网络安全技术

张仕斌　谭 三　易 勇　蒋 毅　编著

清华大学出版社

网络安全技术

张仕斌　谭三　易勇　蒋毅　编著

清华大学出版社
北京

内容简介

随着计算机的日益普及，计算机网络的发展，网络安全问题在世界各国已经引起了普遍关注，已成为当今网络技术的一个重要研究课题。网络安全技术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、信息论等多学科的综合性学科。本书利用通俗的语言全面阐述了网络安全原理和实践技术，主要内容包括：网络安全基础知识、密码技术、访问控制与防火墙技术、入侵检测与安全审计技术、黑客与病毒防范技术、操作系统安全技术、数据库系统安全技术、数据安全技术和 Web 安全技术等。

全书内容丰富，深入浅出，构思新颖，突出实用，系统性强。本书既可以作为普通高等院校计算机、通信、网络工程、信息安全等相关专业的本科生和研究生的教学用书，也可作为计算机、通信、信息等领域研究人员和专业技术人员的参考用书。

图书在版编目(CIP)数据

网络安全技术/张仕斌等编著. —北京：清华大学出版社，2004
ISBN 7－302－09156－0

Ⅰ. 网… Ⅱ. 张… Ⅲ. 计算机网络－安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2004)第 077828 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010－62776969
责任编辑：宋　韬
封面设计：付剑飞
印 装 者：北京市清华园胶印厂
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：22　**字数**：505 千字
版　　次：2004 年 8 月第 1 版　2004 年 8 月第 1 次印刷
书　　号：ISBN 7－302－09156－0/TP·6456
印　　数：1～5000
定　　价：33.00 元

前　言

随着 Internet 的迅猛发展和信息社会的到来，网络已经影响到社会的政治、经济、文化、军事和社会生活的各个方面。以网络方式获取信息和交流信息已成为现代信息社会的一个重要特征。同时，随着人们对网络信息系统依赖的日益增强，网络正在逐步改变人们的工作方式和生活方式，成为当今社会发展的一个主题。

在人类进入信息化时代的今天，人们对信息的安全传输、安全存储、安全处理的要求越来越显得十分迫切和重要，它不仅关系到战争的胜负，国家的安危，科技的进步，经济的发展，而且也关系到每个人的切身利益。但是，网络作为一把双刃剑，在加速人类社会信息化的同时，也给信息安全保障带来了极大的挑战。网络犯罪事件已屡见不鲜，且呈逐年上升趋势。因此，随着电子商务、电子现金、数字货币、网络银行等业务的兴起以及各种专用网（如金融网）的建设，伴随着这些业务而产生的互联网和网络信息的安全问题，也已成为人们关注的热点问题。

当前，我国的网络安全正面临着严峻的挑战：一方面随着电子政务工程的启动，电子商务的开展以及国家关键基础设施的网络化，使得现有的网络安全设施建设显得日益滞后；另一方面，黑客攻击、病毒传播以及形形色色的网络攻击事件日益增多和成功率一直居高不下，从侧面反映出广大网民的网络防护意识和网络安全知识的欠缺。而市面上现有的介绍网络安全技术的诸多书籍总是存在这样或那样的不足。正是针对这种现状，本书作者在总结多年的教学经验和从事网络安全研究成果的基础上编写了本书。

主要内容

网络安全技术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。因此，网络安全研究的内容十分广泛，它涉及密码学理论，安全体系结构，安全协议，网络信息分析，网络安全监控，应急处理等，其中密码学理论是网络安全的关键技术。本书利用通俗的语言全面阐述了网络安全原理和实践技术，主要包括：网络安全基础知识、密码技术、访问控制与防火墙技术、入侵检测与安全审计技术、黑客与病毒防范技术、操作系统安全技术、数据库系统安全技术、数据安全技术和 Web 安全技术等诸多知识。

特点

本书具有科学严谨的体系结构，内容丰富，深入浅出，构思新颖，突出实用，系统性强，并利用通俗的语言全面阐述了网络安全原理与实践技术。全书的写作始终遵循这样一个目标：为网络安全领域提供一本既可以作为教学用书，也可以作为专业技术人员参考的书籍。

本书及电子课件使用方法

本书共分9章。在每章的开头都列出了本章所要求掌握的知识点;在每章结尾都对本章的所学内容进行了相应的总结;为了方便读者在学完本章后,检验学习成果和加深对本章内容的理解和掌握,本书在每章的最后都给出了相应的实践检验题(包括理论实践和上机实践)。同时,为了便于多媒体教学,本书配有相应的电子教案(PowerPoint),有教学需求的教师可到网址:http://www.bojia.net下载。

适应对象

网络安全技术是信息安全及其相关专业的主要专业课,本书根据编著者近年来的教学实践及科研经验,在编写本书的过程中充分考虑到网络安全技术这门课程的教学及课程的特点,根据不同对象、不同使用要求,组织了部分高校中多年从事网络及网络安全技术教学的老师,力求编写出适合于信息安全及相关专业本科生、研究生学习与应用的教材,也可作为计算机、通信、信息等领域研究人员和专业技术人员的参考书。

编写分工

全书由张仕斌负责统稿和审校工作。其中,第1章网络安全概述,由吴震编写;第2章密码技术,由张仕斌、刘文清编写;第3章访问控制与防火墙技术,由林勇编写;第4章入侵检测与安全审计技术,由谭三、田永红编写;第5章黑客与病毒防范技术,由张德银、陈敏编写;第6章操作系统安全技术,由叶剑新、彭城编写;第7章数据库系统安全技术,由唐开太、许翔燕编写;第8章数据安全技术,由蒋毅、刘双虎编写;第9章Web安全技术,由易勇、李国友编写。同时,参与本书编排的人员还有王安贵、陈郭宜、程小英、谭小丽、卢丽娟、刘育志、吴淬砺、赵明星、贺洪俊、李小平、史利、张燕秋、周林英、黄茂英、李力、李小琼、李修华、田茂敏、苏萍、巫文斌、邹勤、粟德容、童芳、李中全、蒋敏、刘华菊、袁媛、李建康等,在此一并感谢。

由于编写时间仓促,书中疏漏之处在所难免,欢迎广大读者和同行批评指正。

延伸服务:如果读者愿意参加"网络安全技术"的学习培训,或是在学习过程中发现问题,或有更好的建议,欢迎致函。同时,我们也非常愿意同网络安全技术高手保持经常的联系,E-mail:bojia@bojia.net,网址:http://www.bojia.net,我们将认真负责地对待每位读者的来信。

作　者

2004年6月

目　录

第 1 章　网络安全概述 …… 1
1.1　网络信息安全基础知识 …… 1
1.1.1　网络信息安全的内涵 …… 1
1.1.2　网络信息安全的关键技术 …… 1
1.1.3　网络信息安全分类 …… 2
1.1.4　网络信息安全问题的根源 …… 3
1.1.5　网络信息安全策略 …… 3
1.2　网络信息安全体系结构与模型 …… 5
1.2.1　ISO/OSI 安全体系结构 …… 5
1.2.2　网络信息安全解决方案 …… 9
1.2.3　网络信息安全等级与标准 …… 12
1.3　网络信息安全管理体系(NISMS) …… 14
1.3.1　信息安全管理体系的定义 …… 14
1.3.2　信息安全管理体系的构建 …… 14
1.4　网络信息安全评测认证体系 …… 15
1.4.1　网络信息安全度量标准 …… 15
1.4.2　各国测评认证体系与发展现状 …… 17
1.4.3　我国网络信息安全评测认证体系 …… 18
1.5　网络信息安全与法律 …… 18
1.5.1　网络信息安全立法的现状与思考 …… 19
1.5.2　我国网络信息安全的相关政策法规 …… 20
1.6　本章小结 …… 20
1.7　实践检验 …… 21
理论巩固 …… 21
第 2 章　密码技术 …… 22
2.1　密码技术概述 …… 22
2.1.1　密码技术的起源、发展与应用 …… 22
2.1.2　密码技术基础 …… 24
2.1.3　标准化及其组织机构 …… 28
2.2　对称密码技术 …… 29
2.2.1　对称密码技术概述 …… 29
2.2.2　古典密码技术 …… 30
2.2.3　序列密码技术 …… 34
2.2.4　数据加密标准(DES) …… 35
2.2.5　国际数据加密算法(IDEA) …… 42
2.2.6　高级加密标准(AES) …… 43

2.3 非对称密码技术 …… 45
2.3.1 非对称密码技术概述 …… 45
2.3.2 RSA 算法 …… 46
2.3.3 Diffie－Hellman 密钥交换协议 …… 49
2.3.4 ElGamal 公钥密码技术 …… 49
2.3.5 椭圆曲线密码算法 …… 50
2.4 密钥分配与管理技术 …… 54
2.4.1 密钥分配方案 …… 55
2.4.2 密钥管理技术 …… 60
2.4.3 密钥托管技术 …… 62
2.4.4 公钥基础设施(PKI)技术 …… 65
2.4.5 授权管理基础设施(PMI)技术 …… 70
2.5 数字签名 …… 72
2.5.1 数字签名及其原理 …… 72
2.5.2 数字证书 …… 75
2.5.3 数字签名标准与算法 …… 76
2.6 信息隐藏技术 …… 78
2.6.1 信息隐藏技术原理 …… 78
2.6.2 数据隐写术(Steganography) …… 80
2.6.3 数字水印 …… 81
2.7 本章小结 …… 84
2.8 实践检验 …… 85
理论巩固 …… 85
上机实践 …… 86
第 3 章 访问控制与防火墙技术 …… 87
3.1 访问控制技术 …… 87
3.1.1 访问控制技术概述 …… 87
3.1.2 访问控制策略 …… 87
3.1.3 访问控制的常用实现方法 …… 89
3.1.4 Windows NT/2K 安全访问控制手段 …… 89
3.2 防火墙技术基础 …… 91
3.2.1 防火墙概述 …… 91
3.2.2 防火墙的类型 …… 92
3.3 防火墙安全设计策略 …… 96
3.3.1 防火墙体系结构 …… 96
3.3.2 网络服务访问权限策略 …… 97
3.3.3 防火墙设计策略及要求 …… 98
3.3.4 防火墙与加密机制 …… 99
3.4 防火墙攻击策略 …… 99

3.4.1 扫描防火墙策略 …… 99
3.4.2 通过防火墙认证机制策略 …… 99
3.4.3 利用防火墙漏洞策略 …… 100
3.5 第4代防火墙的主要技术 …… 100
3.5.1 第4代防火墙的主要技术与功能 …… 100
3.5.2 第4代防火墙技术的实现方法 …… 102
3.5.3 第4代防火墙抗攻击能力分析 …… 103
3.6 防火墙发展的新方向 …… 104
3.6.1 透明接入技术 …… 104
3.6.2 分布式防火墙技术 …… 105
3.6.3 以防火墙为核心的网络信息安全体系 …… 110
3.7 防火墙选择原则与常见产品 …… 111
3.7.1 防火墙选择原则 …… 111
3.7.2 常见产品 …… 112
3.8 本章小结 …… 114
3.9 实践检验 …… 115
理论巩固 …… 115
上机实践 …… 115
第4章 入侵检测与安全审计 …… 117
4.1 入侵检测系统概述 …… 117
4.1.1 入侵检测定义 …… 118
4.1.2 入侵检测的发展及未来 …… 118
4.1.3 入侵检测系统的功能及分类 …… 120
4.1.4 入侵响应 …… 123
4.1.5 入侵跟踪技术 …… 124
4.2 入侵检测系统(IDS)的分析方法 …… 127
4.2.1 基于异常的入侵检测方法 …… 128
4.2.2 基于误用的入侵检测方法 …… 132
4.3 入侵检测系统结构 …… 135
4.3.1 公共入侵检测框架(CIDF)模型 …… 135
4.3.2 简单的分布式入侵检测系统 …… 137
4.3.3 基于智能代理技术的分布式入侵检测系统 …… 137
4.3.4 自适应入侵检测系统 …… 140
4.3.5 智能卡式入侵检测系统实现 …… 141
4.3.6 典型入侵检测系统简介 …… 144
4.4 入侵检测工具简介 …… 147
4.4.1 日志审查(Swatch) …… 147
4.4.2 访问控制(TCP Wrapper) …… 149
4.4.3 Watcher 检测工具 …… 151

4.5 现代安全审计技术 …… 153
4.5.1 安全审计现状 …… 153
4.5.2 安全审计标准 CC 中的网络信息安全审计功能定义 …… 155
4.5.3 分布式入侵检测和安全审计系统 S_Audit 简介 …… 156
4.6 本章小结 …… 159
4.7 实践检验 …… 159
理论巩固 …… 159
上机实践 …… 159
第 5 章 黑客与病毒防范技术 …… 161
5.1 黑客及防范技术 …… 161
5.1.1 黑客原理 …… 161
5.1.2 黑客攻击过程 …… 164
5.1.3 黑客防范技术 …… 166
5.1.4 特洛伊木马简介 …… 167
5.2 病毒简介 …… 168
5.2.1 病毒的概念及发展史 …… 168
5.2.2 病毒的特征及分类 …… 171
5.3 病毒检测技术 …… 172
5.3.1 病毒的传播途径 …… 172
5.3.2 病毒检测方法 …… 173
5.4 病毒防范技术 …… 174
5.4.1 单机环境下的病毒防范技术 …… 174
5.4.2 小型局域网的病毒防范技术 …… 175
5.4.3 大型网络的病毒防范技术 …… 176
5.5 病毒防范产品介绍 …… 178
5.5.1 病毒防范产品的分类 …… 178
5.5.2 防杀计算机病毒软件的特点 …… 179
5.5.3 对计算机病毒防治产品的要求 …… 179
5.5.4 常见的计算机病毒防治产品 …… 180
5.6 本章小结 …… 182
5.7 实践检验 …… 183
理论巩固 …… 183
上机实践 …… 183
第 6 章 操作系统安全技术 …… 184
6.1 操作系统安全概述 …… 184
6.1.1 操作系统安全的概念 …… 184
6.1.2 操作系统安全的评估 …… 185
6.1.3 操作系统的安全配置 …… 188
6.2 操作系统的安全设计 …… 189

6.2.1 操作系统的安全模型 …… 189
6.2.2 操作系统安全性的设计方法及原则 …… 190
6.2.3 对操作系统安全性认证 …… 192
6.3 Windows 系统安全防护技术 …… 192
6.3.1 Windows 2000 操作系统安全性能概述 …… 192
6.3.2 Windows 2000 安全配置 …… 195
6.4 Unix/Linux 操作系统安全防护技术 …… 200
6.4.1 Solaris 系统安全管理 …… 200
6.4.2 Linux 安全技术 …… 201
6.5 常见服务的安全防护技术 …… 211
6.5.1 WWW 服务器的安全防护技术 …… 211
6.5.2 Xinetd 超级防护程序配置 …… 213
6.5.3 SSH 程序 …… 216
6.6 本章小结 …… 217
6.7 实践检验 …… 218
理论巩固 …… 218
上机实践 …… 218
第 7 章 数据库系统安全技术 …… 219
7.1 数据库系统安全概述 …… 219
7.1.1 数据库系统安全简介 …… 219
7.1.2 数据库系统的安全策略与安全评估 …… 223
7.1.3 数据库系统安全模型与控制 …… 226
7.2 数据库系统的安全技术 …… 227
7.2.1 口令保护技术 …… 228
7.2.2 数据库加密技术 …… 228
7.2.3 数据库备份与恢复技术 …… 230
7.3 数据库的保密程序及其应用 …… 235
7.3.1 Protect 的保密功能 …… 235
7.3.2 Protect 功能的应用 …… 236
7.4 Oracle 数据库的安全 …… 236
7.4.1 Oracle 的访问控制 …… 237
7.4.2 Oracle 的完整性 …… 239
7.4.3 Oracle 的并发控制 …… 241
7.4.4 Oracle 的审计追踪 …… 243
7.5 本章小结 …… 243
7.6 实践检验 …… 244
理论巩固 …… 244
上机实践 …… 244

第 8 章 数据安全技术 …… 245
8.1 数据安全技术简介 …… 245
8.1.1 数据完整性 …… 245
8.1.2 数据备份 …… 247
8.1.3 数据压缩 …… 249
8.1.4 数据容错技术 …… 251
8.1.5 数据的保密与鉴别 …… 256
8.2 数据通信安全技术 …… 259
8.2.1 互联网模型应用保密和鉴别技术 …… 259
8.2.2 端对端保密和鉴别通信技术 …… 262
8.2.3 应用层上加数据保密和鉴别模块技术 …… 264
8.3 本章小结 …… 265
8.4 实践检验 …… 265
理论巩固 …… 265
上机实践 …… 265
第 9 章 Web 安全技术 …… 266
9.1 因特网安全概述 …… 266
9.1.1 因特网上的安全隐患 …… 266
9.1.2 因特网的脆弱性及根源 …… 267
9.2 Web 与电子商务安全技术 …… 268
9.2.1 Web 与电子商务的安全分析 …… 268
9.2.2 Web 安全防护技术 …… 271
9.2.3 安全套接层协议(SSL) …… 272
9.2.4 电子商务的安全技术 …… 274
9.2.5 主页防修改技术 …… 277
9.3 IP 的安全技术 …… 279
9.3.1 IP 安全概述 …… 279
9.3.2 IP 安全体系结构 …… 280
9.3.3 Windows 2000 的 IPSec 技术 …… 286
9.4 E-mail 安全技术 …… 289
9.4.1 E-mail 安全概述 …… 289
9.4.2 E-mail 的安全隐患 …… 291
9.4.3 PGP 标准 …… 292
9.4.4 S/MIME 标准 …… 295
9.4.5 PGP 软件的使用实例 …… 298
9.5 安全扫描技术 …… 300
9.5.1 安全扫描技术的分类 …… 300
9.5.2 安全扫描系统的设计 …… 302
9.5.3 安全扫描工具与产品 …… 304

9.6 网络安全管理技术 …… 307
9.6.1 网络安全管理的必要性 …… 307
9.6.2 传统的网络管理技术及其发展 …… 308
9.6.3 基于 ESM 理念的安全管理机制 …… 310
9.6.4 网络安全管理体系实现的功能 …… 310
9.6.5 安全管理系统与常见安全技术或产品的关系 …… 312
9.7 网络信息过滤技术 …… 313
9.7.1 信息阻塞 …… 314
9.7.2 信息定级与自我鉴定 …… 315
9.7.3 其他的一些客户端封锁软件 …… 318
9.8 身份认证技术 …… 318
9.8.1 身份认证概述 …… 318
9.8.2 单机状态下的身份认证 …… 319
9.8.3 网络环境下的身份认证 …… 322
9.8.4 Windows NT 安全认证子系统 …… 326
9.9 虚拟专用网络(VPN)技术 …… 327
9.9.1 VPN 概述 …… 327
9.9.2 VPN 的关键安全技术 …… 330
9.9.3 VPN 的实现方法 …… 331
9.9.4 VPN 产品与解决方案 …… 333
9.10 本章小结 …… 334
9.11 实践检验 …… 334
理论巩固 …… 334
上机实践 …… 335
参考文献 …… 337

第 1 章　网络安全概述

知识点

- 网络信息安全基础知识
- 网络信息安全体系结构与模型
- 网络信息安全管理体系
- 网络信息安全评测认识体系
- 网络信息安全与法律

1.1　网络信息安全基础知识

1.1.1　网络信息安全的内涵

在网络出现以前，信息安全指对信息的机密性、完整性和可获性的保护，即面向数据的安全。互联网出现以后，信息安全除了上述概念以外，其内涵又扩展到面向用户的安全，即鉴别、授权、访问控制、抗否认性和可服务性，以及在于内容的个人隐私、知识产权等的保护。这两者的结合就是现代的信息安全体系结构。

网络安全从其本质上讲就是网络上信息的安全，指网络系统的硬件、软件及其系统中的数据的安全。网络信息的传输、存储、处理和使用都要求处于安全的状态。

网络信息安全根据其本质的界定，应具有以下的基本特征。

- 保密性：保密性是指信息不泄漏给非授权的个人、实体和过程，或供其使用的特性。
- 完整性：完整性是指信息未经授权不能被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性。对网络信息安全进行攻击其最终目的就是破坏信息的完整性。
- 可用性：可用性是指合法用户访问并能按要求顺序使用信息的特性，即保证合法用户在需要时可以访问到信息及相关资产。
- 可控性：可控性是指授权机构对信息的内容及传播具有控制能力的特性，可以控制授权范围内的信息流向以及方式。
- 可审查性：在信息交流过程结束后，通信双方不能抵赖曾经做出的行为，也不能否认曾经接收到对方的信息。

1.1.2　网络信息安全的关键技术

网络信息安全的关键技术主要包括主机安全技术、身份认证技术、访问控制技术、加

密技术、防火墙技术、安全审计技术与安全管理技术等各种技术，在以后的章节中，将介绍现在常见几种技术。

1.1.3 网络信息安全分类

网络信息安全根据不同的分类方法有多种不同的分类，表 1－1 就是其中的一种分类。

表 1－1 网络信息安全的分类

技 术	分 类		说 明
信息安全	监察安全	监控查验	发现违规
			确定入侵
			定位损害
			监控威胁
		犯罪起诉	起诉
			量刑
		纠偏建议	
	管理安全	技术管理安全	多级安全用户鉴别术的管理
			多级安全加密术的管理
			密钥管理术的管理
		行政管理安全	人员管理
			系统管理
		应急管理安全	应急的措施组织
			入侵的自卫与反击
	技术安全	实体安全	环境安全(温度、湿度、气压等)
			建筑安全(防雷、防水、防鼠等)
			网络与设备安全
		软件安全	软件的安全开发与安装
			软件的安全复制与升级
			软件加密
			软件安全性能测试
		数据安全	数据加密
			数据存储安全
			数据备份
		运行安全	访问控制
			审计跟踪
			入侵告警与系统恢复等
	立法安全	有关信息安全的政策、法令、法规	
	认知安全	办学	
		奖惩与扬抑	
		信息安全宣传与普及教育	

1.1.4　网络信息安全问题的根源

网络安全事故发生的几个原因如下：

- 现有网络系统和协议还是不健全、不完善、不安全的。
- 思想麻痹，没有清醒地意识到黑客入侵所会导致的严重后果，舍不得投入必要的人力、财力和物力来加强网络的安全性。
- 没有采用正确的安全策略和安全机制。
- 缺乏先进的网络安全技术、工具、手段和产品。
- 缺乏先进的灾难恢复措施和备份意识。

局域网(站点)安全事故发生的几个原因如下：

- 网络系统的流量。
- 网络提供的和使用的服务。
- 网络与 Internet 的连接方式。
- 网络的知名度。
- 网络对安全事故的准备情况。

1.1.5　网络信息安全策略

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。实现网络安全，不但要靠先进的技术，而且也得靠严格的管理、法律约束和安全教育，主要包括以下内容。

- 威严的法律：安全的基石是社会法律、法规和手段，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。
- 先进的技术：先进的技术是信息安全的根本保障，用户对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。
- 严格的管理：各网络使用机构、企业和单位应建立相应的信息安全管理办法，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。

网络安全策略是一个系统的概念，它是网络安全系统的灵魂与核心，任何可靠的网络安全系统都是架构在各种安全技术的集成的基础上的，而网络安全策略的提出，正是为了实现这种技术的集成。可以说网络安全策略是为了保护网络安全而制定的一系列法律、法规和措施的总和。当前制定的网络安全策略主要包含 5 个方面的策略。

1. 物理安全策略

物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件设备和通信链路免受自然灾害、人为破坏和搭线攻击；验证用户的身份和使用权限，防止用户越权操作；确保计算机系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非法进入计算机控制室和各种盗窃、破坏活动的发生。

2. 访问控制策略

访问控制是网络安全防范和包含的主要策略，它的主要任务是保证网络资源不被非

法使用和访问。它也是维护网络系统安全，保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到包含作用，但访问控制可以说是保证网络安全最重要的核心策略之一。它主要由入网访问控制、网络权限控制、目录级安全控制、属性安全控制、网络服务器安全控制、网络检测和锁定控制及网络端口和节点的安全控制组成。

- 入网访问控制：入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许他们在哪台工作站入网。用户的入网访问控制可分为 3 个步骤：用户名的识别与验证；用户口令的识别与验证；用户账号的默认限制检查。3 个关卡中只要任何一关未过，该用户便不能进入该网络。
- 网络的权限控制：网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源。可以指定用户对这些文件、目录、设备能够执行哪些操作。因此可以根据访问权将用户分为：特殊用户（系统管理员）、一般用户和审计用户。
- 目录级安全控制：网络应允许控制用户对目录、文件、设备的访问。用户在目录级制定的权限对所有文件和子目录有效，用户还可进一步制定对目录下的子目录和文件的权限。访问权限一般有 8 种：系统管理员权限、读权限、写权限、创建权限、删除权限、修改权限、文件查找权限、存取控制权限。8 种访问权限的有效组合可以让用户有效地完成任务，同时又能有效地控制用户对服务器资源的访问，从而加强了网络和服务器的安全。
- 属性安全控制：当用文件、目录和网络设备时，网络系统管理员应给文件、目录等指定访问属性。属性安全控制可以将给定的属性与网络服务器的文件、目录和网络设备联系起来。属性设置可以覆盖已经指定的任何受托者指派的有效权限。属性往往可以控制以下几个方面的权限：向某个文件写数据，复制一个文件，删除文件或目录，查看目录和文件，执行文件，共享，系统属性等。网络的属性可以保护重要的目录和文件防止用户对目录和文件的误删除、执行、修改、显示等。
- 网络服务器安全控制：是在服务器控制台上执行一系列操作。用户使用控制台可以装载和卸载模块，可以安装和删除软件等操作。服务器的安全控制包括可以设置口令来锁定服务器控制台，以防止非法用户修改、删除重要信息或破坏数据；可以设定服务器登录时间限定、非法访问者检测和关闭的时间间隔等。
- 网络检测和锁定控制：网络管理员应对网络实施监控，服务器应记录用户对网络资源的访问，对分发的网络访问，服务器应以图形或文字、声音等形式报警，以引起管理员的注意。如果不法之徒试图进入网络，网络服务器应会自动记录企图尝试进入网络的次数，如果非法访问的次数达到设定数值，那么该账号将被自动锁定。
- 网络端口和结点的安全控制：网络中服务器的端口往往使用自动回呼设备、静默调制解调器加以保护，并以加密的形式来识别结点的身份。自动回呼设备用

于防止假冒合法用户，静默调制解调器用以防范黑客的自动拨号程序对计算机进行攻击。网络还常对服务器端和用户端采取控制，用户必须携带证实身份的验证器（如智能卡、磁卡、安全密码发生器）。在对用户的身份进行验证之后，才允许用户进入用户端。然后，用户端和服务器端再进行相互验证。

3. 防火墙控制

它是控制进出两个方向通信的门槛。在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的侵入。

4. 信息加密策略

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。常用的方法有链路加密、端到端加密和节点加密 3 种。链路加密的目的是保护网络结点之间的链路信息安全；端到端加密的目的是对源端用户到目的端用户的数据提供保护；节点加密的目的是对源节点到目的节点之间的传输链路提供保护。用户可根据网络情况酌情选择上述加密方式。

5. 网络安全管理策略

在网络安全中，除了采用上述措施之外，加强网络的安全管理，制定有关规章制度，对于确保网络的安全和可靠的运行，将起到十分有效的作用。网络的安全管理策略包括：确定安全管理的等级和安全管理的范围；制定有关网络使用规程和人员出入机房管理制度；制定网络系统的维护制度和应急措施等。

随着网络技术的发展，计算机网络将日益成为工业、农业和国防等方面的重要信息交换手段，渗透到社会生活的各个领域。因此认清网络的脆弱性和潜在威胁，采取强有力的安全策略，对于保障网络的安全性将变得十分重要。

1.2　网络信息安全体系结构与模型

1.2.1　ISO/OSI 安全体系结构

1982 年，开放系统互联（OSI）参考模型建立之初，就开始进行 OSI 安全体系结构的研究。1989 年 12 月 ISO 颁布了计算机信息系统互联标准的第二部分，即 ISO7498 - 2 标准，并首次确定了开放系统互联（OSI）参考模型的安全体系结构。我国将其称为 GB/T9387 - 2 标准，并予以执行。ISO 安全体系结构包括了 3 部分内容：安全服务、安全机制和安全管理。

1. 安全服务

安全服务是由参与通信的开放系统的某一层所提供的服务，它确保了该系统或数据传输具有足够的安全性。ISO 安全体系结构确定了 5 大类安全服务：认证、访问控制、数据保密性、数据完整性和不可否认（抗抵赖）。下面予以分别介绍。

（1）认证服务

这种安全服务提供某个实体的身份保证。该服务有两种类型：对等实体认证和数据源认证。

- 对等实体认证：这种安全服务由（N）层提供时，（N + 1）层实体可确信其对等实