中国科学出版集团
新世纪书局

网络安全

21世纪高等院校计算机应用规划教材

刘天华
孙　阳　编著
朱宏峰

- 以学以致用为原则，从工程应用的角度出发，注重知识的实用性，理论与实际相结合
- 详细介绍计算机网络安全理论的基础，充分阐述网络安全的相关技术，选取典型网络安全问题进行方案设计
- 在网络安全技术章节，都有一个针对该章内容的典型项目方案设计，可在实际工程中灵活运用

科学出版社

21 世纪高等院校计算机应用规划教材

网络安全

刘天华　孙　阳　朱宏峰　编著

科学出版社

内 容 简 介

本书以构建计算机网络安全体系为框架，全面介绍了网络安全的基本概念、网络安全体系结构以及网络安全管理的各项内容和任务。全书共13章，内容涵盖了网络安全的概念、网络安全体系结构、网络实体安全、网络安全协议、密码与认证技术、操作系统与数据库安全、应用系统安全、访问控制与VPN技术、防火墙与隔离网闸技术、入侵检测技术、计算机病毒与恶意代码防范技术、网络安全检测与评估技术等。

本书注重知识的实用性，将理论与实际相结合，在全面介绍计算机网络安全理论的基础上，充分阐述了网络安全的相关技术，选取典型网络安全问题进行方案设计，使读者在系统把握网络安全技术的基础上，正确有效地运用网络安全技术解决实际问题。

本书可作为计算机相关专业的本科生教材，或信息管理与信息系统相关专业的参考书，也可作为安全管理人员、网络与信息系统管理人员、IT咨询顾问与IT技术人员的参考手册和培训教材。

图书在版编目（CIP）数据

网络安全/刘天华，孙阳，朱宏峰编著. —北京：科学出版社，2010.4

21世纪高等院校计算机应用规划教材

ISBN 978-7-03-027017-7

Ⅰ.①网… Ⅱ.①刘…②孙…③朱… Ⅲ.①计算机网络－安全技术－高等学校－教材 Ⅳ.①TP393.08

中国版本图书馆CIP数据核字（2010）第044178号

责任编辑：张 鑫 / 责任校对：刘雪连
责任印刷：新世纪书局 / 封面设计：彭琳君

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com

中国科学出版集团新世纪书局策划
北京市艺辉印刷有限公司印刷
中国科学出版集团新世纪书局发行 各地新华书店经销

*

2010年4月 第 一 版 开本：16开
2010年4月第一次印刷 印张：22.25
印数：1—3 000 字数：541 000

定价：36.00元

（如有印装质量问题，我社负责调换）

前　言

计算机网络就像一把双刃剑，它在实现信息交流与共享，极大便利和丰富社会生活的同时，由于网络本身的脆弱性加上人为攻击与破坏，因此而产生的计算机网络安全问题是各国政府有关部门、各大行业以及每个计算机用户都十分关注的重要问题。在高等院校，对计算机专业以及相关专业学生需要开设计算机网络安全技术课程，普及计算机网络安全知识，提高我国的计算机网络安全技术水平，保护我国信息的安全。

为了适应当前计算机网络安全技术发展的需要，解决实际计算机网络中存在的安全问题，更好地培养高素质的计算机网络安全人才，增强技术人员的实践能力，我们编写了这本书。

本书经过作者多年的教学实践与科研经验，内容结构逻辑性强，关注各个环节的安全问题，涵盖了计算机网络安全需要的多方面的基础理论和实践技术。本书以学以致用为原则，从工程应用的角度出发，注重知识的实用性，将理论与实际相结合，在全面介绍计算机网络安全理论的基础上，充分阐述了网络安全的相关技术，选取典型网络安全问题进行方案设计，使读者在系统把握网络安全技术的基础上，正确有效地运用网络安全技术解决实际问题。本书最突出的特点就是应用性强，在网络安全技术相关的章节后面，都有一个针对本章内容的典型项目方案设计，这个方案设计综合了相关技术知识，可在工程应用中进行灵活运用。

本书结构可分为 3 个部分。

第 1 部分：基础篇（第 1~5 章），介绍了网络安全的技术基础。这部分内容对计算机网络安全的范畴进行总体把握，注重基础知识的阐述，主要突出计算机网络的管理和技术两个方面，其中技术侧重于加强安全系统的自我完善，预防安全问题的发生。

第 2 部分：应用篇（第 6~11 章），介绍了网络安全技术。这部分内容对计算机网络安全涉及的技术进行全面介绍，关注工程上应用广泛的网络技术及其可能遇到的安全问题，侧重于提高安全系统的被动防御和主动防御能力，阻止安全问题的发生。

第 3 部分：设计篇（第 12~13 章），介绍了网络安全检测与评估技术以及网络安全系统的设计。这部分内容给出了对具体计算机网络的安全问题进行检测与评估的相关技术，以便对具体计算机网络进行分析，将结果作为反馈信息，进一步完善和提高网络的安全性，达到设计更安全的系统的目的。

本书具有教材和技术资料的双重特征，既可作为计算机相关专业的本科生教材，也可作为信息管理与信息系统相关专业的参考书，亦可供安全管理人员参考使用。

阅读本书之前需要具备操作系统、数据库系统和计算机网络技术的预备知识，主要包括常用的操作系统的配置、关系数据库管理系统的管理、计算机网络应用层协议的实现等。

本书由刘天华、孙阳、朱宏峰编著并完成全书统稿，参加本书讨论与编写的还有蒋宁、陈枭、吴磊、谭振华、王学毅、李舒、杨林蛟、赵楠、陈晓梅等人。

计算机网络学科内容广泛，发展迅速，计算机网络安全相关内容也在不断发展和更新。由于作者水平有限，书中难免存在不足和错误之处，敬请广大读者批评指正。

编　者

2010年4月

目　录

第 1 章　网络安全概述 ……1

1.1　计算机网络安全的概念……1

1.1.1　计算机网络安全的定义……1

1.1.2　计算机网络安全的含义……1

1.1.3　计算机网络安全的主要内容……2

1.2　计算机网络面临的主要威胁……3

1.2.1　网络实体威胁……3

1.2.2　网络系统威胁……3

1.2.3　恶意程序威胁……4

1.2.4　网络的其他威胁……5

1.2.5　影响网络安全的因素……5

1.3　计算机网络安全的 3 个层次……6

1.3.1　安全立法……6

1.3.2　安全管理……8

1.3.3　安全技术措施……8

1.4　计算机网络安全的法律和法规……9

1.4.1　国外的相关法律和法规……9

1.4.2　我国的相关法律和法规……9

1.5　小结……13

1.6　习题……13

第 2 章　网络安全体系结构 ……14

2.1　安 全 模 型……14

2.1.1　P2DR 模型……14

2.1.2　PDRR 模型……16

2.2　网络安全体系结构……16

2.2.1　Internet 网络体系层次结构……16

2.2.2　网络安全体系结构框架……18

2.3　安全策略与运行生命周期……24

2.3.1　安全策略定义……24

2.3.2　安全系统的开发与运行……26

2.3.3　安全系统的生命周期……27

2.4　小结……28

2.5　习题……28

第 3 章　网络实体安全 ……29

3.1　计算机网络机房与环境安全……29

3.1.1　机房的安全等级……30

3.1.2　机房的安全保护……30

3.1.3　机房的三度要求……31

3.1.4　机房的电磁干扰防护……33

3.1.5　机房接地保护与静电保护……35

3.1.6　机房电源系统……36

3.1.7　机房的防火、防水与防盗……37

3.2　计算机网络机房存储介质防护……38

3.3　安全管理……41

3.3.1　安全管理的定义……41

3.3.2　安全管理的原则与规范……41

3.3.3　安全管理的主要内容……42

3.3.4　健全管理机构和规章制度……44

3.4　机房设计依据的规范标准……46

3.5　小结……47

3.6　习题……47

第 4 章　网络安全协议 ……48

4.1　数据链路层安全通信协议……48

4.1.1　PPP 协议……48

4.1.2　PPTP 协议……50

4.1.3　L2TP 协议……51

4.2　网络层安全通信协议……54

4.3　传输层安全通信协议……60

4.3.1　SSL/TLS 协议簇……61

4.3.2　SSL/TLS 应用……67

4.3.3 安全性分析 ……68
4.4 应用层安全通信协议 ……69
4.4.1 电子邮件安全协议 ……69
4.4.2 SET 协议 ……72
4.4.3 SNMP 协议 ……76
4.4.4 S-HTTP 协议 ……80
4.5 小结 ……80
4.6 习题 ……81
4.7 实验 ……81
第 5 章 密码与认证技术 ……82
5.1 密码学概述 ……82
5.1.1 密码学基本概念 ……82
5.1.2 密码体制分类 ……83
5.1.3 信息加密方式 ……85
5.2 加密算法 ……86
5.2.1 DES 算法 ……86
5.2.2 IDEA 算法 ……90
5.2.3 RSA 公开密钥密码算法 ……91
5.2.4 典型散列算法——MD5 算法 ……92
5.3 认证技术 ……94
5.3.1 认证技术基本概念 ……94
5.3.2 认证协议的基本技术 ……95
5.3.3 数字签名技术 ……97
5.3.4 身份认证技术 ……99
5.3.5 消息认证技术 ……101
5.3.6 数字签名与消息认证 ……101
5.4 常用加密软件 ……102
5.5 小结 ……105
5.6 习题 ……106
5.7 实验 ……106
第 6 章 操作系统与数据库安全 ……107
6.1 网络操作系统安全技术 ……107
6.1.1 操作系统安全的概念及准则 ……107
6.1.2 操作系统安全防护的一般方法 ……111
6.1.3 操作系统的安全模型 ……115
6.2 Windows 系统安全技术 ……118
6.2.1 Windows XP 系统安全 ……118
6.2.2 Windows Server 2003 系统安全 ……126
6.3 UNIX/Linux 系统安全技术 ……133
6.3.1 UNIX/Linux 安全基础 ……133
6.3.2 UNIX/Linux 安全机制 ……135
6.3.3 UNIX/Linux 安全措施 ……141
6.4 数据库安全 ……146
6.4.1 数据库安全概述 ……146
6.4.2 数据库安全机制 ……151
6.4.3 数据库安全技术 ……158
6.4.4 攻击数据库的常用方法 ……161
6.5 Oracle 数据库安全技术 ……163
6.5.1 Oracle 数据库安全策略 ……163
6.5.2 Oracle 数据库安全实现方法 ……165
6.6 小结 ……170
6.7 习题 ……170
6.8 实验 ……170
第 7 章 应用系统安全 ……171
7.1 Web 站点安全 ……171
7.1.1 Web 站点安全概述 ……171
7.1.2 Web 站点的安全策略 ……172
7.1.3 Web 站点的一般攻击方法 ……172
7.1.4 Web 站点设计推荐 ……175
7.2 电子邮件系统安全 ……178
7.2.1 电子邮件系统安全概述 ……178
7.2.2 电子邮件系统安全策略 ……179
7.2.3 电子邮件系统的一般攻击方法 ……181
7.2.4 分布式两层电子邮件系统设计方法 ……185

7.2.5 电子邮件系统设计推荐……186
7.3 FTP 系统安全……191
7.3.1 FTP 系统安全概述……191
7.3.2 FTP 系统的安全策略……192
7.3.3 FTP 系统的一般攻击方法……193
7.3.4 FTP 系统设计推荐……194
7.4 DNS 系统安全……197
7.4.1 DNS 系统安全概述……197
7.4.2 DNS 系统的安全策略……198
7.4.3 DNS 系统的一般攻击方法……199
7.4.4 DNS 系统设计推荐……200
7.5 网络欺骗及防范……202
7.5.1 ARP 欺骗及防范……203
7.5.2 IP 欺骗及防范……204
7.5.3 DNS 欺骗及防范……206
7.5.4 Web 欺骗及防范……207
7.6 小结……209
7.7 习题……209
7.8 思考题……209
7.9 实验……209
第 8 章 访问控制与 VPN 技术……210
8.1 访问控制技术概述……210
8.1.1 访问控制技术概念……210
8.1.2 访问控制技术一般方法……211
8.2 自主访问控制……214
8.2.1 自主访问控制概述……214
8.2.2 自主访问控制访问模式……217
8.2.3 自主访问控制实例……219
8.3 强制访问控制……223
8.3.1 强制访问控制概述……223
8.3.2 强制访问控制的模型……224
8.3.3 强制访问控制实例……225
8.4 基于角色的访问控制……226
8.4.1 基于角色的访问控制概述……226
8.4.2 基于角色的访问控制中的角色管理……227
8.4.3 ROLE-BASE 模型实现……228
8.5 VPN 概述……230
8.5.1 VPN 工作原理……230
8.5.2 VPN 系统结构与分类……232
8.6 VPN 实现的关键技术……234
8.6.1 隧道技术……234
8.6.2 加密技术……235
8.6.3 QoS 技术……236
8.7 VPN 设计实例……236
8.7.1 内联网 VPN 设计方案……237
8.7.2 外联网 VPN 构建方案……237
8.7.3 远程接入 VPN 构建方案……238
8.8 小结……239
8.9 习题……239
8.10 思考题……239
8.11 实验……239
第 9 章 防火墙与隔离网闸……240
9.1 防火墙概述……240
9.1.1 防火墙的概念……240
9.1.2 防火墙的特性……240
9.1.3 防火墙的功能……241
9.2 防火墙体系结构……241
9.2.1 双重宿主主机体系结构……242
9.2.2 屏蔽主机体系结构……242
9.2.3 屏蔽子网体系结构……243
9.2.4 防火墙体系结构的组合形式……243
9.3 防火墙技术……243
9.3.1 防火墙所使用的主要技术……243
9.3.2 防火墙的分类……244
9.3.3 防火墙的缺点……247
9.4 防火墙设计实例……248
9.4.1 常见攻击方式和防火墙防御……248

9.4.2 基于 PIX 系列防火墙设计实例 ····· 249
9.4.3 基于个人防火墙配置方法 ····· 251
9.5 隔离网闸概述 ····· 256
9.6 物理隔离网闸 ····· 256
9.6.1 物理隔离网闸定义 ····· 256
9.6.2 物理隔离的技术原理 ····· 256
9.6.3 物理隔离网闸的组成 ····· 258
9.6.4 物理隔离网闸的功能 ····· 258
9.6.5 物理隔离网闸的应用定位 ····· 259
9.6.6 物理隔离网闸与防火墙 ····· 261
9.7 网络隔离产品配置实例 ····· 261
9.7.1 产品介绍 ····· 261
9.7.2 配置模式与配置方法 ····· 262
9.8 小结 ····· 264
9.9 习题 ····· 264
9.10 思考题 ····· 264
9.11 实验 ····· 264

第 10 章 入侵检测技术 ····· 265

10.1 入侵检测概述 ····· 265
10.1.1 入侵检测系统的基本概念 ····· 265
10.1.2 入侵检测系统的结构 ····· 265
10.1.3 入侵检测系统的需求特性 ····· 266
10.1.4 入侵检测系统的分类 ····· 267
10.2 入侵检测的技术实现 ····· 268
10.2.1 入侵检测模型 ····· 268
10.2.2 误用检测与异常检测 ····· 270
10.2.3 分布式入侵检测 ····· 273
10.2.4 其他检测技术 ····· 274
10.3 入侵检测技术的性能指标和评估标准 ····· 275
10.3.1 影响入侵检测系统的性能指标 ····· 275
10.3.2 入侵检测系统测试评估标准 ····· 276
10.4 入侵检测系统实例 ····· 276
10.5 小结 ····· 283
10.6 习题 ····· 283
10.7 思考题 ····· 283
10.8 实验 ····· 283

第 11 章 计算机病毒、恶意代码及防范 ····· 284

11.1 计算机病毒概述 ····· 284
11.1.1 计算机病毒的概念 ····· 284
11.1.2 计算机病毒的特征 ····· 285
11.1.3 计算机病毒的分类 ····· 286
11.1.4 计算机病毒的传播 ····· 287
11.1.5 计算机病毒的防范方法 ····· 287
11.2 计算机网络病毒及防范方法 ····· 289
11.2.1 计算机网络病毒的特点 ····· 289
11.2.2 计算机网络病毒的防范方法 ··· 290
11.3 网络恶意代码及防范方法 ····· 293
11.3.1 网络恶意代码的概念 ····· 293
11.3.2 网络恶意代码的分类 ····· 293
11.3.3 网络恶意代码的关键技术 ····· 296
11.3.4 网络恶意代码的防范方法 ····· 300
11.4 网络病毒与恶意代码实例 ····· 301
11.5 小结 ····· 303
11.6 习题 ····· 303
11.7 思考题 ····· 303
11.8 实验 ····· 303

第 12 章 网络安全检测与评估技术 ····· 304

12.1 网络安全漏洞 ····· 304
12.1.1 网络安全漏洞定义 ····· 305
12.1.2 网络安全漏洞威胁 ····· 306
12.1.3 网络安全漏洞的分类 ····· 307
12.2 网络安全漏洞检测技术 ····· 308
12.2.1 端口扫描技术 ····· 309
12.2.2 操作系统探测技术 ····· 312

12.2.3 安全漏洞探测技术……313
12.3 网络安全评估标准……318
12.3.1 网络安全评估标准概述……319
12.3.2 TCSEC，ITSEC 和 CC 的基本构成……320
12.4 网络安全评估方法……324
12.4.1 CEM 网络安全评估模型……324
12.4.2 基于指标分析的网络安全综合评估模型……325
12.4.3 基于模糊评价的网络安全状况评估模型……326
12.5 网络安全检测评估系统实例……327
12.5.1 Internet Security Scanner……328
12.5.2 Nessus……329
12.6 小结……331
12.7 习题……331
12.8 思考题……331
第 13 章 网络安全方案设计……332
13.1 大型网络安全整体解决方案……332
13.1.1 技术解决方案……332
13.1.2 安全服务解决方案……336
13.1.3 技术支持解决方案……338
13.1.4 实施建议与意见……339
13.2 某高校图书馆的网络安全方案……340
13.2.1 拓扑简要介绍……340
13.2.2 方案设备选型……341
13.3 小结……344
附录 国际及国家网络安全相关标准……345
参考文献……346

第 1 章

网络安全概述

CHAPTER 01

Internet 的广泛应用使人们在生产方式、生活方式及思想观念等方面都发生了巨大变化，推动了人类社会的发展和人类文明的进步，把人类带入了崭新的信息化时代。

计算机网络就像一把双刃剑，它在实现信息交流与共享、为人们带来极大便利和丰富社会生活的同时，由于网络本身的脆弱性加上人为攻击与破坏，也对国家安全、社会公共利益以及公民个人合法权益造成了现实危害和潜在威胁。因此，加强对信息网络安全技术和管理的研究，无论是对个人还是组织、机构，甚至国家、政府都有非同寻常的重要意义。

1.1 计算机网络安全的概念

1.1.1 计算机网络安全的定义

安全是指不发生意外事故，不出现意外情况。从这个角度来说，计算机网络安全是指为了使计算机网络运行正常，通过采用全方位的管理措施和强有力的技术手段，保证在一个网络环境里，使经过计算机网络的数据具有机密性、完整性和可用性。

国际标准化组织（ISO）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、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。”美国国防部国家计算机安全中心将计算机安全定义为：“一般说来，安全的系统会利用一些专门的安全特性来控制对信息的访问，只有经过适当授权的人，或者以这些人的名义进行的进程可以读、写、创建和删除这些信息。”我国公安部计算机管理监察司将计算机安全定义为：“计算机安全是指计算机资产安全，即计算机信息系统资源和信息资源不受自然和人为有害因素的威胁和危害。”

上面是狭义的计算机网络安全的内容。广义上讲，凡是涉及网络上信息的机密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络信息安全所要研究的领域。广义的计算机网络安全还应该包括网络实体安全，如机房的安全保护、防火措施、防水措施、静电防护、电源系统保护等。

1.1.2 计算机网络安全的含义

计算机网络安全是一门综合性学科，涉及计算机科学、网络技术、通信技术、密码与认证技术等多个领域的知识。

（1）网络系统安全

网络系统安全是信息处理和传输系统的安全，包括法律法规的保护，计算机机房环境的保护，计算机结构设计上的安全，硬件系统的可靠、安全运行，操作系统和应用软件的安全，数据库系统的安全等。这方面侧重于保护系统正常的运行，本质是保护系统的合法操作和正常运行。

（2）系统信息安全

系统信息安全包括用户口令鉴别、用户存取权限控制、数据存取权限控制、安全审计、计算机病毒防治、数据加密等。

（3）信息内容安全

信息内容安全包括保护信息的机密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、假冒、诈骗等行为，保护用户的利益和隐私。

（4）信息传播安全

信息传播防止和控制非法、有害信息传播产生的后果，维护道德、法律和国家的利益，包括不良信息的过滤等。

计算机网络安全的本质含义是计算机网络上的信息安全。但其具体含义随着对象的不同而不断变化，在不同的环境会有不同的解释。如果网络的对象是网络用户，计算机网络安全的含义是保证用户所传输信息的机密性、真实性和完整性；如果网络的对象是网络管理者，计算机网络安全的含义是对接入网络的权限加以控制，并规定每个用户的接入权限；如果网络的对象是安全保密部门，计算机网络安全的含义是保证国防等国家机密信息的机密性，保卫国家安全，维护国家利益；如果网络的对象是社会教育相关部门，计算机网络安全的含义是保证网络上的内容健康，对社会的稳定起到积极作用。

1.1.3 计算机网络安全的主要内容

1. 计算机网络安全的内容

计算机网络安全主要包括以下两方面的内容。

（1）网络实体的安全性

网络实体的安全性即网络设备及其设备上运行的网络软件的安全性，使网络设备能够正常提供网络服务。

（2）网络系统的安全性

网络系统的安全性即网络存储的安全性和网络传输的安全性。存储安全是指信息在网络节点上静态存放状态下的安全性。传输安全是指信息在网络中动态传输过程中的安全性。

2. 计算机网络安全的目标

计算机网络安全的基本目标是保护信息的机密性、完整性、可用性、可控性和不可抵赖性。

（1）完整性

完整性是指信息在存储或传输过程中保持不被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性。对于军用信息来说，完整性被破坏可能意味着延误战机、自相残杀或闲置战斗力。对信息安全发动攻击主要是为了破坏信息的完整性。商用信息更注重信息的完整性。

（2）可用性

可用性是指信息可被合法用户访问并按要求顺序使用的特性，即指当需要时可以使用所需

信息。对可用性的攻击就是阻断信息的可用性，例如，破坏网络和有关系统的正常运行就属于对可用性进行攻击。

（3）机密性

机密性是指信息不泄露给未经授权的个人和实体，或被未经授权的个人和实体利用的特性。军用信息安全尤为注重信息的机密性。

（4）可控性

可控性是指信息在整个生命周期内都可由合法拥有者加以安全的控制。

（5）不可抵赖性

不可抵赖性是指用户无法在事后否认曾经对信息进行的生成、签发、接收等行为。

1.2 计算机网络面临的主要威胁

1.2.1 网络实体威胁

网络实体包括网络设备及设备上运行的网络软件，网络实体所受到的威胁主要有以下 4 个方面。

（1）自然因素的威胁。它分为自然灾害（如雷电、地震、水灾、火灾等）、物理损坏（如网络设备损坏、硬盘物理损坏等）和设备故障（如意外断电、电磁干扰等）3 个方面。特点是自然因素性、突发性和非针对性。这种威胁破坏信息的完整性和可用性（无损信息的保密性）。对这种威胁的防范一般是实施防护措施，建立数据备份和安全制度。

（2）电磁泄漏（如监听计算机操作过程）产生信息泄漏、受电磁干扰和痕迹泄露等威胁。特点是难以觉察性、人为实施的故意性、信息的无意泄漏性。这种威胁破坏信息的保密性（无损信息的完整性和可用性）。对这种威胁的防范一般是实施辐射防护、加密和隐藏销毁。

（3）操作失误（如删除文件、格式化硬盘等）和意外事故（如系统崩溃等）的威胁。特点是人为实施的无意性和非针对性。这种威胁破坏信息的完整性和可用性（无损信息的保密性）。对这种威胁的防范一般是采用状态检测、报警确认和应急恢复等方法。

（4）计算机网络机房的环境威胁。特点是损失大、可控性强、可管理性强。这种威胁对信息的完整性、可用性和保密性都可能产生影响。这种威胁的解决方法是加强机房管理、运行管理、安全组织和人员管理。

网路实体安全是信息安全的最根本保障，是不可或缺的组成部分。网络系统中的硬件和软件在设计时考虑到所承受的安全威胁，采取相应的措施。同时，通过安全意识的提高、安全制度的完善、安全操作的保证等方式可使操作人员和管理人员在网络实体安全方面达到要求。

1.2.2 网络系统威胁

网络系统威胁主要有两个方面：网络存储威胁和网络传输威胁。

网络存储威胁是指信息在网络节点上静态存放状态下受到的威胁，主要是网络内部或外部对信息的非法访问。

网络传输威胁是指信息在动态传输过程中受到的威胁，主要有以下几种威胁。

（1）截获（interception）：攻击者从网络上窃听他人的通信内容。

（2）中断（interruption）：攻击者有意中断他人在网络上的通信。

（3）篡改（modification）：攻击者故意篡改网络上传送的报文。

（4）伪造（fabrication）：攻击者伪造信息在网络上传送。

截获信息的攻击称为被动攻击，而中断、篡改和伪造这些更改信息和拒绝用户使用资源的攻击称为主动攻击。被动攻击和主动攻击的情况如图 1.1 所示。

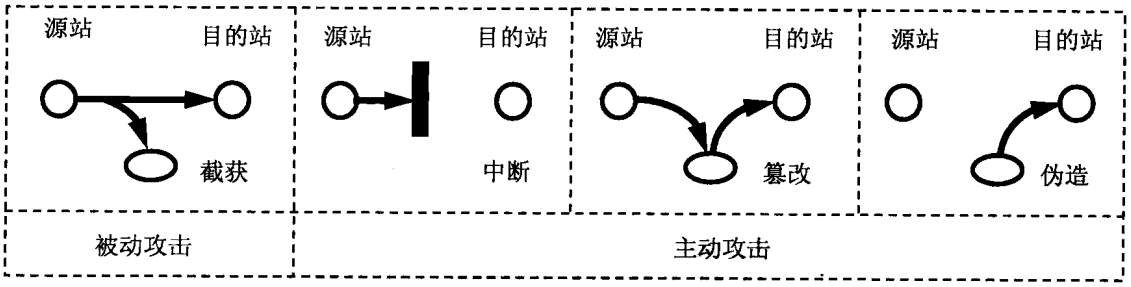

图 1.1 被动攻击与主动攻击

在被动攻击中，攻击者只是观察和分析某一个协议数据单元而不干扰信息流。主动攻击是指攻击者对某个连接中通过的协议数据单元进行各种处理。主动攻击可以进一步划分为 3 种：拒绝服务、更改报文流和伪造连接初始化。

拒绝服务是指攻击者向因特网上的服务器不停地发送大量分组，使因特网或服务器无法提供正常服务。更改报文流包括对通过连接的协议数据单元的真实性、完整性和有序性的攻击。伪造连接初始化是攻击者重放以前已经被记录的合法连接初始化序列，或者伪造身份而企图建立连接。

对付被动攻击可采用各种数据加密技术；而对付主动攻击，则需要将加密技术与适当的鉴别技术相结合。

1.2.3 恶意程序威胁

有一种特殊的主动攻击是恶意程序（rogue program）的攻击。恶意程序对网络安全威胁较大的主要有以下几种。

（1）计算机病毒（computer virus）。病毒是附着于程序或文件中的一段计算机代码，它可以在计算机之间传播，通过修改其他程序来把自身或其变种复制进去。计算机病毒一边传播一边感染计算机，可破坏硬件、软件和文件。例如，从 1999 年的“梅莉莎”病毒、CIH 病毒及 2000 年的“爱虫”病毒到 2001 年的“欢乐时光”病毒，计算机病毒纷纷利用计算机网络作为自己繁殖和传播的载体及工具，呈现出愈演愈烈的势头，且造成的危害也越来越大。

（2）计算机蠕虫（computer worm）。通过网络的通信功能将自身从一个节点发送到另一个节点并启动运行的程序。例如，蠕虫可以向电子邮件地址簿中的所有联系人发送自己的副本，那些联系人的计算机也将执行类似的操作，结果使得整个 Internet 的速度减慢。

（3）特洛伊木马（Trojan horse）。一种程序，它执行的功能超出所声称的功能，该功能被用户在不知情的情况下使用。例如，一个编译程序除了执行编译任务以外，还把用户的源程序偷偷地复制，这种编译程序就是一种特洛伊木马。

（4）逻辑炸弹（logic bomb）。一种当运行环境满足某种特定条件时执行其他特殊功能的程序。例如，一个编译程序平时运行得很好，但当系统时间为 13 日且为星期五时，它会删除系统中的所有文件，这种程序就是一种逻辑炸弹。

1.2.4 网络的其他威胁

网络还面临一些其他的威胁，比如内部破坏、单位内部人员对计算机系统的破坏或泄密，又比如恶意诽谤，不法分子通过网络散布和传播一些对国家、社会、集体和个人有害的信息等。

1.2.5 影响网络安全的因素

影响网络安全的因素有很多，总体来说影响网络安全的因素主要有以下 3 个方面。

1．自然因素

（1）自然灾害的影响。水灾、火灾、地震、雷电等自然灾害往往给系统造成难以恢复的破坏，有的会损害系统设备，有的则会破坏数据，甚至毁掉整个系统和数据。

（2）环境的影响。计算机设备本身能够产生电磁辐射，也怕外界电磁波的辐射和干扰，自身辐射带有信息，容易被别人接收，造成信息泄漏。此外，静电、灰尘、有害气体等也可能给系统带来破坏。

（3）辅助保障系统的影响。辅助保障系统，如水、电、空调工作中断或工作不正常会影响系统运行。

2．技术因素

（1）网络硬件存在安全方面的缺陷。例如，计算机的可靠性差，计算机的许多核心技术不过关，其关键的安全性参数是否有误还需经过检验。

（2）网络软件存在的安全漏洞。任何软件系统，包括系统软件和应用软件，都无法避免安全漏洞的存在。目前流行的许多操作系统、浏览器等均存在网络安全漏洞，还有一些常用软件本身的漏洞等。几乎所有的病毒都是借助于系统或软件的漏洞进行攻击和传播的。

（3）系统配置不当造成的其他安全漏洞。如在网络中路由器配置错误、口令文件缺乏安全的保护、命令的不合理使用等，都会带来或多或少的安全漏洞。黑客大多都是利用这些漏洞攻击网络，比如 IP 地址标识可以被其他用户窥探到，这为假冒身份提供了方便。

3．人为因素

（1）人为无意失误。软件开发过程中可能留下的缺陷或逻辑错误，这些漏洞和逻辑错误就是黑客攻击网络的首选途径，从而导致网络信息的严重破坏。网络管理者在管理网络的过程中，如果安全配置不正确，则可能造成网络的安全漏洞；如果资源的访问控制设定不合理，则可能导致一些资源被破坏。比如用户安全意识不强、口令选择不慎、用户将自己的账号转借他人等都会对网络安全带来威胁。

（2）人为恶意攻击。人为恶意攻击可对计算机网络造成极大的危害，分为非破坏性攻击和破坏性攻击。非破坏性攻击威胁信息的保密性，在不影响网络正常工作的情况下对重要的机密信息进行截获等。破坏性攻击威胁信息的可用性和完整性，对他人相关信息进行中断和篡改，对有利于自己的信息进行伪造等。

对网络进行恶意攻击的人员包括心存不满的员工、软硬件测试人员、网络技术爱好者、好奇的年青人、黑客（hacker）、以政治或经济利益为目的的间谍等。来自内部用户的安全威胁远大于外部网用户的安全威胁。

1.3 计算机网络安全的3个层次

计算机网络安全的实质就是安全立法、安全管理和安全技术措施的综合实施，这3个层次分别对安全策略进行限制、监视和保障。

1.3.1 安全立法

法律是规范人们一般社会行为的准则。法律从形式上分为宪法、法律、法规、法令、条令、条例和实施办法、实施细则等，从内容上分为社会规范和技术规范。

计算机网络时代向传统法律提出了许多前所未有的挑战，健全的安全法律法规体系是确保信息安全的基础，不论是国外还是国内，以法律的形式规定和规范信息安全工作是有效实施安全措施的有力保证。

1. 安全立法的内容

安全立法包括以下3个方面的内容。

（1）公法。公法的内容应包括对网络进行管理的行政法内容，对网络纠纷进行裁决的诉讼法内容，对网络犯罪行为进行追究的刑法、刑事诉讼法的内容。

（2）私法。私法是从民法的角度，对网络主体及其权利义务、网络行为、网络违法行为的民事责任做出规定。

（3）网络利用的法律问题。这部分内容是针对人们利用网络进行网络以外的活动而做出法律规定。

2. 国外安全立法的现状

发达国家较早开展了相关计算机应用的法律问题，制定了一些相关的法律和法规，用来规范计算机在社会和经济活动中的使用。

（1）美国立法现状

美国不仅信息技术具有国际领先水平，而且信息安全法律体系也比较完备。

以信息为主要内容的有《电子信息自由法案》、《个人隐私保护法》、《公共信息准则》、《削减文书法》、《消费者与投资者获取信息法》、《儿童网络隐私保护法》、《电子隐私条例法案》等；以基础设施为主要内容的《1996年电信法》；以计算机安全为主要内容的《计算机保护法》、《网上电子安全法案》、《反电子盗窃法》、《计算机欺诈及滥用法案》、《网上禁赌法案》等；以电子商务为主要内容的《统一电子交易法》、《国际国内电子签名法》、《统一计算机信息交易法》、《网上贸易免税协议》等；以知识产权为主要内容的《千禧年数字版权法》、《反域名抢注消费者保护法》等。

（2）欧盟立法现状

欧盟自成立以来，已制定推出了关于构建新型科技信息社会的一整套政策，如《有关实施对电信管制一揽子计划的第五份报告》、《电子通信服务的新框架》、《电子欧洲——一个面向全体欧洲人的信息社会》等政策性文件；还有《关于聚焦电信、媒体、信息技术内容及相关规范的绿皮书》、《欧洲共同体委员会信息社会的版权和有关权利的绿皮书》等对信息化产生重大影响的规范性文件。此外，欧盟还出台了《促进21世纪的信息产业的长期社会发展规划》

及相应的行动计划。这些政策性文件涉及因特网、电信、通信和信息服务市场、许可证制度、信息保护、税赋及电子商务等各个方面的内容。

（3）俄罗斯立法现状

俄罗斯维护信息安全的政策与措施的基本目标，是为发展以信息为基础的各方面事业创造良好条件，防止外部和内部敌对势力破坏。

1994年俄罗斯通过了信息安全保护法《政府通信和信息联邦机构法》。针对信息、安全保护的法规有：《数字签名法》、《信息化和信息保护法》、《国家秘密法》、《信息保护设备认证法》以及针对加密设备的研制、生产、实现和应用的法规等。统领全局的《国家信息安全构想》于2000年获批，该学说明确了俄罗斯在信息领域的利益，为俄罗斯制定了许多确保国家安全和公民权利的具体措施，是制定和起草其他有关信息安全保障国家政策、法律、提案和专门计划的基础。

（4）日本立法现状

日本从国家整体发展战略的高度构建信息安全体系。在出台有关发展战略构想的同时，日本全面重视信息安全立法工作，制定了一系列相关的法律和法规。

2000年出台了《防止非法接入法》，以建立防止和刑事处罚非法接入或属于这种行为的活动规章。同年的《电子签名：鉴别法》对电子签名的有效性作了详细规定，依据国际通用测评认证标准修订的《电子商务网络安全对策指针》则进一步健全了电子商务的安全管理机制。另外针对信息电子证书的需要，还对《商业登记法》作了修订。为避免关键基础设施遭受电脑恐怖活动攻击，日本政府推出了《关于防范关键基础设施电脑恐怖活动的特别行动计划》。《日本信息安全指导方针》为日本电子政府计划作了全面规划，而《确保电子政务实施过程中的信息安全行动方案》则是为了保证电子政务的安全。

国际上其他很多国家也制定了比较成熟的信息安全法律。

3. 我国安全立法的现状

在我国，1994年2月18日，国务院颁布了《中华人民共和国计算机信息系统安全保护条例》，这是一个标志性、基础性的法规。到目前为止，我国信息安全的法律体系可分为4个层面。

（1）一般性法律规定。这些法律法规并没有专门对信息安全进行规定，但是这些法律法规所规范和约束的对象包括涉及信息安全的行为，如宪法、国家安全法、国家秘密法、治安管理处罚条例等。

（2）规范和惩罚信息网络犯罪的法律。这类法律包括《中华人民共和国刑法》、《全国人大常委会关于维护互联网安全的决定》等。

（3）直接针对信息安全的特别规定。这类法律法规主要有《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网安全保护管理办法》、《中华人民共和国电信条例》等。

（4）具体规范信息安全技术、信息安全管理等方面的规定。这类法律法规主要有《商用密码管理条例》、《计算机病毒防治管理办法》、《计算机信息系统国际联网保密管理规定》、《金融机构计算机信息系统安全保护工作暂行规定》等。

我国虽然制定了信息安全相关的法律法规，但是总体上我国的安全立法还处于起步阶段。目前我国安全立法的主要特点体现在以下几个方面。

（1）信息安全法律法规体系初步形成。