通信行业职业技能鉴定培训丛书

网络通信安全管理员

通信行业职业技能鉴定指导中心　编

北京邮电大学出版社
www.buptpress.com

通信行业职业技能鉴定培训丛书

网络通信安全管理员

通信行业职业技能鉴定指导中心　编

北京邮电大学出版社
·北京·

内 容 简 介

本书系统全面地介绍了当前网络通信安全管理人员所必须具备的理论基础、业务常识、操作实际应用等技能要求，从安全定义、TCP/IP 协议安全、攻击与防御、安全管理、法律法规等基础理论知识入手，重点在主机安全、网络安全、数据恢复、安全审计与评估等四方面展开，详细地介绍了操作系统安全、数据库维护管理、服务器系统的安全、计算机恶意代码与防护、防火墙技术、入侵检测技术、密码学技术、网络设备安全、数据恢复管理、安全审计与评估等内容。

本书结构清晰，实用性强，通俗易懂，对具体工作具有较高的指导意义，可作为通信与信息服务业的网络与信息安全保障人员的技能培训教材，也可作为工程技术人员和管理人员的技术参考书。

图书在版编目(CIP)数据

网络通信安全管理员/通信行业职业技能鉴定指导中心编．--北京：北京邮电大学出版社，2010.3
(通信行业职业技能鉴定培训丛书)
ISBN 978-7-5635-0655-2

Ⅰ.①网… Ⅱ.①通… Ⅲ.①计算机通信网－安全技术－职业技能鉴定－教材 Ⅳ.①TN915.08

中国版本图书馆 CIP 数据核字(2010)第 038067 号

书　　名：网络通信安全管理员
编　　者：通信行业职业技能鉴定指导中心
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
发 行 部：电话：010－62282185　传真：010－62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京忠信诚胶印厂
开　　本：889 mm×1 194 mm　1/16
印　　张：25.75
字　　数：862 千字
版　　次：2010 年 3 月第 1 版　2010 年 3 月第 1 次印刷

ISBN 978-7-5635-0655-2　　定　价：70.00 元

《网络通信安全管理员》
编委会名单

序

伴随着电信业改革进程的不断深入和信息通信技术的快速发展，我国信息通信网络在业务规模、网络能力、技术层次等方面实现了跨越式发展，已经成为支撑经济社会发展的重要基础设施，日益渗透到政治、经济、军事、文化和社会生活等方方面面；国家网络空间的安全已经成为影响国家经济繁荣、社会进步乃至国家安全的重大威胁。

目前，我国信息安全从业人员的技术水平、职业素质、信息安全保障的基本技能、信息安全事件的处置和应急响应能力，都还不能满足通信与信息服务业的要求。开展网络与信息安全就业资格和岗位资质培训，提升从业人员的网络与信息安全素质和整体水平，是有效提升通信与信息服务业的网络与信息安全保障能力、积极应对当前网络威胁的重要任务之一。

作为通信与信息服务业的网络与信息安全保障能力建设的一个重要部分，工业和信息化部通信行业职业技能鉴定指导中心组织行业专家编写了一本《网络通信安全管理员》教材。该教材将网络通信安全管理人员与从业技术人员为培训对象，系统介绍了网络通信相关的安全理论、应用配置、操作维护等内容，并辅以具体案例、考试指南、题库，理论与实践相得益彰，可作为通信行业职业技能鉴定的基础教材，亦可为网络通信安全管理工作提供技术指导。

提升通信与信息服务业的网络与信息安全保障能力，维持公众对信息社会的“信任”和“信心”，是顺应我国国民经济信息化发展趋势和全球化变革潮流的必然选择。国际电联《全球网络安全议程》（GCA）网络安全国际合作框架报告已经将“推进个人和机构的能力建设，从而强化跨行业以及上述各个领域的知识和专业技术”作为主要战略目标之一。相信随着网络通信安全管理人员培训工作的展开和深入，将为我国通信与信息服务业的网络与信息安全保障和持续发展能力奠定坚实的基础。希望互联网信息网络安全领域的同行们再接再厉，为促进我国互联网的有序、健康与协调发展继续努力。

2009 年 7 月于北京

前　言

随着互联网应用日益普及，信息资源重要性日益凸显，整个社会对互联网的依赖程度日益加大，而互联网信息系统本身的脆弱性及安全隐患，以及针对信息系统的各类病毒和网络黑客攻击行为愈来愈激烈，严重威胁着互联网信息系统的安全。为通信与信息服务业培养和造就一批具备基本网络安全防护知识、拥有发现和处置网络安全事件基本技能，具有与法律执行部门、计算机应急响应组织沟通和协作配合的基本素质的网络与信息安全技术人员，已经成为有效提升通信与信息服务业的网络与信息安全保障能力、积极应对当前网络威胁、维持我国信息化可持续发展的重要任务之一。为了将网络通信安全技术人员的培养纳入标准化、规范化轨道，我中心组织编写了网络通信安全管理员技能鉴定配套教材。

教材紧扣网络通信安全管理员职业标准的要求，采用正文与实验手册相结合的方式，从基础理论、主机安全管理、网络安全管理、数据恢复管理、安全审计与评估五大块着手，依照标准的理论与技能要求细化为信息安全基础、操作系统安全配置、数据库维护管理、服务器系统的安全配置、计算机恶意代码与防护、防火墙技术、入侵检测技术、密码学技术、网络设备安全、数据恢复管理、安全审计与评估等11个章节进行阐述，将中级、高级、技师、高级技师的要求融入每个章节，同时配备详细的考试指南，给考生提供详细的教材阅读指引。

本书主要由国家计算机网络应急技术处理协调中心广东分中心、广东邮电职业技术学院、北京启明星辰信息技术有限公司、绿盟科技联合编写。本书编写得到广东省通信管理局、广东省通信行业职业技能鉴定中心给予的大力支持，特致谢意！

由于编写者水平有限，加之时间仓促，书中错漏在所难免，敬请读者、同行及专家批评指正。

工业和信息化部通信行业职业技能鉴定指导中心

2009年7月

目 录

1 安全基础 …… 1

1.1 安全定义 …… 1

1.1.1 信息化发展与信息安全 …… 1

1.1.2 互联网信息网络安全 …… 2

1.1.3 安全的基本要求 …… 2

1.2 TCP/IP 安全性分析 …… 3

1.2.1 Internet 协议（IP） …… 3

1.2.2 传输控制协议（TCP） …… 3

1.2.3 安全性分析 …… 5

1.3 通用攻击技术简介 …… 5

1.3.1 攻击的分类 …… 5

1.3.2 攻击的一般流程 …… 5

1.3.3 攻击的技术方法 …… 6

1.4 安全防御体系简述 …… 8

1.4.1 动态防御模型 …… 8

1.4.2 安全防御技术简介 …… 8

1.5 信息安全管理简述 …… 9

1.5.1 信息安全管理体系 …… 9

1.5.2 建立信息安全管理体系的原则 …… 10

1.6 安全法律法规 …… 10

2 操作系统安全配置 …… 12

2.1 操作系统安全概述 …… 12

2.1.1 Windows 操作系统 …… 12

2.1.2 UNIX 操作系统 …… 13

2.2 Windows 2003 Server 安全配置 …… 15

2.2.1 基本安装配置事项 …… 15

2.2.2 Windows 2003 Server 注册表安全设置项 …… 18

2.2.3 Windows 2003 Server 空会话 …… 19

2.2.4 Windows 2003 Server 用户管理 …… 19

2.2.5 Windows 2003 Server 访问控制 …… 21

2.2.6 Windows 2003 Server 本地安全策略 23
2.2.7 Windows 2003 Server 组策略 25
2.2.8 Windows 2003 Server 安全模板与安全分析工具 27
2.2.9 Windows 2003 Server 安全审核 30
2.2.10 Windows 2003 Server 系统日志文件 31
2.2.11 Windows 2003 Server 容错 35
2.2.12 Windows 2003 Server 事故恢复 35
2.3 Linux Redhat AS4 安全配置 36
2.3.1 基本安装配置事项 36
2.3.2 Linux Redhat AS4 口令与账户安全 39
2.3.3 文件权限 42
2.3.4 文件完整性与加密 46
2.3.5 文件备份 47
3 数据库系统维护管理 49
3.1 数据库概述 49
3.1.1 数据库体系架构 49
3.1.2 数据库主要类型 50
3.1.3 关系数据库管理系统 51
3.1.4 数据库安全概述 51
3.2 常见数据库安装及管理 52
3.2.1 Oracle 安装及管理 52
3.2.2 SQL Server 安装及管理 60
3.2.3 MySQL 安装及管理 71
3.3 常见数据库攻击手段 76
3.3.1 破解弱口令或默认的用户名及口令 76
3.3.2 利用未用的和不需要的数据库服务和功能中的漏洞 82
3.3.3 针对未打补丁的数据库漏洞 84
3.3.4 SQL 注入 88
3.3.5 窃取备份（未加密）的磁带 93
3.4 数据库安全防护 94
3.4.1 Oracle 安全防护 94
3.4.2 SQL Server 安全防护 98
3.4.3 MySQL 安全防护 99
4 服务器系统安全配置 101
4.1 服务器安全概述 101
4.2 Windows 服务器安全配置 101

4.2.1 DNS Server 配置及管理 …… 101
4.2.2 Web Server 配置及管理 …… 106
4.2.3 FTP Server 配置及管理 …… 111
4.2.4 E-mail Server 配置及管理 …… 114
4.3 Web 的安全性 …… 120
4.3.1 Web 的安全问题 …… 120
4.3.2 确保 Web 服务的安全 …… 122
4.3.3 浏览器的安全性 …… 124
4.4 UNIX 服务器安全配置 …… 126
4.4.1 Telnet 和 SSH 配置及管理 …… 126
4.4.2 DNS Server 配置及管理 …… 130
4.4.3 Web Server 配置及管理 …… 135
4.4.4 FTP Server 配置及管理 …… 139
4.4.5 E-mail Server 配置及管理 …… 142
4.5 安全编程与应用 …… 145
4.5.1 缓冲溢出 …… 145
4.5.2 缓冲溢出实例 …… 145
4.5.3 用户数据合法性检查 …… 147
4.5.4 返回值（Return Values） …… 148
5 计算机恶意代码与防护 …… 149
5.1 计算机恶意代码的主要类型 …… 149
5.2 计算机恶意代码分析 …… 150
5.3 常见恶意代码感染迹象与处理 …… 150
5.4 计算机恶意代码防护 …… 152
5.4.1 防治策略 …… 153
5.4.2 预防技术 …… 153
5.4.3 病毒免疫法 …… 155
5.4.4 基本的防病毒方式 …… 155
5.5 计算机恶意代码攻防应用实例 …… 156
5.5.1 首例破坏硬件文件型病毒—— CIH …… 156
5.5.2 首例病毒与蠕虫结合的“病毒” —— Sircam …… 156
5.5.3 首例蠕虫与黑客相结合的“病毒” —— Code Red II …… 157
5.5.4 VBScript 病毒—— VBS/Redlof 蠕虫 …… 159
5.5.5 冲击波（mblaster）蠕虫 …… 159
5.5.6 振荡波病毒 …… 160
5.6 防病毒系统 …… 161
5.6.1 单机工作站 …… 161

5.6.2 文件服务器 …… 161
5.6.3 邮件服务器 …… 161
5.6.4 防火墙网关 …… 162
5.6.5 企业防病毒体系 …… 162
6 防火墙技术 …… 164
6.1 防火墙简介 …… 164
6.1.1 防火墙的基本概念 …… 164
6.1.2 防火墙的作用 …… 165
6.1.3 防火墙的发展阶段 …… 167
6.1.4 防火墙应用举例 …… 169
6.2 防火墙关键技术 …… 170
6.2.1 数据包过滤技术 …… 170
6.2.2 代理技术 …… 175
6.2.3 状态检测技术 …… 178
6.2.4 地址翻译技术 …… 180
6.2.5 虚拟专用网 …… 181
6.3 防火墙实用指南 …… 183
6.3.1 防火墙应具备的基本功能 …… 183
6.3.2 选购防火墙的参考标准 …… 183
6.4 防火墙技术展望 …… 185
6.4.1 防火墙包过滤技术发展趋势 …… 185
6.4.2 防火墙的体系结构发展趋势 …… 187
6.4.3 防火墙的系统管理发展趋势 …… 188
7 入侵检测技术 …… 190
7.1 入侵检测概述 …… 190
7.1.1 入侵检测的基本概念 …… 190
7.1.2 IDS 系统的分类 …… 191
7.1.3 IDS 发展历程 …… 192
7.2 入侵检测关键技术 …… 194
7.2.1 包俘获 …… 194
7.2.2 主机 IDS 检测技术 …… 195
7.2.3 主机入侵检测系统事件分类 …… 197
7.2.4 异常检测技术 …… 198
7.2.5 误用检测技术 …… 200
7.2.6 其他入侵检测系统技术 …… 205
7.2.7 事件规则 …… 205

7.2.8 检测实例 …… 212
7.3 IDS 应用指南 …… 213
7.3.1 IDS 的部署方式 …… 213
7.3.2 应用部署案例 …… 215
7.3.3 IDS 的性能指标 …… 216
7.3.4 IDS 的功能指标 …… 217
8 密码学技术 …… 220
8.1 密码技术简介 …… 220
8.2 消息完整性 …… 221
8.3 E-mail 标准 …… 222
8.4 攻击模式 …… 224
8.4.1 获取口令 …… 224
8.4.2 放置特洛伊木马程序 …… 224
8.4.3 WWW 的欺骗技术 …… 225
8.4.4 电子邮件攻击 …… 225
8.4.5 通过一个节点来攻击其他节点 …… 225
8.4.6 网络监听 …… 225
8.4.7 寻找系统漏洞 …… 225
8.4.8 利用账号进行攻击 …… 226
8.4.9 偷取特权 …… 226
8.5 PKI 介绍 …… 226
8.5.1 PKI 及其构件 …… 226
8.5.2 数字证书与 CA 系统架构 …… 228
8.5.3 PKI 体系的应用 …… 233
9 网络设备安全 …… 236
9.1 交换技术 …… 236
9.1.1 交换机自身安全配置 …… 238
9.1.2 交换机的安全应用 …… 239
9.2 路由技术 …… 240
9.2.1 路由的组成 …… 241
9.2.2 路由算法 …… 241
9.2.3 路由原理 …… 243
9.2.4 路由协议 …… 244
9.2.5 新一代路由器 …… 245
9.2.6 路由器安全配置 …… 246
9.2.7 路由器自身安全 …… 252

9.3 网络设备安全应用 …… 254
9.3.1 流量分析 …… 254
9.3.2 大型网络流量分析 …… 255
9.3.3 大型网络异常流量分析 …… 256
9.3.4 网络攻击抵御 …… 261
10 数据恢复管理 …… 265
10.1 数据备份技术介绍 …… 265
10.2 操作系统数据的备份与恢复 …… 266
10.2.1 Windows 系统备份与恢复 …… 266
10.2.2 UNIX 系统备份与恢复 …… 268
10.3 数据库备份与恢复 …… 270
10.3.1 Oracle 数据库备份与恢复 …… 270
10.3.2 SQL Server 数据库备份和恢复 …… 277
10.3.3 MySQL 数据库备份与恢复操作 …… 281
10.4 数据恢复安全应用实例 …… 285
10.4.1 Oracle 数据恢复 …… 285
10.4.2 SQL Server 数据恢复 …… 287
10.4.3 MySQL 数据恢复 …… 288
11 安全审计与评估 …… 293
11.1 系统安全审计 …… 293
11.1.1 系统日志介绍 …… 293
11.1.2 Windows 系统日志管理 …… 294
11.1.3 UNIX 系统日志管理 …… 296
11.1.4 通过日志对系统活动进行审计 …… 301
11.2 安全评估 …… 301
11.2.1 漏洞扫描基本概念 …… 301
11.2.2 网络漏洞扫描技术 …… 302
11.2.3 应用实例：Microsoft IIS 4.0/5.0 Unicode 解码错误可远程执行命令漏洞 …… 312
11.2.4 安全漏洞的发现及应对策略 …… 314
11.3 风险评估理论与方法 …… 314
11.3.1 信息安全风险评估概述 …… 314
11.3.2 风险评估的术语与定义 …… 315
11.3.3 信息安全风险评估策略 …… 316
11.3.4 风险评估实施流程 …… 317
11.3.5 风险评估实施流程图 …… 318

附录　操作实验 …… 327
A.1 第 2 章实验 …… 327
A.1.1 实验一：Windows 加固 …… 327
A.1.2 实验二：UNIX 加固 …… 328
A.2 第 3 章实验 …… 330
A.2.1 实验一：MySQL 注入攻击 …… 330
A.2.2 实验二：SQL Server 加固 …… 332
A.3 第 4 章实验 …… 333
A.3.1 实验一：Windows 下 Web、FTP 服务器安全配置 …… 333
A.3.2 实验二：利用 SSL 给 IIS 加把锁 …… 335
A.3.3 实验三：给 Linux 下的 Web 服务器进行安全加固 …… 337
A.4 第 5 章实验 …… 338
A.4.1 实验一：灰鸽子木马实验 …… 338
A.4.2 实验二：radmin 木马控制目标主机实验 …… 342
A.5 第 6 章实验 …… 346
A.5.1 实验一：普通网络环境防火墙配置路由模式 …… 346
A.5.2 实验二：普通网络环境防火墙配置混杂模式 …… 350
A.6 第 7 章实验 …… 354
A.6.1 实验一：通过超级终端登录探测引擎,并进行配置 …… 354
A.6.2 实验二：对控制中心进行基本配置操作 …… 357
A.6.3 实验三：如何生成日志报表 …… 360
A.6.4 实验四：设置每月自动备份日志 …… 361
A.6.5 实验五：sniffer pro 抓包实验 …… 362
A.7 第 8 章实验 …… 365
A.7.1 实验一 交换机 VACL 配置 …… 365
A.7.2 实验二 动态 ACL …… 366
A.7.3 实验三 策略路由 …… 368
A.8 第 9 章实验 …… 369
A.8.1 实验一：PGP 实验 …… 369
A.8.2 实验二：PKI 体系实验手册 …… 375
A.9 第 10 章实验 …… 389
A.9.1 实验一：Windows 系统备份与恢复 …… 389
A.9.2 实验二：MySQL 数据库备份与恢复 …… 391
A.10 第 11 章实验 …… 391
A.10.1 实验一：典型的漏洞扫描产品的基本操作应用 …… 391
参考文献 …… 394

1 安全基础

自互联网诞生以来，安全问题应运而生，并随着网络应用的发展变得越来越重要。社会信息化驱动时代变革与进步的旅程，也使隐私保护、资产保障面临极大挑战。本章主要围绕互联网信息网络安全的相关问题，阐述安全的定义和要求，同时对引发互联网信息网络安全问题的 TCP/IP 协议的脆弱性作了简要描述，对互联网的攻击及防御技术、信息网络安全管理以及目前国内外的相关法律法规作了简要介绍。

1.1 安全定义

安全是信息化过程中提出的课题。在信息化发展的不同阶段，存在着不同视角对安全的理解。密码学家 Bruce Schneier 说："安全是一个过程"，而不单纯是一项产品或技术，这体现了与时俱进的动态性与自适应性。技术能够解决物理和工程的难题，通过系统的评估、严谨的设计、全面的测试可排除错误，使之安全可靠。而安全作为一个过程，应当能将该过程一次又一次地应用于网络或信息等实体对象，并且通过这样的操作提高系统的安全性。

1.1.1 信息化发展与信息安全

全面推进国家信息化是我国本世纪初期国民经济与社会文化发展的重要战略目标，是国家实现现代化的基本途径。伴随信息化建设进程的发展，互联网近年来在我国得到迅速发展：至 2009 年 12 月，我国上网人数达到 3.84 亿人，超过美国居世界第一位。网络的普遍应用已日益渗透到我国政治、经济、文化生活的各个角落。

由于信息技术以网络化方式应用的特殊属性，产生了日益深刻的信息安全问题。这种问题全面涉及、影响并威胁到国家、社会和个人的安全利益。信息安全问题，本质上不是一个单纯的技术问题，还是复杂的社会和政治问题，信息和数据安全的范围要比计算机安全和网络安全更为广泛，它包括了信息系统中从信息的产生直至信息的应用这一全部过程。随着信息化社会的不断发展，信息的商品属性也慢慢显露出来，信息商品的存储和传输的安全也日益受到广泛关注。如果非法用户获取系统的访问控制权，从存储介质或设备上得到机密数据或专利软件，或根据某种目的修改了原始数据，那么网络信息的保密性、完整性、可用性、真实性和可控性将遭到破坏。如果信息在通信传输过程中，受到不同程度的非法窃取，或被虚假的信息和计算机病毒以冒充等手段充斥最终的信息系统，使得系统无法正常运行，造成真正信息的丢失和泄露，会给使用者带来经济或者政治上的巨大损失。

信息安全研究所涉及的领域相当广泛。从信息的层次来看，包括信息的来源、去向，内容的真实无误及保证信息的完整性，信息不会被非法泄露扩散保证信息的保密性，信息的发送和接收者无法否认自己所做过的操作行为而保证信息的不可否认性。从网络层次来看，网络和信息系统随时可用，运行过程中不出现故障，若遇意外打击能够尽量减少损失并尽早恢复正常，保证信息的可靠性。系统的管理者对网络和信息系统有足够的控制和管理能力保证信息的可控性。网络协议、操作系统和应用系统能够互相连接、协调运行，保证信息的互操作性。准确跟踪实体运行达到审计和识别的目的，保证信息可计算性。从设备层次来看，包括质量保证、设备备份、物理安全等。从经营管理层次来看，包括人员可靠性、规章制度完整性等。

由此可见，信息安全研究所涉及的领域相当广泛，信息安全实际上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。而我们在本书中所阐述的互联网信息网络安全主要针对的是互联网信息安全中的网络安全问题。

1.1.2 互联网信息网络安全

互联网信息网络安全的根本目的就是防止通过互联网传输的信息被非法使用。从企业和个体角度来看，涉及个人隐私或商业利益的信息在互联网上传输时，其保密性、完整性和真实性应受到关注，避免其他人或商业对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私，造成用户资料的非授权访问和破坏。从国家层面来看，互联网网络安全问题涉及必将关系到国家的主权和声誉、社会的繁荣和稳定、民族文化的继承和发扬等一系列重要问题。

互联网信息网络安全的具体含义涉及社会生活的方方面面，从使用防火墙、防病毒、信息加密、身份鉴别与授权等技术，到企业的规章制度、网络安全教育和国家的法律政策，直至采用必要的实时监控预警手段、应用风险评估管理体系和制定灵活有效的安全策略应变措施，加强互联网信息网络安全的审计与管理。

互联网信息网络安全较全面地对计算机和计算机之间相连接的传输线路全过程进行管理，特别是对网络的组成方式、拓扑结构和网络应用的重点研究。它包括了各种类型的局域网、通信与计算机相结合的广域网，以及更为广泛的计算机互联网络。因此，保护互联网网络系统中的硬件、软件及其数据不受偶然或者恶意因素而遭致破坏、更改、泄露，系统连续可靠稳定运行，网络服务不中断等，已构成互联网信息网络安全的主要内容。

1.1.3 安全的基本要求

计算机系统要防止资源和数据被独占，防止数据和程序被非法修改、删除及泄露，在一定程度上，封闭性有利于保证信息的安全性。如何在保持网络开放灵活性的同时保证安全性成为研究的热点。目前使用TCP/IP技术构成的网络上的安全措施及其相应的网络安全产品主要有两大类：开放型（如数据加密）及被动防护型（如防火墙）。它们主要是根据以下四个方面的安全需求而设计和应用的。

1．数据的保密性

数据的保密性是数据不泄露给非授权用户、实体或过程，或供其利用的特性。数据加密可用来实现保密性目标，使得加密后的数据能够保证在传输、使用和转换过程中不被第三方非法获取。数据经过加密变换后，将明文转换成密文，只有经过授权的合法用户，使用自己的密钥，通过解密算法才能将密文还原成明文。反之，未经授权的用户因不掌握加密或解密密钥，无法获得原文的信息，限制其对特定数据的访问。数据保密可以说是许多安全措施的基本保证，它分为网络传输保密和数据存储保密。除了使用密码技术外，对于数据的存储保密性也可以使用访问控制机制来实现。网络和系统管理员根据不同的应用需求和等级职责，将数据进行分类，配置不同的访问模式，控制数据的流向。

2．数据的完整性

数据的完整性是数据未经授权不能进行改变的特性，即只有得到允许才能修改数据，并且能够判别出数据是否已被篡改。存储的数据或经网络传输后的数据，必须与其最后一次被修改或传输前的内容与形式一致，目的是保证信息系统上的数据处于一种完整和未受损的状态，数据不会因为存储和传输的过程，而被有意或无意改变、破坏或丢失。系统需要一种方法来确认数据在此过程中没有被改变。这种改变可能来源于自然灾难、人的有意和无意行为、因质量和其他因素导致的设备故障、环境和通信的影响以及不可预知的软件错误等方面。显然保证数据的完整性使用一种方法是不够的，在应用数据加密技术的基础上，可综合运用故障应急方案和多种预防性技术，比如归档、备份、校验、崩溃转储和故障前兆分析等手段来实现这一目标。

3．数据的可用性

数据的可用性是可被授权实体访问并按需求使用的特性，即攻击者不能占用所有的资源而阻碍授权者的工作。由于互联网是开放的网络，需要时就可以得到所需要的数据是网络设计和发展的基本目标，因此数据的可用性要求系统当用户需要时能够存取所需要的数据，或是说应用系统提供的服务，能够免于遭受恶劣影响，甚至被完全破坏而不可使用的情形。如果一个合法用户需要访问系统或网络服务时，系统和网络不能提供正常的服务，那么与文件资料被锁在保险柜里，开关和密码系统混乱而不能取出一样，数据虽然完好无损存于系统中，却无法使用。例如网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对数据可用性的攻击。当然，有些数据信息是付费以后才能被调用的，使用鉴别技术可以实现此功能。

4．数据的可控性

数据的可控性是指可以控制授权范围内的信息流向及行为方式，如对数据的访问、传播及内容具有控制能力。首先，系统需要能够控制谁能够访问系统或网络上的数据，以及如何访问，即是否可以修改数据还是只能读取数据。这首先要通过采用访问控制表等授权方法得以实现；其次，即使拥有合法的授权，系统仍需要对网络上的用户进行验证，以确保他确实是他所声称的那个人，通过握手协议和数据加密进行身份验证；最后，系统还要将用户的所有网络活动记录在案，包括网络中机器的使用时间、敏感操作和违纪操作等，为系统进行事故原因查询、定位、事故发生前的预测、报警以及为事故发生后的实时处理提供详细可靠的依据或支持。审计对用户的正常操作也有记载，可以实现统计、计费等功能，而且往往有些诸如修改数据的“正常”操作恰恰是攻击系统的非法操作，同样需要加以警惕。

1.2 TCP/IP 安全性分析

Internet 创建于 1966 年，称为 ARPAnet。支撑 Internet 的 TCP/IP 协议从一开始就没有充分考虑到安全设计。，目前几乎所有的安全问题均与 TCP/IP 有所关联。分析 TCP/IP 协议的安全性，自然地成为研究计算机网络安全的首要课题。

1.2.1 Internet 协议（IP）

IP 地址是一个 32 位的地址，可以在 TCP/IP 网络中说明一台主机的唯一性。一个 IP 包头的大小为 20 字节。IP 包头中包含一些信息和控制字段，以及 32 位的源 IP 地址和 32 位的目的 IP 地址。这个字段包括一些信息：如 IP 的版本号、长度、服务类型和其他配置。每一个 IP 数据报文都是单独的信息，从一个主机传递到另一个主机。主机把收到的 IP 数据包整理成一个可使用的形式。这种开放式的构造使得 IP 层很容易成为黑客的目标。

1.2.2 传输控制协议（TCP）

TCP 是一个面向连接的协议；对于两台计算机的通信，它们必须通过握手过程和信息交换。一旦这些步骤完成，一个连接就建立了。TCP 因此保证了可靠的传输。一旦一个连接建立并且数据开始传输时，如果有任何部分的信息在此过程中丢失，TCP 将重新传输。TCP 协议用于多数的互联网服务，如 HTTP、FTP、SMTP 等。

1．TCP 包头

TCP 包头的标记区建立和中断一个基本的 TCP 连接。有三个标记来完成这些过程：

- SYN：同步序列号
- FIN：发送端没有更多的数据需要传输的信号
- ACK：识别数据包中的确认信息

2．建立一个 TCP 连接：SYN 和 ACK

建立 TCP 连接，必须要经过三次握手。三次握手由下面几步构成（本例中使用客户机/服务器模式）：

（1）客户端（或请求端）通过激活一个 TCP 包头中的 SYN 标记来执行一个 active open。这个 TCP 包头包括：用于连接的端口号；序列号字段中的初始序列号（ISN）。这个号是随机产生的，在客户端和服务器传输数据流时用于同步。

（2）服务器通过向客户端发送其自己的 SYN 而执行了一个 passive open，包含服务器的 ISN；对于客户端的一个确认（ACK）。

（3）最后，客户端返回一个 ACK 给服务器。现在客户端和服务器可以通过比特流来传输数据，并且连接建立。

图 1.1 显示了整个过程。

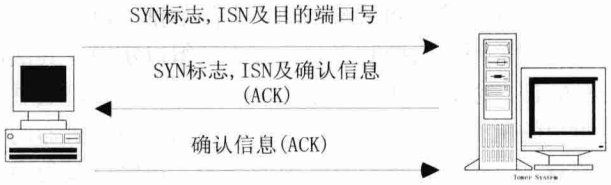

图 1.1　建立一个 TCP 连接的整个过程

3．中断一个 TCP 连接：FIN 和 ACK

因为 TCP 连接是全双向的，中断一个 TCP 连接需要四个步骤。全双向意味着数据独立的在两个方向上流动，因此两个连接都必须被关闭，为了正确的关闭 TCP 连接，任何一个主机都必须发送一个 FIN（就是激活 TCP 包头中的 FIN 标记），当一台主机接受到一个 FIN，它必须终止流动在另一个方向的数据，通过发送一个 FIN 到另一端的应用程序，一个会话结束。大多数的应用程序将关闭两个方向上的数据流，然而，仅仅关闭一个方向并且在半关闭的模式中进行操作是可能的。

结束一个 TCP 连接的四个基本步骤是，

（1）服务器通过激活 FIN 标记执行一个 Active close（客户端经常结束应用程序，但是服务器将开始 TCP 连接的结束），这个行动终止了从服务器到客户机的数据流。

（2）客户端通过发送一个 ACK 到服务器，执行了一个 passive close。

（3）客户端也发送它自己的 FIN 给服务器，以终止从客户端到服务器的数据流。

（4）最后服务器发送一个 ACK 返回给客户端，TCP 连接被终止了，图 1.2 展示了完整的过程。

图 1.2　中断一个 TCP 连接的完整过程

4．端口

TCP 和 UDP 都使用端口的概念。一台运行 TCP/IP 的机器几乎总是同时有不同的应用程序在运行。它们必须都能够同时通信。为了使信息能够被正确的引导，每个程序被赋予了特别的 TCP 或 UDP 端口号。进入计算机的网络数据包都包含了一个端口号并且被操作系统发送到相应的程序。几十年来，主要的端口号已经标准化了，例如，文件传输协议使用 TCP 20 和 21 端口号，DNS 使用 TCP 和 UDP 的 53 端口号，Web 服务器使用 80 端口号，SNMP 使用 UDP 161 和 162 端口号，E-mail 服务器使用 TCP 25 端口号。

TCP 和 UDP 都有 65536 个可用的端口。Internet Assigned Numbers Authority（IANA）规定前 1023 个端口作为 well-know 端口。well-know 端口专门为服务器端的应用程序保留下来，一个服务器应用程序能够使用任何未被限定的端口，及那些大于 1023 的端口，而不需要向 IANA 申请。