章主要介绍网络攻击技术中的网络扫描和监听技术，重点介绍扫描技术中的被动策略扫描和主动策略扫描，以及网络监听的概念和 Sniffer 监听工具的使用。第 5 章介绍黑客攻击的目的、黑客入侵的一般步骤、网络后门的概念与黑客隐身的方法、木马和网络代理跳板以及黑客常用的网络攻击手段。第 6 章介绍网络入侵检测、手工检测入侵的方法及入侵检测产品，并介绍了如何用 Snort 建立一个入侵检测系统和分布式攻击的防范策略以及黑客诱骗技术。第 7 章介绍审计的具体要求、电子政务安全审计中应重点审计的几个方面以及如何恢复被入侵的系统。

第三部分：包括第 8 章和第 9 章，介绍系统的安全与防护，主要是介绍安全综合解决方案。其中第 8 章介绍操作系统安全，例如 Windows 操作系统的安全配置方案。第 9 章介绍应用软件安全漏洞分析、数据库攻击和安全、大型数据库的常见安全漏洞、常见的编程错误引起的安全漏洞、数据库安全基本架构、攻击数据库的常用方法、数据库加密技术、数据库的备份与灾难恢复以及数据库安全性策略等内容。

第四部分：这部分主要是第10章，主要介绍本课程的实验指导内容，目的是让学生从实践中验证有关理论知识和技术的应用，并通过一系列的相关实训提高学生对计算机系统、网络管理与网络安全方面的技能和解决实际问题的能力，强调理论与实践相结合，着重培养学生理论联系实际能力和网络安全的意识。

由于计算机安全技术的内容非常丰富，本书的理论教学以“必需、够用”为度，加强了实践性教学环节，以提高学生的实际技能的原则组织编写，讲究知识性、系统性、条理性、连贯性，力求激发学生的学习兴趣，精心组织编写内容，做到了由浅入深、由易到难、删繁就简、突出重点、循序渐进，适于课堂教学和实践教学。

考虑到“计算机安全技术”课程的实际情况，本书按教学时数为30学时、实验时数为36学时进行编写。本课程的先修课程为“C/C++语言程序设计”、“数据结构”、“操作系统”、“计算机原理与接口技术”、“计算机网络”，并行课程为“网络系统集成与管理”或“组网技术”。本书全套课件可在 http://jsj.sqzy.edu.cn/网址上下载。

本书由侯迎春担任主编并负责统稿工作，刘传领、邢文凯担任副主编。第1、3、10章由侯迎春编写，第2、4章由李德启编写，第5、6章由刘传领编写，第7章由周子平编写，第8章由魏先勇编写，第9章由邢文凯编写。

本书的出版得到了商丘职业技术学院精品课程建设项目的资助。商丘职业技术学院范建华教授对本书提出了很好的意见与建议，特在此表示感谢！我们在编写本书的过程中参考了某些网站上提供的资料，谨向这些资料的作者和提供者表示感谢！

本书难免有不妥和错误之处，敬请广大读者指正。

编 者

2008年10月

目　录

第 1 章　计算机安全基础知识 …… (1)
1.1　计算机安全概述 …… (1)
1.1.1　计算机系统面临的威胁和攻击 …… (1)
1.1.2　计算机系统安全的重要性 …… (2)
1.1.3　计算机安全技术的发展和现状 …… (2)
1.1.4　计算机安全技术研究的内容和目的 …… (3)
1.1.5　计算机安全系统的设计原则 …… (5)
1.2　网络安全体系结构 …… (6)
1.2.1　网络安全的含义 …… (6)
1.2.2　网络安全存在的问题 …… (6)
1.2.3　网络安全的层次体系 …… (7)
1.2.4　对网络安全的攻击技术和类型 …… (8)
1.2.5　网络安全机制应具有的功能 …… (10)
1.2.6　网络安全常用技术 …… (11)
1.2.7　安全协议 …… (12)
1.3　网络安全标准及安全等级 …… (14)
1.3.1　国际上的安全级别评价标准 …… (14)
1.3.2　我国网络安全评价标准 …… (16)
1.3.3　网络安全的相关法规 …… (16)
1.4　计算机软件安全 …… (17)
1.4.1　软件的安全技术概述 …… (17)
1.4.2　软件分析技术 …… (18)
1.4.3　常用的软件保护技术 …… (19)
1.4.4　软件的加壳与脱壳 …… (24)
1.4.5　软件安全保护建议 …… (25)
1.5　计算机病毒及其防御 …… (26)
1.5.1　计算机病毒基础知识 …… (26)
1.5.2　计算机病毒的防御 …… (30)
习　题 …… (36)
第 2 章　访问控制与防火墙技术 …… (38)
2.1　实体安全概述 …… (38)
2.1.1　物理安全策略 …… (38)
2.1.2　信息存储的备份 …… (39)
2.1.3　安全管理及其他问题的防范 …… (39)
2.2　访问控制 …… (39)

2.2.1 访问控制的概念和目标 …… (39)
2.2.2 访问控制的策略和实现 …… (40)
2.3 防火墙 …… (44)
2.3.1 防火墙技术 …… (44)
2.3.2 防火墙的体系结构 …… (48)
2.3.3 防火墙设计及安全策略配置 …… (51)
2.3.4 防火墙技术的发展趋势 …… (53)
习 题 …… (55)
第 3 章 加密与认证 …… (56)
3.1 密码技术 …… (56)
3.1.1 私钥密码技术 …… (56)
3.1.2 公钥密码技术 …… (59)
3.1.3 PGP 简介 …… (62)
3.1.4 SSH 安全协议 …… (65)
3.2 数字证书、数字认证与公钥基础设施 …… (66)
3.2.1 数字证书 …… (66)
3.2.2 数字认证 …… (67)
3.2.3 公钥基础设施 …… (68)
3.3 加密与认证的应用 …… (70)
3.3.1 虚拟专用网 …… (70)
3.3.2 IP 安全协议 IPSec …… (73)
3.3.3 基于 IPsec 的虚拟专用网 …… (76)
3.3.4 安全套接字层 SSL 及 SSL VPN …… (77)
习 题 …… (80)
第 4 章 端口监听与扫描技术 …… (82)
4.1 计算机网络监听概述 …… (82)
4.1.1 网络监听的原理 …… (82)
4.1.2 检测网络监听的手段 …… (87)
4.2 网络监听工具——Sniffer(嗅探器) …… (88)
4.2.1 Sniffer 的工作环境 …… (88)
4.2.2 Sniffer 网络监听的工作原理 …… (89)
4.2.3 怎样在网上发现 Sniffer …… (90)
4.2.4 怎样防止被 Sniffer …… (91)
4.2.5 Sniffer 软件的安装 …… (91)
4.2.6 使用 Sniffer 查询流量信息 …… (92)
4.3 端口扫描技术 …… (93)
4.3.1 端口扫描的概念 …… (93)
4.3.2 端口扫描技术的原理 …… (93)
4.3.3 端口号 …… (93)
4.3.4 简单端口扫描技术 …… (94)

4.3.5 秘密扫描技术 …… (94)
4.3.6 SOCKS 端口探测技术 …… (95)
4.3.7 反弹扫描 …… (95)
4.3.8 UDP 扫描 …… (96)
4.3.9 ICMP 扫描 …… (97)
4.3.10 端口扫描工具 …… (97)
4.3.11 端口扫描侦察工具 …… (97)
习 题 …… (98)
第 5 章 网络入侵与攻击 …… (99)
5.1 初识黑客 …… (99)
5.2 黑客攻击的目的及步骤 …… (100)
5.2.1 黑客攻击的目的 …… (100)
5.2.2 黑客攻击的一般步骤 …… (101)
5.3 常见的黑客攻击技术 …… (101)
5.3.1 口令攻击 …… (101)
5.3.2 漏洞攻击 …… (102)
5.3.3 拒绝服务攻击 …… (103)
5.3.4 放置特洛伊木马程序 …… (104)
5.3.5 缓冲区溢出攻击 …… (104)
5.3.6 网络中的欺骗技术 …… (109)
5.4 黑客工具 …… (111)
5.4.1 木马程序 …… (111)
5.4.2 扫描工具 …… (112)
5.4.3 破解工具 …… (113)
习 题 …… (115)
第 6 章 入侵检测技术与蜜罐技术 …… (116)
6.1 网络入侵检测概述 …… (116)
6.1.1 信息收集 …… (117)
6.1.2 信号分析 …… (118)
6.2 分层协议模型与 TCP/IP 协议 …… (119)
6.2.1 TCP/IP 协议模型 …… (119)
6.2.2 TCP/IP 协议报文格式 …… (120)
6.3 网络数据包的截获 …… (131)
6.3.1 以太网环境下的数据截获 …… (131)
6.3.2 交换网络环境下的数据截获 …… (131)
6.4 网络入侵检测系统 …… (132)
6.4.1 入侵检测系统概述 …… (132)
6.4.2 入侵检测技术 …… (133)
6.4.3 入侵检测产品选择要点 …… (134)
6.4.4 入侵检测技术发展方向 …… (135)

6.5　蜜罐技术 …… (135)
6.5.1　蜜罐技术 …… (136)
6.5.2　蜜空间技术 …… (136)
6.5.3　蜜网技术 …… (137)
习　题 …… (137)
第 7 章　安全审计与系统恢复 …… (138)
7.1　安全审计 …… (138)
7.1.1　安全审计概述 …… (138)
7.1.2　日志的审计 …… (139)
7.1.3　安全审计的实施 …… (142)
7.2　Windows NT 中的访问控制与安全审计 …… (143)
7.2.1　Windows NT 中的访问控制 …… (143)
7.2.2　Windows NT 中的安全审计 …… (144)
7.3　系统恢复 …… (147)
7.3.1　系统恢复和信息恢复 …… (147)
7.3.2　系统恢复的过程 …… (147)
习　题 …… (153)
第 8 章　Windows XP 的安全 …… (154)
8.1　Windows XP 的安全特性 …… (154)
8.1.1　操作系统的安全 …… (154)
8.1.2　Windows XP 的安全特性 …… (154)
8.1.3　Windows XP 安全架构 …… (156)
8.1.4　安全标识符 …… (157)
8.2　Windows XP 的安全配置 …… (157)
8.2.1　Windows XP 的安装 …… (157)
8.2.2　Windows XP 系统的两种不同登录方式 …… (158)
8.2.3　Windows XP 系统的安全策略 …… (159)
8.2.4　Windows XP 系统“本地安全策略” …… (161)
8.2.5　Windows XP 的组策略 …… (163)
8.3　Windows XP 常用的系统进程和服务 …… (168)
8.3.1　Windows XP 常用的系统进程 …… (168)
8.3.2　Windows XP 的系统服务 …… (169)
8.4　Windows XP 的注册表 …… (171)
8.4.1　注册表由来 …… (171)
8.4.2　注册表基本知识 …… (171)
8.4.3　Windows XP 注册表的备份与恢复 …… (173)
习　题 …… (176)
第 9 章　数据库及应用系统安全 …… (178)
9.1　数据库系统安全概述 …… (178)
9.1.1　数据库系统的组成 …… (178)

9.1.2 数据库系统安全评估标准 …… (180)
9.1.3 数据库系统安全性要求 …… (181)
9.1.4 数据库系统安全框架 …… (181)
9.2 数据库系统安全保护机制 …… (184)
9.2.1 用户标识与鉴别 …… (184)
9.2.2 存取控制 …… (185)
9.2.3 数据库加密 …… (186)
9.2.4 数据库审计 …… (190)
9.2.5 数据库系统的备份与恢复 …… (190)
9.3 SQL 数据库的安全管理 …… (192)
9.3.1 SQL Server 安全管理概述 …… (192)
9.3.2 SQL 数据库安全性控制策略 …… (193)
9.3.3 攻击数据库的常用方法 …… (196)
9.3.4 SQL Server 的安全配置 …… (200)
习 题 …… (204)
第 10 章 计算机安全实验 …… (205)
10.1 软件动态分析技术 …… (205)
10.1.1 实验目的 …… (205)
10.1.2 实验理论基础 …… (205)
10.1.3 实验内容 …… (206)
10.1.4 实验步骤 …… (206)
10.2 PGP 的原理与使用实验 …… (206)
10.2.1 实验目的 …… (206)
10.2.2 实验步骤 …… (207)
10.2.3 思考题 …… (207)
10.3 瑞星防火墙配置实验 …… (207)
10.3.1 实验目的 …… (207)
10.3.2 实验理论基础 …… (208)
10.3.3 实验内容 …… (208)
10.3.4 实验步骤 …… (208)
10.4 使用 Sniffer 捕获加密包和非加密包 …… (208)
10.4.1 实验目的 …… (208)
10.4.2 实验步骤 …… (208)
10.5 端口扫描实验 …… (209)
10.5.1 实验目的 …… (209)
10.5.2 实验原理 …… (209)
10.5.3 实验内容 …… (211)
10.5.4 思考题 …… (211)
10.6 DoS 攻击实验 …… (211)
10.6.1 实验目的 …… (211)

10.6.2 实验内容 …… (211)
10.6.3 实验要求 …… (213)
10.6.4 思考题 …… (213)
10.7 缓冲区溢出实验 …… (217)
10.7.1 实验目的 …… (217)
10.7.2 实验要求 …… (218)
10.7.3 实验内容 …… (218)
10.7.4 思考题 …… (222)
10.8 入侵检测原理与 Snort 的使用实验 …… (222)
10.8.1 实验目的 …… (222)
10.8.2 注意事项和预备工作 …… (222)
10.8.3 实验原理 …… (223)
10.8.4 实验内容 …… (225)
10.8.5 思考题 …… (226)
10.9 剖析特洛伊木马 …… (226)
10.9.1 实验目的 …… (226)
10.9.2 实验背景 …… (226)
10.9.3 实验内容 …… (226)
10.9.4 思考题 …… (227)
10.10 Windows XP 用户帐户的管理 …… (227)
10.10.1 实验目的 …… (227)
10.10.2 实验步骤 …… (227)
参考文献 …… (228)

第1章　计算机安全基础知识

【教学目标】

掌握计算机安全的含义及帐户基本对象；了解计算机安全策略、安全规则、安全因素、外部威胁；掌握一般防范措施；掌握计算机及网络安全的分类；掌握计算机安全解决方案和网络安全措施；掌握计算机及网络安全的评估方法。

掌握计算机软件安全的概念、安全需求；了解计算机软件安全技术标准、计算机安全级别。

掌握计算机病毒的分类、传播方法、工作方式、特点及破坏行为；掌握宏病毒及网络病毒的特征；了解病毒的预防、检查和清除方法。

【教学重点和难点】

- 计算机安全的含义、对象及机制
- 软件分析技术
- 计算机病毒的防御

随着计算机在社会各个领域的广泛应用和迅速普及，计算机系统及其网络的安全、保密问题越来越受到人们的重视。计算机安全(Computer Security)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　计算机安全概述

1.1.1　计算机系统面临的威胁和攻击

计算机系统面临的威胁和攻击大体上可以分成两大类：一类是对实体的威胁和攻击；另一类是对信息的威胁和攻击。计算机犯罪和病毒则包含了对计算机系统实体和信息两个方面的威胁和攻击。

(1)对计算机系统实体的威胁和攻击，主要是指对计算机及其外部设备和网络的威胁和攻击。

(2)对计算机系统信息的威胁和攻击，主要是指计算机系统的信息被泄露和破坏。信息泄露是指偶然地或故意地获得(侦收、截获、窃取或分析破译)目标系统中的信息，特别是敏感信息，造成泄露事件；信息破坏是指偶然事故或人为破坏，使信息的正确性和可用性受到破坏，造成大量信息被破坏、被修改或丢失。

计算机犯罪是指行为人运用所掌握的计算机专业知识，以计算机为工具或以计算机资产为攻击对象，给社会造成严重危害的行为。其中，计算机资产包括硬件、软件以及计算机系统中存储、处理或传输的数据及通信线路。目前比较普遍的计算机犯罪有：黑客非法侵入、网上制作传播有害信息、利用计算机实施欺骗、越权使用计算机资源等。随着计算机技术的发展，未来还可能会出现更多其他的犯罪形式。

计算机犯罪与传统犯罪相比，具有隐蔽性、跨国性、专业性、自动连续性、诱惑性以及严重的

社会危害性等特点。

计算机系统的不安全环节包括数据输入部分、数据处理部分、通信线路、软件部分、输出部分、存取控制部分等。

造成计算机不安全的原因，包括自然灾害构成的威胁、偶然无意构成的威胁、人为攻击的威胁。

由于计算机系统本身存在存储密度高、数据可访问性、信息聚生性、保密困难性、介质的剩磁效应、电磁泄露性、通信网络脆弱等弱点，这些弱点一旦被利用，系统的资源就会受到很大损失。

1.1.2 计算机系统安全的重要性

(1)对组织机构、目标、任务的影响。大型信息系统在组织机构内已不仅是完成一般的统计等数据处理任务，而是要扩大到对整个计划、预测、决策管理的支持，是系统管理、经营的一环。社会重要部门的主要管理业务的计算机化，使得系统的安全一旦出现问题则意味着许多管理工作无法正常进行。军事指挥部门的信息系统不安全，将危及国家的安全；经济管理部门的信息系统不能正常工作，将打乱某些经济运行工作；企业信息系统故障，将使正常经营受到影响，甚至打乱生产秩序；社会服务信息系统中止服务，将会产生社会问题(如股票、民航等)，并使其失去信誉，影响市场。

(2)对信息资源的影响。大型信息系统的重要特征之一是信息量大，并且这些信息涉及内部重要信息甚至机密。因此，信息本身的泄露、被修改或丢失等都将带来巨大的损失。国家重要军事、经济部门的信息系统中，必定有许多国家机密信息，任何形式的破坏都会给国家带来损害。企业的信息必然涉及经营及商业秘密，在市场竞争环境中，将对企业有关键性的影响。银行储蓄信息的改变往往意味着资金的转移和被窃取。

(3)对单位形象及信誉的影响。在当前市场经济体制的环境下，大型信息服务系统及企业形象与信誉对企业自身的发展关系极大，如果其信息系统不能正常工作，失去人们的信任，那么它将丢掉市场，这对企业来讲是致命的。

综上所述，大型信息系统的地位和作用对组织机构是极为重要的。因此，这类系统更容易成为被攻击的目标。

1.1.3 计算机安全技术的发展和现状

一个事物的发展过程可给我们一些有益启示。纵观 IT 发展的历史，计算机及信息安全的概念与内涵也是随着时间的推移而有所不同的。

“计算机安全”概念最早提出时约在 1969 年。当时美国兰德公司给美国国防部的报告中指出“计算机太脆弱了，有安全问题”——这是首次公开提到计算机安全。在当时和其后的一段时期，“计算机安全”的内涵主要是指实体安全，即物理安全。

到了 20 世纪七八十年代，由于各类计算机管理系统开始发展，各种应用开始增多，“计算机安全”开始逐步演化为“计算机信息系统安全”。这时，“安全”概念已经不仅仅指实体的安全，还包括软件与信息等的安全。

到了 20 世纪 80 年代后期，“网络安全”和“信息安全”才开始逐步被广泛采用。近几年，“安全”概念已经不仅仅指安全防范，而且包含了安全保障的含义，即包括监控、保护、应急处理、恢复等系统性的保障。这种概念和内涵还会随着历史的发展继续发生变化。

1. 我国计算机安全和信息安全存在的问题

我国在计算机安全和信息安全方面还存在不少问题，主要表现为：

(1)我国关于网络安全和信息安全的法律、法规、标准及管理协调仍有缺陷，整体尚不完善；一些基础设施不完善；已确定的法律、法规在实际执行和操作中的相关保证措施还不够系统、不配套，实施有一定的困难。

(2)从技术、市场看，目前一些核心技术及产品是国外的，自主知识产权的技术及产品还难以满足需要。总体上看，我国安全产业整体规模还很小，占整个 IT 产业的比例也较低。

(3)从实际应用方面看，对信息安全的完整认识、投入、管理及人才培养等方面还有待加强。

因此，总体上看，我国的网络安全和信息安全仍处在初级阶段。

2. 正确认识计算机安全

(1)计算机安全问题是持续发展的，一定要动态地看待计算机安全问题。

计算机安全的概念及内涵是不断发展和演变的，尤其是安全具有相对性，随着信息技术及相关技术和应用的发展，信息安全的实质、形式、意义都会变化，这也必定引起人们对信息安全的概念、范畴、重要性、特点以及保障措施等方面认识的变化。因此，从动态的观点，从“量”与“质”关系的观点，从不断变化的观点看待计算机安全问题，尤为重要。

(2)安全不是绝对的，一般单位、企业所需要的是适度的安全。

企业应该采购什么级别的安全设备，投入多少才合适，类似的问题长期以来一直困扰着各个企事业单位的安全管理人员。安全要重视，但一定要看具体情况，综合分析投入是否值得。对于很多企事业单位来说，盲目追求设备的先进不是最佳方案，也许可以用更简单、更适用的方案来替代。因此，实事求是的风险评估机制，对企业来说是非常重要的。

(3)安全要重视综合性和整体性，特别是要重视管理。

多方面的调查表明，企事业单位的安全问题，有 70% 出自内部，外部攻击基本上是少数的。因此，加强企事业单位的内部管理，实现综合和整体的安全管理策略，应该是企业需要长期注意的问题。

1.1.4　计算机安全技术研究的内容和目的

国际标准化组织将“计算机安全”定义为“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因遭到破坏、更改和泄露”。由该定义可知，一切影响计算机安全的因素和保障计算机安全的措施都是计算机安全技术的研究内容，其主要包括以下七个方面：

(1)实体安全。主要是指保证计算机设备和通信线路及设施(建筑物等)的安全。与实体安全相关的技术有计算机系统的环境安全、计算机的故障诊断技术、抗电磁干扰技术、防电磁泄漏技术、实体访问控制技术、媒体的存放与管理技术等以及计算机病毒的预防。

(2)数据安全。是指为保证计算机系统中数据库(或数据文件)免遭破坏、修改、泄露和窃取等威胁和攻击而采用的技术方法，主要包括各种用户识别技术、口令验证技术、存取控制技术和数据加密技术以及建立备份、异地存放、妥善保管等技术和方法。

(3)软件安全。是指为保证计算机系统中的软件(如操作系统、数据库系统或应用程序)免遭破坏、非法拷贝、非法使用而采用的技术和方法，包括各种口令的控制与鉴别、软件加密技术、软件防拷贝技术和防动态跟踪技术等。对自己开发的软件，应建立一套严格的开发及控制技术，保

证软件无隐患，满足某种安全标准。此外，不要随便复制未经检测的软件。

(4)网络安全。是指为保证网络及其节点安全而采用的技术和方法，主要包括报文鉴别技术、数字签名技术、访问控制技术、数据加密技术、密钥管理技术，保证线路安全传输而采用的安全传输介质及网络检测、跟踪与隔离技术、路由控制和流量分析控制技术等。利用这些技术和方法，可以及时发现网络中的不正常状态，并采取相应的措施。

(5)运行安全。包括运行与管理技术、系统的使用与维护技术、随机故障维修技术、软件可靠性与可维护性保证技术、操作系统的故障分析与处理技术、机房环境的检测与维护技术、实测系统及其设备运行状态、记录及统计分析技术等。利用这些技术和方法，可以及时发现运行中的异常情况，及时报警，同时提示用户采取适当措施，或进行随机故障维修和软件故障的测试与维修，或进行安全控制与审计。

(6)防病毒威胁。指利用各种病毒扫描和消除工具及技术，定期地检测、诊断和消除系统中的病毒，并采取一整套预防方法，防止病毒入侵。

(7)防计算机犯罪。计算机犯罪是指利用计算机知识和技术，故意泄露和破坏计算机系统中的机密信息或窃取计算机资源，危害系统实体和信息安全的犯罪行为。防止计算机犯罪，就是通过一定的技术手段和方法，杜绝计算机犯罪的发生，并在计算机犯罪实际发生以后，能及时提供犯罪的有关活动信息，跟踪或侦察犯罪，制裁打击犯罪分子。

研究计算机信息安全技术的目的包括以下五个方面：

(1)可用性(Availability)。网络信息的可用性包括对静态信息的可得到和可操作性及对动态信息内容的可见性。安全系统能够对用户授权，提供某些服务，即经过授权的用户可以得到系统资源，并且享受到系统提供的服务，防止非法抵制或拒绝对系统资源或系统服务的访问和利用，增强系统的效用。

(2)完整性(Integrity)。网络信息的完整性是指信息在存储或传输时不被修改、破坏，不出现信息包的丢失、乱序等，即不能为未授权的第三方修改。信息的完整性是信息安全的基本要求，破坏信息的完整性是影响信息安全的常用手段。当前，运行于互联网上的协议(如 TCP/IP 等)，能够确保信息数据包级别的完整性，即做到了传输过程中不丢失信息包，不重复接收信息包，但却无法制止未经授权的第三方对信息包内部的修改。

保证信息完整性的通常做法是将信息或数据附加上特定的信息块，系统可以用这个信息块检验数据信息的完整性，信息块的内容通常是原信息或数据的函数。只有那些经过授权的用户，才允许对数据或信息进行增加、删除和修改。而未经过授权的用户，只要对数据或信息进行改动就立刻会被发现，同时使系统自动采取保护措施。

(3)保密性(Confidentiality)。网络信息的保密性是指网络信息的内容不会被未授权的第三方所知。保密性要求在数据存储、处理和传输中，私有或秘密的信息不会被泄露给未经授权的个体。在很多组织中，保密性的重要性位于可用性和完整性之后。但对于某些系统或大多数系统中指定的数据(如鉴别数据)而言，保密性是非常重要的。

(4)真实性(Authenticity)。网络信息的真实性是指信息的可信度，主要是指对信息所有者或发送者的身份的确认。它包括可控性(Controllability)和可追踪性(Accountability)。

可控性就是对信息及信息系统实施安全监控。可追踪性要求可以根据某个实体的行为唯一地追溯到该实体。可追踪性常常是一个组织的策略要求，它为行为的不可否认、非法行为的威慑、故障隔离、入侵检测和预防、故障的事后恢复和法律行动等提供直接支持。

(5)保证(Assurance)。保证是对安全措施(技术的和操作的)、系统及其处理的数据提供预

定保护的信心基础。当实现了下列条件时，其他四项安全目的(可用性、完整性、保密性和真实性)在一个具体实现中被充分满足：所要求的安全功能被提供并被正确实现；有足够的措施用以防止无意(由用户或软件造成)的错误；对于故意的渗透或旁路有足够的抵制。

保证是一种基本要素，缺乏保证则其他各种目的就不能被满足。但是，保证又是一个连续统一体，不同的系统所需要的保证总量是不一样的。

另外，美国计算机安全专家提出了一种新的安全框架，包括可用性、完整性、保密性、真实性、实用性(Utility)、占有性(Possession)，即在原来的基础上增加了实用性、占有性，认为这样才能解释各种网络安全问题。网络信息的实用性是指信息加密的密钥不可丢失(不是泄密)，丢失了密钥的信息也就丢失了信息的实用性。网络信息的占有性是指存储信息的节点、磁盘等信息载体不可被盗用，从而保证对信息的占用权。保护信息占有性的方法有使用版权、专利、商业秘密性，提供物理和逻辑的存取限制，维护和检查有关盗窃文件的审计记录、使用标签等。

1.1.5　计算机安全系统的设计原则

计算机安全系统的设计是一个周而复始、螺旋上升的过程。事实上，绝对的安全是不存在的，人们要做的是在保密性、可用性、完整性和成本之间取得最大限度的平衡。有这样一句话："七分管理，三分技术。"可见，安全保证的两大支柱是管理和技术，只有在管理方面明确思路，技术才有用武之地。

下面仅从技术角度给出计算机安全系统的一些设计原则。

(1)木桶原则。"木桶的最大容积取决于最短的一块木板"，安全机制和安全服务设计的首要目的是防止最常用的攻击手段，因此应提高整个系统的"安全最低点"的安全性能。

(2)整体性原则。应提供安全防护、监测和应急恢复，以便在网络发生被攻击、破坏事件的情况下，尽可能地恢复网络信息中心的服务，减少损失。

(3)有效性与实用性原则。这一原则要求在确保安全性的基础上，把安全处理的运算量减小或分摊，减少用户记忆、存储工作和安全服务器的存储量、计算量。

(4)安全性评价原则。实用安全性与用户需求和应用环境紧密相关，因此，应根据不同的应用环境采取相应的安全措施。

(5)动态化原则。这一原则要求整个系统内尽可能引入更多的可变因素，并具有良好的扩展性。由于用户在不断增加，网络规模在不断扩大，网络技术本身的发展变化也很快，而安全措施是防范性的、持续不断的，所以制订的安全措施必须不断适应网络发展和环境变化。

(6)设计为本原则。安全与保密方面的设计应与系统设计相结合，即在系统进行总体设计时要考虑安全系统的设计，二者合二为一。

(7)有的放矢、各取所需原则。在考虑安全问题解决方案时，必须考虑性能与价格的平衡。不同的系统所要求的安全侧重点各不相同，应把有限的经费花在刀刃上。

除以上原则外，以下再给出美国著名信息系统安全顾问沃得提出的 23 条设计原则，以供参考：

(1)成本效率原则。应使系统效率最高而成本最低，军事设施除外。

(2)简易性原则。简单易行的控制比复杂的控制更有效和可靠，且受人欢迎、节约成本。

(3)超越控制原则。(紧急情况下)一旦控制失灵，要采取预定的控制措施和方法步骤。

(4)公开设计与操作原则。保密并不是一种强有力的安全方式，过分依赖可能会导致控制失灵。对控制的公开设计和操作，反而会使信息保护得以增强。

(5)最小特权原则。只限于需要才给予这部分特权,但应限定其他系统特权。

(6)分工独立性原则。控制、设计、执行和操作的不应该是同一人。

(7)设计陷阱原则。在访问控制中设置一种易入的陷阱,以引诱某些人进行非法访问,然后将其抓获。

(8)环境控制原则。对于环境控制这一类的问题,应予以重视。

(9)接受能力原则。如果某种控制手段不能为用户或受这种影响控制的人所接受,控制则无法实现。因此,采用的控制措施应使用户能够接受。

(10)承受能力原则。应该把各种控制设计成可容纳最多的威胁,同时也能容纳那些很少遇到的威胁的系统。

(11)检查能力原则。要求各种控制手段产生充分的证据,以显示已完成的操作是正确无误的。

(12)防御层次原则。要建立多重控制的强有力系统,如信息加密、访问控制和审计跟踪等。

(13)记账能力原则。无论谁进入系统后,对其所作所为一定要负责,且系统要予以详细登记。

(14)分割原则。把受保护的东西分割为几个部分,并逐步加以保护,以增强其安全性。

(15)环状结构原则。采用环状结构的控制方式最保险。

(16)外围控制原则。重视"篱笆"和"围墙"的控制作用。

(17)规范化原则。控制要规范化,使系统成为"可论证的安全系统"。

(18)错误拒绝原则。当控制出错时,必须能完全地关闭系统,以防受攻击。

(19)参数化原则。控制能随着环境的变化予以调节。

(20)敌对环境原则。可以抵御最坏的用户企图,容忍最差的用户能力及其他可怕的用户错误。

(21)个人干预原则。在每个危急关头或作重大决策时,为慎重起见,必须有人为干预。

(22)隐蔽性原则。对职员和受控对象隐蔽控制手段或其操作的详情。

(23)安全印象原则。在公众面前应保持一种安全、平静的形象。

上述原则对于计算机安全系统设计是十分重要的,并且这些原则还会随着计算机安全技术的发展而不断完善。

1.2 网络安全体系结构

1.2.1 网络安全的含义

网络信息既有存储于网络节点上信息资源,即静态信息;又有传播于网络节点间的信息,即动态信息。而这些静态信息和动态信息中有些是开放的,如广告、公共信息等,有些是保密的,如私人间的通信、政府及军事部门、商业机密等。网络安全一般是指网络信息的保密性、完整性、可用性及真实性。

1.2.2 网络安全存在的问题

1. 协议设计

(1)制订协议时常忽视安全问题。一般设计人员制订协议时,通常首先强调功能性,而安全