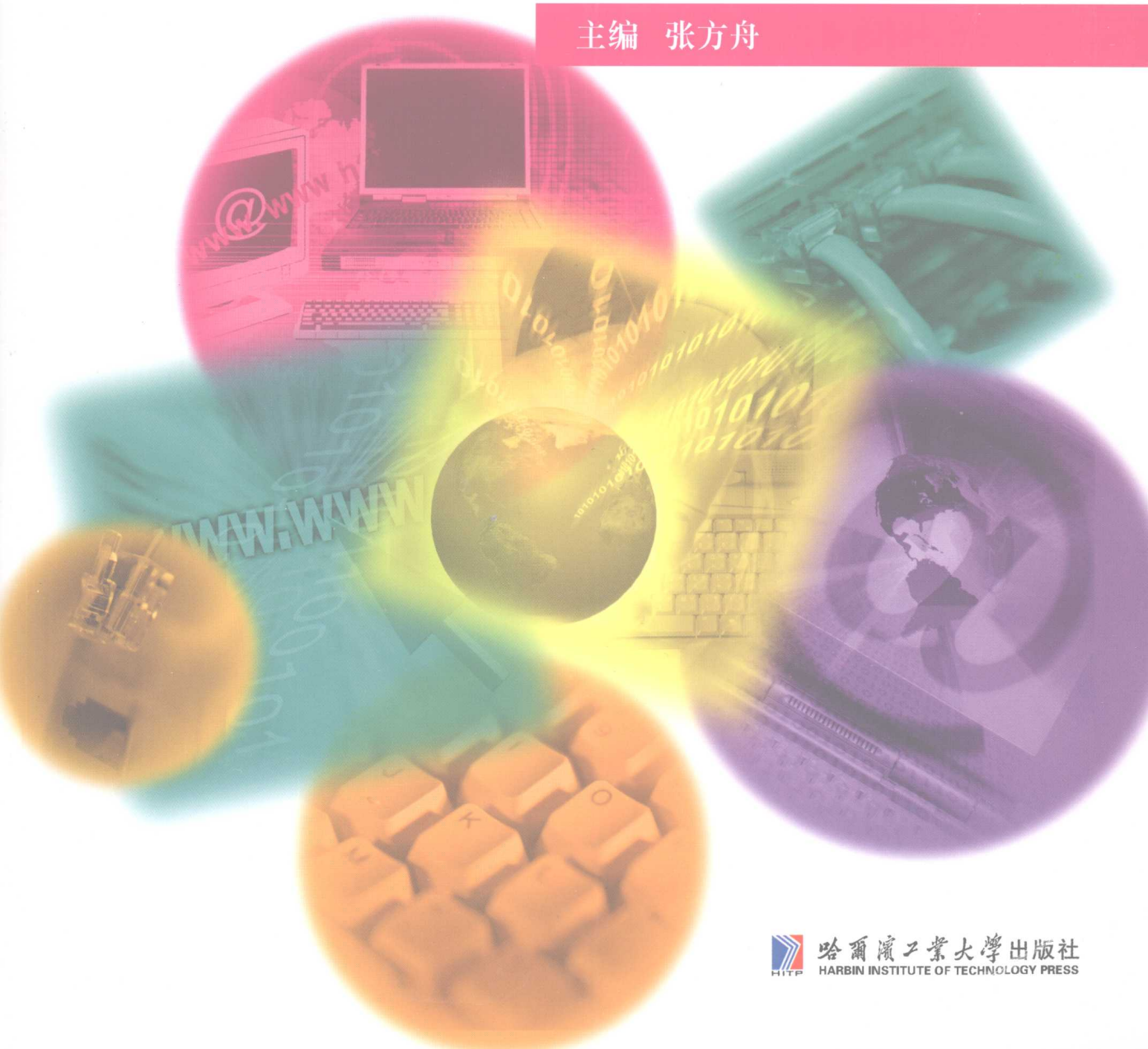
高等学校“十一五”规划教材·计算机系列

计算机网络与信息安全

主编　张方舟



哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

高等学校“十一五”规划教材·计算机系列

计算机网络与信息安全

主　编　张方舟
副主编　陈　伟　宋春玉

哈爾濱工業大學出版社

内 容 简 介

本书围绕计算机网络安全这个中心，对计算机网络安全基础知识和计算机网络安全技术作了比较全面的介绍。本书最大特色是将安全理论、安全工具与安全编程三方面内容有机结合在一起，更有力于读者对理论的掌握和上机实践。本书还配有专门的网站 http://security.dqpi.edu.cn/security，以供读者实践与练习。

全书共分 11 章。第 1～3 章主要介绍网络安全的基本概念、网络协议基础及网络安全编程基础；第 4～6 章详细介绍攻击技术“五部曲”——隐藏 IP，踩点扫描，获得系统或管理员权限，种植后门，在网络中隐身；第 7～9 章介绍各大主流操作系统的安全配置方案，加密与解密技术的应用，防火墙及入侵检测技术；第 10 章介绍从内容安全的角度看计算机网络安全；第 11 章从工程的角度介绍网络安全工程方案的编写。

图书在版编目(CIP)数据

计算机网络与信息安全/张方舟主编.—哈尔滨：哈尔滨工业大学出版社，2008.8

(高等学校“十一五”规划教材·计算机系列)

ISBN 978-7-5603-2772-3

Ⅰ.网… Ⅱ.张… Ⅲ.计算机网络－安全技术－高等学校－教材 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2008)第 128612 号

责任编辑 贾学斌 王桂芝

出版发行 哈尔滨工业大学出版社

社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006

传 真 0451－86414749

网 址 http://hitpress.hit.edu.cn

印 刷 肇东粮食印刷厂

开 本 787mm×1092mm 1/16 印张 12.5 字数 320 千字

版 次 2008 年 9 月第 1 版 2008 年 9 月第 1 次印刷

书 号 ISBN 978-7-5603-2772-3

定 价 25.00 元

高等学校“十一五”规划教材·计算机系列

编 委 会

序

当今社会已进入前所未有的信息时代，以计算机为基础的信息技术对科学的发展、社会的进步，乃至一个国家的现代化建设起着巨大的推进作用。可以说，计算机科学与技术已不以人的意志为转移地对其他学科的发展产生了深刻影响。需要指出的是，学科专业的发展都离不开人才的培养，而高校正是培养既有专业知识、又掌握高层次计算机科学与技术的研究型人才和应用型人才最直接、最重要的阵地。

随着计算机新技术的普及和高等教育质量工程的实施，如何提高教学质量，尤其是培养学生的计算机实际动手操作能力和应用创新能力是一个需要值得深入研究的课题。

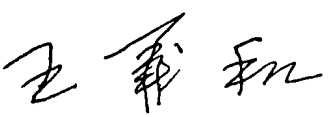
虽然提高教学质量是一个系统工程，需要进行学科建设、专业建设、课程建设、师资队伍建设、教材建设和教学方法研究，但其中教材建设是基础，因为教材是教学的重要依据。在计算机科学与技术的教材建设方面，国内许多高校都做了卓有成效的工作，但由于我国高等教育多模式和多层次的特点，计算机科学与技术日新月异的发展，以及社会需求的多变性，教材建设已不再是一蹴而就的事情，而是一个长期的任务。正是基于这样的认识和考虑，哈尔滨工业大学出版社组织哈尔滨工业大学、东北林业大学、大庆石油学院、哈尔滨师范大学、哈尔滨商业大学等多所高校编写了这套“高等学校计算机类系列教材”。此系列教材依据教育部计算机教学指导委员会对相关课程教学的基本要求，在基本体现系统性和完整性的前提下，以必须和够用为度，避免贪大求全、包罗万象，重在**突出特色**，体现**实用性和可操作性**。

(1)在体现科学性、系统性的同时，突出实用性，以适应当前IT技术的发展，满足IT业的需求。

(2)教材内容简明扼要、通俗易懂，融入大量具有启发性的综合性应用实例，加强了实践部分。

本系列教材的编者大都是长期工作在教学第一线的优秀教师。他们具有丰富的教学经验，了解学生的基础和需要，指导过学生的实验和毕业设计，参加过计算机应用项目的开发，所编教材适应性好、实用性强。

这是一套能够反映我国计算机发展水平，并可与世界计算机发展接轨，且适合我国高等学校计算机教学需要的系列教材。因此，我们相信，这套教材会以适用于提高广大学生的计算机应用水平为特色而获得成功！



2008 年 1 月

前　言

在现代生活中，国家的基础设施、国防基础设施以及与人们息息相关的各行各业的建设与发展，对计算机网络的依赖程度都在不断增大，计算机网络已成为国家发展和人们日常生活中不可或缺的重要组成部分。

但是，随着计算机在人类生活各领域中的广泛应用和科学技术的进步，计算机网络安全问题也日显突出。计算机病毒的不断产生和传播，计算机遭到非法入侵，重要资料被破坏或丢失，由此造成网络系统的瘫痪等，已给各个国家及众多公司造成巨大的经济损失，甚至危及到国家和地区的安全。计算机安全问题已引起世界各国的关注，我国也已予以充分的重视并设法解决。

从技术上讲，网络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、数论、信息论等多种学科的综合性学科。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，不受偶然或恶意原因的破坏、更改、泄露，确保系统连续、可靠、正常地运行，网络服务不中断等。网络安全不仅仅是一个技术问题，也是一个社会问题和法律问题。要解决信息网络的安全问题，必须采取技术和立法等多种手段进行综合治理。

本书围绕计算机网络安全，并结合现行的法律法规，对计算机网络安全基础知识和计算机网络安全技术作了比较全面的介绍，目的在于让读者对其有一个综合全面的认识。

全书共分 11 章。第 1～3 章主要介绍网络安全的基本概念、网络协议基础及网络安全编程基础；第 4～6 章详细介绍攻击技术“五部曲”——隐藏 IP，踩点扫描，获得系统或管理员权限，种植后门，在网络中隐身；第 7～9 章介绍各大主流操作系统的安全配置方案，加密与解密技术的应用，防火墙及入侵检测技术；第 10 章介绍从内容安全的角度看计算机网络安全；第 11 章从工程的角度介绍网络安全工程方案的编写。

本书由大庆石油学院张方舟、袁文翠、赵健民，黑龙江科技学院陈伟、宋春玉编写。其具体分工如下：本书第 1 章、第 5 章、第 9 章由张方舟编写，第 2 章、第 3 章由陈伟编写，第 4 章、第 6 章由袁文翠编写，第 7 章、第 8 章由赵健民编写，第 10 章、第 11 章由宋春玉编写，其中张方舟任主编并统稿，陈伟、宋春玉任副主编。

由于网络安全涉及的知识范围较广，技术较新，编写时难免有疏漏和不当之处，望广大读者和专家批评指正。

编　者

2008.6

目　录

第 1 章 网络安全概述 …… 1

1.1 网络安全的攻防研究 …… 1
1.1.1 安全攻击、安全机制和安全服务 …… 1
1.1.2 网络安全防范体系框架结构 …… 1
1.1.3 网络安全防范体系层次 …… 2
1.1.4 网络安全防范体系设计准则 …… 3
1.2 研究网络安全的必要性和社会意义 …… 4
1.2.1 研究网络安全的必要性 …… 4
1.2.2 研究网络安全的社会意义 …… 5
1.3 网络安全的应急处理体系 …… 6
1.3.1 计算机应急响应与我国互联网应急处理体系 …… 6
1.3.2 应急响应组织和体系的建设 …… 8
1.4 网络安全的管理体系 …… 10
1.4.1 网络面临的安全威胁 …… 10
1.4.2 信息安全管理体系模型 …… 11
1.4.3 信息安全管理体系建设思路 …… 11
1.5 网络安全的法律法规体系 …… 12
1.5.1 我国信息网络安全法律体系 …… 12
1.5.2 我国信息网络安全法律体系的特点 …… 13
1.5.3 我国信息网络安全法律体系的完善 …… 13
1.6 网络安全的标准体系 …… 14
1.6.1 国际组织 …… 14
1.6.2 国内组织 …… 15
1.6.3 标准组研究现状 …… 15
小　结 …… 16
习　题 …… 16

第 2 章 网络安全基础 …… 17

2.1 OSI 概述 …… 17
2.1.1 OSI 概述 …… 17
2.1.2 OSI 参考模型 …… 17
2.2 TCP/IP 协议簇 …… 18

2.2.1 TCP/IP 协议簇 …… 18
2.2.2 IP 协议（Internet Protocol） …… 19
2.2.3 子网掩码 …… 21
2.2.4 TCP 协议 …… 22
2.2.5 UDP 协议 …… 24
2.2.6 ICMP 协议 …… 25
2.3 常用的网络服务 …… 26
2.3.1 常用的网络服务 …… 26
2.3.2 常用服务端口 …… 27
2.4 常用的网络命令 …… 28
2.4.1 系统内置的网络测试工具 ping …… 28
2.4.2 nbtstat 命令 …… 30
2.4.3 netstat 命令 …… 31
2.4.4 tracert 命令 …… 31
2.4.5 rcp 命令 …… 32
2.4.6 net 命令 …… 32
2.4.7 ftp 命令 …… 34
2.4.8 at 命令 …… 34
小 结 …… 35
习 题 …… 35

第 3 章 网络安全编程基础 …… 36

3.1 网络安全编程概述 …… 36
3.1.1 网络编程概述 …… 36
3.1.2 Windows 内部机制 …… 37
3.2 Java 语言编程 …… 38
3.2.1 Java 语言编程 …… 38
3.2.2 Java Socket 编程 …… 39
3.2.3 Java 读写注册表 …… 42
3.2.4 Java 中定时器 timer 类的实现 …… 42
3.2.5 在 Applet 中读取文件内容 …… 43
3.2.6 Java 在 web 应用中获取服务器资源的几种方法 …… 44
3.2.7 在 Java 的应用过程中获取系统属性 …… 44
3.2.8 安全策略文件 …… 46
3.3 网络安全编程规范 …… 46
3.3.1 Java 信息安全的必要性 …… 46
3.3.2 Java 语言本身的安全性 …… 47
3.3.3 Java 语言的编程规范 …… 47
小 结 …… 49
习 题 …… 49

第 4 章 网络扫描与网络监听 …… 50

4.1 黑 客 …… 50
4.1.1 黑客概述 …… 50
4.1.2 黑客简介 …… 50
4.1.3 国内黑客的发展与文化状况 …… 51
4.1.4 黑客常见攻击步骤 …… 51
4.1.5 黑客入侵攻击四种最新趋势 …… 53
4.1.6 黑客攻击五部曲 …… 54
4.2 网络扫描 …… 55
4.2.1 网络安全扫描技术 …… 56
4.2.2 端口扫描技术 …… 56
4.2.3 半连接(SYN)扫描 …… 57
4.2.4 漏洞扫描技术 …… 57
4.3 网络监听 …… 57
4.3.1 网络监听的原理 …… 58
4.3.2 检测网络监听的方法 …… 59
4.3.3 嗅探器(Sniffer)工作原理 …… 60
小 结 …… 61
习 题 …… 61

第 5 章 网络入侵 …… 62

5.1 社会工程学攻击 …… 62
5.1.1 社会工程学攻击 …… 62
5.1.2 社会工程学——信息刺探 …… 63
5.2 物理攻击与防范 …… 63
5.2.1 物理攻击方法 …… 63
5.2.2 防范措施 …… 63
5.3 暴力攻击 …… 63
5.3.1 字典攻击 …… 63
5.3.2 暴力破解邮箱密码 …… 65
5.3.3 字典攻击和暴力破解的防御 …… 65
5.4 Unicode 漏洞专题 …… 66
5.4.1 漏洞危害 …… 66
5.4.2 漏洞成因 …… 66
5.4.3 漏洞检测 …… 66
5.4.4 解决方法 …… 66
5.4.5 Unicode 漏洞入侵 …… 67
5.4.6 DOS 攻击 …… 70
5.5 拥 塞 …… 71

5.5.1 网络拥塞 …… 71
5.5.2 常见的网络拥塞 …… 72
5.5.3 拥塞控制的基本原理 …… 78
5.6 访问权限获取 …… 78
5.6.1 Unicode 漏洞的详细描述 …… 78
5.6.2 获得管理员权限 …… 79
5.7 恶意代码 …… 81
5.7.1 病毒 …… 81
5.7.2 蠕虫 …… 82
5.7.3 移动代码 …… 82
5.7.4 复合型病毒 …… 82
小 结 …… 83
习 题 …… 84

第 6 章 网络后门与网络隐身 …… 85

6.1 隐蔽与欺骗 …… 85
6.1.1 隐蔽真实 IP …… 85
6.1.2 网络欺骗 …… 86
6.1.3 常用的网络欺骗技术 …… 86
6.2 网络后门 …… 87
6.3 木 马 …… 89
6.3.1 特洛伊木马 …… 89
6.3.2 木马攻击原理 …… 90
6.3.3 木马的伪装方式 …… 91
6.3.4 木马的种类 …… 93
6.3.5 安装木马后门的步骤 …… 94
6.4 网络代理跳板 …… 96
6.4.1 网络代理跳板的特点 …… 96
6.4.2 网络代理跳板安装的步骤 …… 96
6.5 清除日志 …… 98
小 结 …… 101
习 题 …… 102

第 7 章 操作系统安全配置方案 …… 103

7.1 主流操作系统简介 …… 103
7.2 操作系统初级安全配置 …… 106
7.3 操作系统中级安全配置 …… 108
7.4 操作系统高级安全配置 …… 110
小 结 …… 112
习 题 …… 112

第 8 章 密码学与 PKI …… 113

8.1 密码学 …… 113
8.1.1 密码学回顾 …… 113
8.1.2 密码学的应用 …… 115
8.2 单钥加密体制 …… 115
8.2.1 DES 简介 …… 115
8.2.2 算法框架 …… 116
8.2.3 DES 解密 …… 116
8.2.4 DES 的几种工作方式 …… 117
8.3 公钥加密体制 …… 117
8.3.1 公钥加密 …… 117
8.3.2 公钥密码算法 …… 117
8.3.3 公钥密码的服务 …… 119
8.4 PGP 加密技术 …… 121
8.4.1 PGP 概述 …… 121
8.4.2 PGP 的主要特征 …… 121
8.4.3 PGP 密钥体系管理 …… 122
8.4.4 PGP 邮件加密的使用 …… 123
8.4.5 预压缩处理 …… 123
8.4.6 PGP 密钥和口令的安全性问题 …… 124
8.5 PKI …… 124
8.5.1 PKI 基本概念 …… 124
8.5.2 PKI 国内外研究现状 …… 124
8.5.3 PKI 研究意义 …… 125
8.5.4 企业级 PKI 结构组成 …… 125
8.6 安全协议及其验证 …… 127
8.6.1 安全协议的基本概念 …… 127
8.6.2 安全协议 …… 128
8.6.3 安全协议的安全性 …… 129
8.6.4 安全协议的分析 …… 130
小 结 …… 131
习 题 …… 131

第 9 章 防火墙与入侵检测 …… 132

9.1 静态侦测——防火墙 …… 132
9.1.1 防火墙的定义 …… 132
9.1.2 防火墙功能 …… 133
9.1.3 防火墙的种类 …… 133
9.1.4 防火墙操作系统 …… 135

9.1.5 Linux 防火墙之 IPtables 概念与用法 …… 135
9.1.6 防火墙的局限性与脆弱性 …… 139
9.1.7 如何防止非法绕过防火墙 …… 140
9.2 动态侦测——入侵检测 …… 142
9.2.1 入侵检测的基本概念 …… 142
9.2.2 开源的 IDS(入侵检测系统)——Snort …… 143
9.2.3 IDS 的体系结构 …… 143
9.2.4 入侵检测系统的主要功能 …… 145
9.2.5 系统模型 …… 145
9.2.6 IDS 分类 …… 145
9.2.7 入侵检测过程分析 …… 146
9.2.8 IDS 部署实例 …… 146
9.2.9 IDS 存在的问题 …… 147
9.2.10 IDS 技术的发展 …… 148
9.2.11 IDS 的发展趋势 …… 148
9.3 隔　离 …… 149
9.3.1 隔离技术的发展历程 …… 149
9.3.2 隔离技术需具备的安全要点 …… 150
9.3.3 网络隔离的关键点 …… 150
9.3.4 隔离技术的未来发展方向 …… 151
9.4 取　证 …… 151
9.4.1 计算机取证 …… 151
9.4.2 电子证据 …… 151
9.4.3 计算机取证的原则和步骤 …… 152
9.4.4 计算机取证工具 …… 154
9.4.5 计算机取证涉及的法律问题 …… 154
9.4.6 计算机取证遇到的困难 …… 155
小　结 …… 155
习　题 …… 155

第 10 章 内容安全 …… 156

10.1 数据捕获 …… 156
10.1.1 捕获数据报的实现原理 …… 156
10.1.2 捕获数据报的编程实现 …… 156
10.2 协议分析 …… 161
10.3 内容检测与过滤 …… 162
10.3.1 基于内容的攻击 …… 162
10.3.2 基于网络的攻击 …… 163
10.3.3 个人电脑内容过滤 …… 163
10.3.4 企业网络内容过滤 …… 164

10.3.5 互联网骨干网络过滤 …… 164
10.3.6 技术难点和技术趋势 …… 165
10.3.7 东方网内容安全成功案例 …… 165
10.4 匿名机制 …… 167
10.4.1 匿名机制的语法 …… 167
10.4.2 匿名机制的安全考虑 …… 167
10.5 数据隐藏 …… 168
10.5.1 信息隐藏的基本概念 …… 168
10.5.2 信息隐藏的特点 …… 169
10.5.3 信息隐藏技术的方法 …… 169
小 结 …… 170
习 题 …… 170

第 11 章 网络安全方案设计 …… 171

11.1 网络安全方案概念 …… 171
11.1.1 网络安全 …… 171
11.1.2 计算机安全 …… 172
11.2 网络安全方案的框架 …… 173
11.3 网络安全案例需求 …… 175
11.4 解决方案设计 …… 177
11.4.1 公司背景简介 …… 177
11.4.2 安全风险分析 …… 177
11.4.3 解决方案 …… 178
11.4.4 实施方案 …… 178
11.4.5 技术支持和服务承诺 …… 179
11.4.6 产品报价 …… 179
11.4.7 产品介绍 …… 179
11.4.8 第三方检测报告 …… 179
11.4.9 安全技术培训 …… 180
小 结 …… 181
习 题 …… 181
参考文献 …… 182

第1章 网络安全概述

随着信息化进程的深入和互联网的快速发展，网络化已成为信息化发展的大趋势，信息资源也得到最大程度的共享。但是，紧随信息化发展而来的网络安全问题也日渐突出，网络安全问题已成为信息时代人类共同面临的挑战。如果网络信息安全问题得不到很好的解决，必将阻碍信息化发展的进程。

本章学习目标

- 了解网络安全研究的体系
- 了解研究网络安全的必要性及社会意义
- 了解计算机网络安全的相关法规
- 掌握网络安全的应急处理体系

1.1 网络安全的攻防研究

1.1.1 安全攻击、安全机制和安全服务

ITU－T X.800 标准对“网络安全(Network Security)”进行了逻辑上的定义。

(1)安全攻击 (Security Attack)：指损害机构所拥有信息的安全的任何行为。

(2)安全机制 (Security Mechanism)指：指设计用于检测、预防安全攻击或者恢复系统的机制。

(3)安全服务 (Security Service)：指采用一种或多种安全机制以抵御安全攻击、提高机构的数据处理系统安全和信息传输安全的服务。

1.1.2 网络安全防范体系框架结构

为了有效了解用户的安全需求，选择各种安全产品和策略，有必要建立一些系统的方法进行网络安全防范。网络安全防范体系的科学性、可行性是其顺利实施的保障。图 1.1 给出了基于 DISSP 扩展的一个三维安全防范技术体系框架结构：第一维是安全服务，给出了 8 种安全属性(ITU－T REC－X.800－199103－I)；第二维是系统单元，给出了信息网络系统的组成；第三维是结构层次，给出并扩展了国际标准化组织 ISO 的开放系统互联(OSI)模型。

框架结构中的每一个系统单元都对应于某一个协议层次，需要采取多种安全服务才能保证该系统单元的安全。网络平台需要有网络节点之间的认证、访问控制，应用平台需要有针对用户的认证、访问控制，需要保证数据传输的完整性、保密性，需要有抗抵赖性和审计的功能，需要保证应用系统的可用性和可靠性。针对一个信息网络系统，如果在各个系统单元都有相

应的安全措施来满足其安全需求，就认为该信息网络是安全的。

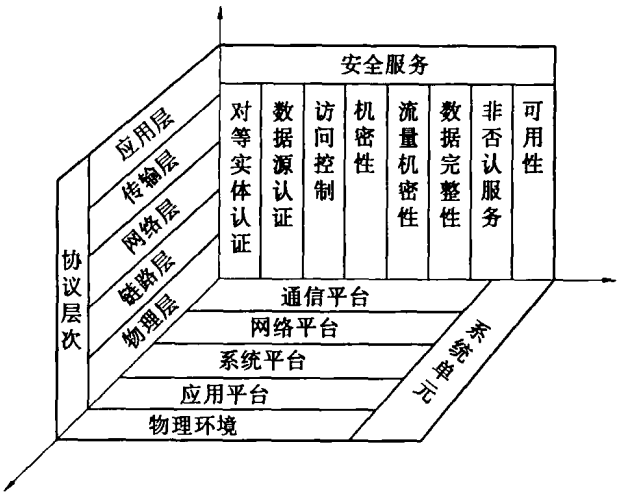


图 1.1 三维安全防范技术体系框架结构

1.1.3 网络安全防范体系层次

作为全方位的、整体的网络安全防范体系也是分层次的，不同层次反映了不同的安全问题，根据网络的应用现状和网络的结构，将安全防范体系的层次划分为物理层安全、系统层安全、网络层安全、应用层安全和安全管理(图 1.2)。

1.物理环境的安全性(物理层安全)

该层次的安全包括通信线路的安全、物理设备的安全、机房的安全等。物理层的安全主要体现在通信线路的可靠性(线路备份、网管软件、传输介质)，软硬件设备安全性(替换设备、拆卸设备、增加设备)，设备的防灾害能力、防干扰能力，设备的运行环境(温度、湿度、烟尘)，不间断电源保障等。

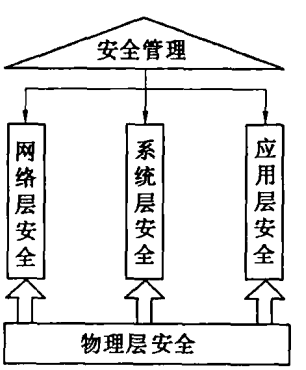


图 1.2 网络安全防范体系层次

2.操作系统的安全性(系统层安全)

该层次的安全问题来自网络内使用的操作系统的安全，如 Windows NT、Windows 2000 等，主要表现在下列 3 个方面。

(1)操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制、系统漏洞等。

(2)对操作系统的安全配置问题。

(3)病毒对操作系统的威胁。

3.网络的安全性(网络层安全)

该层次的安全问题主要体现在网络方面的安全性，包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段和网络设施防病毒等。

4.应用的安全性(应用层安全)

该层次的安全问题主要由提供服务所采用的应用软件和数据的安全性产生，包括 Web 服务、电子邮件系统、DNS 等，此外，还包括病毒对系统的威胁。

5.管理的安全性(管理层安全)

安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化极大程度地影响着整个网络的安全,严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上降低其他层次的安全漏洞。

1.1.4 网络安全防范体系设计准则

根据防范安全攻击的安全需求需要达到的安全目标、对应安全机制所需的安全服务等因素,参照 SSE - CMM(系统安全工程能力成熟模型)和 ISO17799(信息安全管理标准)等国际标准,综合考虑可实施性、可管理性、可扩展性、综合完备性、系统均衡性等方面,网络安全防范体系在整体设计过程中应遵循以下 9 项原则。

1.网络信息安全的木桶原则

网络信息安全的木桶原则是指对信息均衡、全面地进行保护。“木桶的最大容积取决于最短的一块木板”。网络信息系统是一个复杂的计算机系统,它本身在物理上、操作上和管理上的种种漏洞构成了系统的安全脆弱性,尤其是多用户网络系统自身的复杂性、资源共享性使单纯的技术保护防不胜防。攻击者使用的“最易渗透原则”,必然在系统中最薄弱的地方进行攻击。因此,充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测(包括模拟攻击)是设计信息安全系统的必要前提条件。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,其根本目的是提高整个系统的“安全最低点”的安全性能。

2.网络信息安全的整体性原则

网络信息安全的整体性原则要求在网络发生被攻击、破坏事件的情况下,必须尽可能地快速恢复网络信息中心的服务,减少损失。因此,信息安全系统应该包括安全防护机制、安全检测机制和安全恢复机制。安全防护机制是根据具体系统存在的各种安全威胁采取的相应的防护措施,避免非法攻击的进行。安全检测机制检测系统的运行情况,及时发现和制止对系统进行的各种攻击。安全恢复机制是在安全防护机制失效的情况下,进行应急处理和尽量、及时地恢复信息,减少攻击的破坏程度。

3.安全性评价与平衡原则

对任何网络,绝对安全难以达到,也不一定是必要的,所以需要建立合理的实用安全性、用户需求评价和平衡体系。安全体系设计要正确处理需求、风险与代价的关系,做到安全性与可用性相容,做到组织上可执行。评价信息是否安全,没有绝对的评判标准和衡量指标,只能决定于系统的用户需求和具体的应用环境,具体取决于系统的规模和范围、系统的性质和信息的重要程度。

4.标准化与一致性原则

安全体系是一个庞大的系统工程,其设计必须遵循一系列的标准,这样才能确保各个分系统的一致性,使整个系统安全地互联互通、信息共享。

5.技术与管理相结合原则

安全体系是一个复杂的系统工程,涉及人、技术、操作等要素,单靠技术或单靠管理都不可能实现。因此,必须将各种安全技术与运行管理机制、人员思想教育与技术培训、安全规章制度建设相结合。