

计算机

网络安全与防护

Network Security and Protection

张靖 编著

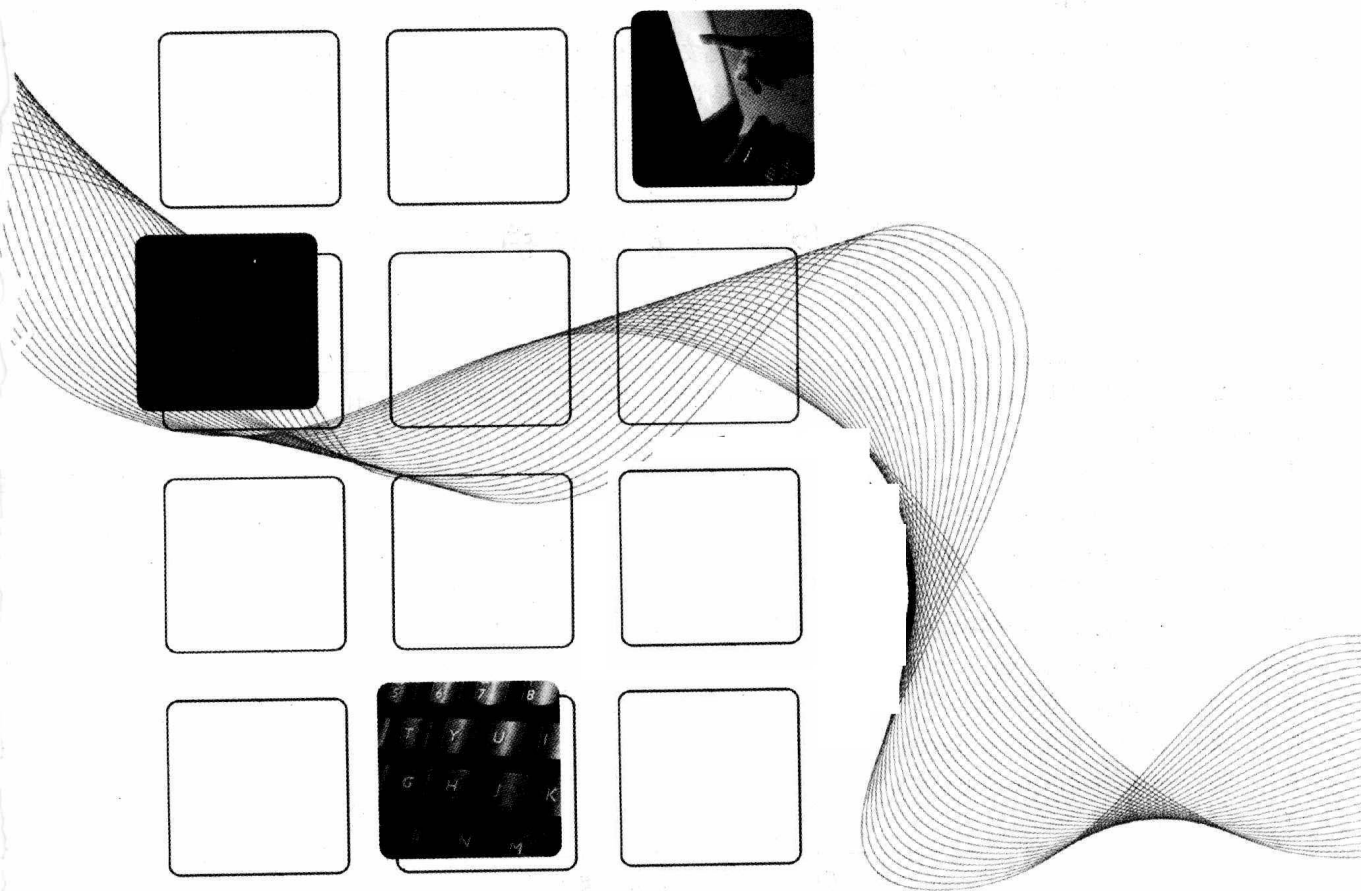


电子科技大学出版社

计算机 网络安全与防护

Computer Network Security and Protection

张靖 编著



电子科技大学出版社

图书在版编目 (CIP) 数据

计算机网络安全与防护 / 张靖编著. -- 成都:

电子科技大学出版社, 2010. 8

ISBN 978-7-5647-0591-6

I. ①计… II. ①张… III. ①计算机网络—安全技术
IV. ①TP393.08

中国版本图书馆 CIP 数据核字 (2010) 第 159255 号

内 容 提 要

本书共 16 章, 主要内容有计算机网络安全概述、网络安全管理及技术基础、密码技术、数据备份和恢复、网络安全隔离、网络接入认证、无线网络安全、IPv6 安全问题、典型网络应用安全保障、系统安全防护、检测和恢复技术、网络安全风险分析和评估、信息系统安全保障等。本书面向应用, 在强调相关基础知识的同时, 阐述和介绍了网络安全管理和防护技术的基本原理、方法、措施以及案例, 加强了理论和实践的结合。

本书既可供从事计算机网络、网络管理、信息安全及相关工作的专业人员学习、研究参考, 也可作为理工专业高年级本科生、研究生学习网络管理、网络安全方面的教材或者参考书。

计算机网络安全与防护

张 靖 编著

出 版: 电子科技大学出版社 (成都市一环路东一段 159 号电子信息产业大厦 邮编: 610051)

策划编辑: 周清芳

责任编辑: 周清芳

主 页: www.uestcp.com.cn

电子邮箱: uestcp@uestcp.com.cn

发 行: 新华书店经销

印 刷: 成都蜀通印务有限责任公司

成品尺寸: 185mm×260mm 印张 21 字数 520 千字

版 次: 2010 年 8 月第一版

印 次: 2010 年 8 月第一次印刷

书 号: ISBN 978-7-5647-0591-6

定 价: 48.00 元

■ 版权所有 侵权必究 ■

- ◆ 邮购本书请与本社发行部联系。电话: (028) 83202463, 83208003。
- ◆ 本书如有缺页、破损、装订错误, 请寄回印刷厂调换。

前 言

我国网民数量已经超过 3 亿，互联网用户数高居世界第一。同时，互联网普及率达到 22.6%，总带宽 625Gbps，IP 地址 1.8 亿个，手机上网用户 1.17 亿……数据大幅增长的背后是信息网络与国民经济的联系日益紧密，购物、交友、获取等信息都可通过网络进行，但随之而来的是网络与信息安全问题日益突出。

随着网络技术的不断发展和应用普及，网络受到破坏和攻击的行为日渐增多，一些系统和资源也越来越频繁地被侵入、修改、盗取等，在众多单位部门和普通百姓日益依赖网络时，却发现网络如此脆弱，发现网络安全的保障体系、运行机制、技术保障，甚至管理都有很多漏洞、缺陷，网络的安全管理和技术保障越来越得到重视，并已成为衡量一个信息系统是否完善、安全的重要标志。

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、应用数学、数论、信息论、管理等多种学科的综合性学科。有关网络管理、网络技术等的文献资料、书籍很多，涉及的专业知识面很广，也有相当的复杂程度。实际上，网络安全与人、设备、环境、政策、技术等因素相关，网络安全除了加强主动预防技术，还要增强评估、监测、恢复等手段。本书根据网络安全存在的问题和技术处理需要，把网络安全相关专业的管理、技术等知识内容比较系统地衔接起来，有利于读者学习、理解、掌握和进一步地深入实践和研究。

自 2001 年开始，作者为计算机科学与技术专业的本科生开设了《计算机网络》、《网络管理》、《网络安全》专业课，2005 年开始承担公安部、人事部信息网络安全专业技术人员继续教育培训《信息网络安全管理》、《信息网络安全技术》、《互联网信息内容安全管理》和《互联网上网服务营业场所安全管理》的授课，并担任主讲教师。作者一直负责校园网的建设、管理和研究工作，本书的内容编排以多年来授课为基础，并融合了工作经历和科研成果，本着“实用、完整、理论联系实际”的原则，与众多从事网络安全工作和研究的同仁一起分享自己的感受。

本书共分 16 章，第 1 章主要介绍网络安全的形势、网络安全概述以及网络攻击；第 2 章介绍网络安全的基本概念和网络攻击技术；第 3 章介绍加（解）密码基本原理和密码技术；第 4 章介绍数据备份和恢复的原理以及相关技术；第 5 章介绍网络管理的概念、功能、结构、协议等基本内容；第 6 章介绍网络安全的常见技术以及手段；第 7 章介绍网络隔离与安全交换，通过逻辑隔离或物理隔离技术，将网络分割成不同的通信域，以达到网络信息高度安全的目的；第 8 章介绍网络终端接入认证技术；第 9 章介绍典型网络应用的安全

技术以及保障措施；第 10 章介绍无线局域网的安全；第 11 章介绍蜜罐技术原理和蜜网技术；第 12 章介绍 IPv6 出现的安全问题以及安全措施；第 13 章介绍信息系统的防护和检测、网络端口扫描和漏洞检测以及响应、恢复技术；第 14 章介绍安全风险分析评估、安全审计的概念和方法；第 15 章介绍信息系统安全保障概念、目标、体系、内容、策略等内容；第 16 章以校园网为例介绍了一个网络安全管理和技术保障的实例，重点介绍了校园网的主要安全内容、安全策略和安全保障技术、措施。

本书编著工作得到了四川机电职业技术学院刘松青老师和攀枝花学院杨晓男、周伟、张翔、张杰、冯霞等老师的大力帮助，他们对本书提出了很多宝贵的意见，在此特别致谢。

由于作者水平有限，时间仓促，书中不足之处甚至错误在所难免，恳请读者批评指正，作者表示衷心感谢。

张 靖
2010 年 6 月

目 录

第 1 章 概述	1
1.1 网络安全形势	1
1.2 我国网络安全形势	2
1.3 网络安全概述	5
1.3.1 网络安全	5
1.3.2 网络不安全因素	6
1.3.3 网络不安全原因	6
1.3.4 网络安全保护内容	7
1.3.5 网络安全威胁	7
1.4 常见的网络攻击	8
1.4.1 拒绝服务攻击	8
1.4.2 网络访问攻击	10
1.4.3 后门软件攻击	11
1.4.4 解密攻击	11
1.5 网络安全的层次和内容	11
1.6 网络安全的趋势	13
第 2 章 网络安全	14
2.1 网络安全的概念	14
2.2 网络安全的意义	14
2.3 计算机网络面对的安全问题	15
2.3.1 物理安全	15
2.3.2 安全威胁	16
2.4 网络安全的相关问题	19
2.4.1 网络安全的基本要求	19
2.4.2 网络安全的目标	20
2.4.3 安全威胁	20
2.4.4 安全服务	20
2.4.5 安全机制	21
2.4.6 安全策略	22
2.5 TCP/IP 的安全性分析	23
2.6 网络攻击技术分析	24

第3章 密码技术.....	25
3.1 密码技术概述.....	25
3.1.1 密码技术的起源和历史.....	25
3.1.2 密码技术的主要用途.....	25
3.1.3 密码学的基本概念.....	26
3.1.4 密码通信系统的模型.....	27
3.1.5 密码体制.....	27
3.1.6 密钥与密码破译方法.....	30
3.2 常见加密算法介绍.....	31
3.2.1 DES 算法.....	31
3.2.2 RSA 算法.....	40
3.3 密钥分配管理.....	44
3.3.1 密钥的管理.....	44
3.3.2 私钥分配.....	47
3.3.3 公钥分配.....	48
3.4 数字签名技术.....	49
3.4.1 数字签名的概念.....	49
3.4.2 数字签名及验证过程.....	50
3.5 基于 X.509 证书的 PKI.....	51
3.5.1 X.509 标准.....	51
3.5.2 数字证书.....	53
3.5.3 PKI 的概念.....	54
3.5.4 PKI 模型.....	55
3.5.5 PKI 的组成.....	56
3.5.6 CA 系统.....	57
3.5.7 PKI 提供的服务.....	60
3.5.8 PKI 的应用.....	61
3.6 PGP 加密软件.....	62
3.6.1 PGP 简介.....	62
3.6.2 PGP 工作原理.....	62
3.6.3 PGP 密钥管理.....	63
3.6.4 PGP 应用.....	64
第4章 数据备份及恢复.....	67
4.1 数据备份及恢复综述.....	67
4.1.1 数据备份综述.....	67
4.1.2 数据恢复综述.....	68
4.2 数据备份及恢复基本原理.....	69
4.2.1 数据备份的原则.....	70

4.2.2	数据恢复原则.....	71
4.3	数据备份及恢复技术应用.....	72
4.3.1	备份技术.....	72
4.3.2	恢复技术.....	75
4.3.3	备份管理.....	76
4.3.4	备份策略和数据恢复策略.....	76
4.4	高可用技术.....	77
4.4.1	RAID 技术.....	77
4.4.2	集群技术.....	79
4.4.3	双机容错技术.....	79
4.5	安全存储应用.....	80
4.5.1	NAS.....	80
4.5.2	SAN.....	82
4.5.3	IP 存储网络.....	84
第 5 章	网络安全管理.....	89
5.1	网络管理概述.....	89
5.1.1	网络管理的参考模型.....	89
5.1.2	网络管理的基本要素.....	90
5.1.3	网络管理技术的综合.....	91
5.2	网络管理的基本功能.....	91
5.2.1	配置管理.....	91
5.2.2	性能管理.....	92
5.2.3	故障管理.....	93
5.2.4	安全管理.....	93
5.2.5	计费管理.....	94
5.3	网络管理的体系结构.....	95
5.4	SNMP 简介.....	96
5.4.1	SNMP 网络管理体系结构.....	96
5.4.2	管理信息结构.....	98
5.4.3	管理信息库 (MIB, Management Information Base)	98
5.4.4	SNMP 协议.....	99
5.4.5	SNMP 操作.....	100
5.4.6	SNMP 的五种基本原语.....	101
5.4.7	SNMP 的消息格式.....	102
第 6 章	网络安全技术.....	105
6.1	网络安全技术手段.....	105
6.1.1	加密技术.....	105
6.1.2	访问控制技术.....	105

6.1.3	身份认证技术	105
6.1.4	入侵检测技术	106
6.2	防火墙技术	106
6.2.1	防火墙技术概述	106
6.2.2	防火墙技术的定义	106
6.2.3	防火墙的作用	106
6.2.4	防火墙技术的发展	107
6.2.5	防火墙的工作原理	107
6.2.6	防火墙的基本技术	108
6.2.7	防火墙的局限性	109
6.3	入侵检测	110
6.3.1	入侵检测系统的功能和基本结构	111
6.3.2	入侵检测系统的分类	112
6.3.3	入侵检测系统的作用	114
第7章	安全隔离与信息交换	115
7.1	网络安全隔离与信息交换技术概述	115
7.1.1	信息安全隔离的重要性	115
7.1.2	网络安全体系架构的演变	115
7.1.3	隔离技术的发展过程	117
7.1.4	网络隔离系统的安全目的	118
7.2	安全隔离与信息交换技术原理	118
7.2.1	安全隔离与信息交换的“轮渡”模型	118
7.2.2	网络隔离和数据隔离	120
7.2.3	隔离网闸的安全模型	120
7.3	安全隔离与信息交换技术实现	121
7.3.1	基于 OSI 七层模型的隔离实现	121
7.3.2	“摆渡”技术的实现	122
7.4	网络安全中的物理隔离技术	123
7.4.1	基于不同层面的隔离防护技术	123
7.4.2	物理隔离技术	123
7.4.3	桌面级物理隔离产品	126
7.4.4	企业级物理隔离技术	127
7.5	物理隔离网闸的应用发展	130
第8章	网络接入认证	132
8.1	IEEE 802.1x 认证技术	132
8.1.1	IEEE 802.1x 起源	132
8.1.2	IEEE 802.1x 体系结构	132
8.1.3	IEEE 802.1x 认证机制	134

8.1.4	IEEE 802.1x 认证过程	135
8.1.5	IEEE 802.1x 认证特点	137
8.2	PPPoE 认证	138
8.2.1	PPPoE 协议简介	138
8.2.2	PPPoE 协议工作原理	139
8.2.3	PPPoE 帧格式	141
8.2.4	PPPoE 认证的特点	141
8.3	Web 认证	142
8.3.1	Web 认证过程	142
8.3.2	Web 认证的特点	142
8.3.3	Web 认证和 PPPoE 认证技术应用	143
8.3.4	几种认证方式的比较	144
8.4	RADIUS 认证服务器	145
8.4.1	RADIUS 认证机制	145
8.4.2	RADIUS 关键特征	146
8.4.3	RADIUS 认证系统的构成	147
8.4.4	RADIUS 的数据包结构	147
8.4.5	RADIUS 的认证、计费过程	148
8.4.6	RADIUS 认证服务器实现	149
8.5	VPN	153
8.5.1	VPN 的基本概念	153
8.5.2	VPN 常见用途	154
8.5.3	实现 VPN 的隧道协议	155
8.5.4	基于数据链路层的 VPN 协议	156
8.5.5	基于网络层的 IPSec 协议	158
8.5.6	基于会话的 VPN 技术	162
8.5.7	企业构建 VPN 的解决方案	164
8.5.8	VPN 应用的解决方案	166
第 9 章	典型网络应用服务安全	171
9.1	DNS 安全	171
9.1.1	DNS 安全问题	171
9.1.2	DNS 安全解决方案	173
9.2	WWW 安全	177
9.2.1	Web 安全威胁与对策	177
9.2.2	常用 Web 协议	178
9.2.3	Web 安全的实现方法	180
9.2.4	Apache Web 服务器安全机制	181
9.2.5	Web 页面存储安全	183
9.2.6	Web 审计	183

9.3	MAIL 安全.....	183
9.3.1	电子邮件服务器系统.....	183
9.3.2	邮件协议.....	184
9.3.3	电子邮件安全.....	185
9.3.4	电子邮件安全技术.....	187
9.4	FTP 安全.....	193
9.4.1	FTP 概述.....	193
9.4.2	安全防护.....	195
9.5	Telnet.....	196
9.5.1	Telnet 协议.....	196
9.5.2	Telnet 安全.....	196
9.5.3	Telnet 安全防范.....	196
9.6	漏洞和恶意代码.....	199
9.6.1	漏洞概述.....	199
9.6.2	恶意代码.....	203
9.7	计算机病毒.....	207
9.7.1	计算机病毒概念.....	207
9.7.2	计算机病毒的类型.....	208
9.7.3	计算机病毒发展方向.....	208
9.7.4	计算机反病毒技术.....	209
9.7.5	计算机病毒处理措施.....	210
9.8	操作系统安全概述.....	211
9.8.1	操作系统安全.....	211
9.8.2	操作系统主要安全技术.....	211
9.9	P2P 网络及其安全.....	217
9.9.1	P2P 网络的概念.....	217
9.9.2	P2P 网络安全需求.....	218
9.9.3	P2P 安全典型解决办法.....	221
第 10 章	无线网络安全.....	224
10.1	无线网络的特点.....	224
10.2	无线局域网安全.....	225
10.2.1	无线局域网缺陷.....	225
10.2.2	无线局域网安全问题.....	226
10.3	无线局域网安全管理要求.....	227
10.3.1	AP 安全要求.....	227
10.3.2	AC 安全要求.....	228
10.4	无线网攻击.....	228
10.4.1	War Driving.....	228
10.4.2	拒绝服务攻击.....	229

10.4.3	中间人攻击.....	229
10.4.4	欺骗攻击.....	229
10.4.5	暴力攻击.....	230
第 11 章	蜜罐技术.....	231
11.1	蜜罐的概念.....	231
11.1.1	蜜罐的定义.....	231
11.1.2	Honeypot 分类.....	231
11.1.3	蜜罐产品.....	232
11.2	蜜网技术.....	233
11.2.1	蜜网技术.....	233
11.2.2	蜜网工作方式.....	234
11.2.3	蜜网应用.....	236
11.3	Honeypot 主要技术.....	237
11.3.1	网络欺骗技术.....	237
11.3.2	数据捕获.....	238
11.3.3	数据分析.....	238
11.3.4	数据控制.....	238
11.4	蜜罐技术的特点.....	239
11.4.1	蜜罐的优点.....	239
11.4.2	蜜罐的缺点.....	240
11.5	Honeyd 典型应用.....	240
11.5.1	Honeyd 应用.....	240
11.5.2	Honeyd 安装与配置.....	241
第 12 章	IPv6 安全问题.....	244
12.1	IPv6 产生的新问题.....	244
12.2	主要攻击方式.....	244
12.3	传统网络安全工具在 IPv6 下的改进.....	247
12.3.1	漏洞扫描.....	247
12.3.2	防火墙.....	248
12.3.3	入侵检测系统.....	248
12.3.4	网络安全审计系统.....	249
第 13 章	信息系统防护和检测.....	250
13.1	系统安全防护.....	250
13.1.1	认证的能力和技术.....	250
13.1.2	访问控制的能力及技术.....	252
13.1.3	内容安全能力分析及技术.....	253
13.2	系统安全检测.....	255
13.2.1	安全漏洞扫描.....	255

13.2.2	入侵检测.....	255
13.2.3	安全审计.....	256
13.3	扫描技术及分类.....	256
13.3.1	网络安全扫描技术.....	256
13.3.2	端口扫描技术.....	257
13.3.3	漏洞扫描技术.....	259
13.3.4	漏洞扫描工具.....	261
13.4	网络监听.....	262
13.4.1	监听基本原理.....	262
13.4.2	网络监听工具.....	263
13.4.3	防止网络被监听.....	264
13.5	响应和恢复.....	264
13.5.1	响应和恢复必要性.....	264
13.5.2	响应和恢复过程.....	264
13.5.3	响应和恢复前期保障技术.....	265
第 14 章	风险分析与评估	266
14.1	风险分析和评估概念.....	266
14.1.1	风险分析概念.....	266
14.1.2	风险评估相关概念.....	266
14.2	风险分析与评估技术.....	267
14.2.1	确定风险大小.....	267
14.2.2	风险分析与评估目标.....	269
14.2.3	风险分析与评估步骤.....	269
14.2.4	风险分析方法.....	270
14.3	网络安全评估.....	271
14.3.1	网络安全评估发展过程.....	272
14.3.2	网络安全评估研究现状.....	272
14.3.3	网络安全评估标准.....	273
14.4	信息安全风险评估.....	274
14.4.1	风险评估要素.....	274
14.4.2	风险评估过程.....	275
14.4.3	风险评估方式.....	277
14.4.4	风险评估方法.....	277
14.4.5	风险评估流程.....	278
14.5	安全审计.....	280
14.5.1	安全审计概念.....	280
14.5.2	安全审计功能.....	281
14.6	系统安全测评制度.....	281
14.6.1	目的.....	281

14.6.2	阶段.....	281
14.6.3	测评内容.....	282
第 15 章	信息系统安全保障体系.....	283
15.1	信息安全管理目标.....	283
15.2	安全保障基本内容.....	284
15.2.1	通信安全.....	284
15.2.2	环境安全.....	285
15.2.3	内容安全.....	285
15.3	典型信息系统安全模型.....	285
15.3.1	OSI 安全体系结构.....	285
15.3.2	P2DR 模型.....	286
15.3.3	五层网络安全体系.....	287
15.3.4	我国安全保障体系.....	287
15.4	网络安全保护技术体系.....	289
15.4.1	技术体系.....	289
15.4.2	对抗网络攻击保障措施.....	290
15.5	信息系统的安全策略.....	291
15.5.1	安全策略的概念.....	291
15.5.2	安全策略与其他要素的关系.....	293
15.5.3	制订安全策略原则.....	293
15.5.4	安全策略的设计范围.....	294
15.5.5	信息安全策略制订.....	295
15.5.6	安全策略管理.....	295
15.6	人员安全管理.....	296
15.6.1	人员安全管理原则.....	296
15.6.2	人员的审查.....	296
15.6.3	人员的考核.....	297
15.6.4	人员安全培训与教育.....	297
15.6.5	离岗人员的安全管理.....	297
15.7	资产安全管理.....	297
15.7.1	硬件安全管理.....	298
15.7.2	软件安全管理.....	298
15.7.3	技术文档安全管理.....	299
15.8	物理安全管理.....	300
15.8.1	机房环境安全技术.....	300
15.8.2	通信线路安全.....	302
15.8.3	设备安全.....	302
15.8.4	电源系统安全.....	303

第 16 章 网络安全保障实例.....	304
16.1 校园网面对的主要安全问题.....	304
16.2 网络安全策略.....	305
16.2.1 环境安全策略.....	305
16.2.2 安全管理职责和条文.....	306
16.2.3 安全管理组织机构.....	307
16.2.4 安全管理政策与制度.....	308
16.2.5 应急响应.....	310
16.3 校园网安全技术实施.....	312
16.3.1 设备的物理安全.....	313
16.3.2 设备冗余.....	315
16.3.3 设备的逻辑安全.....	315
16.3.4 路由安全.....	316
16.3.5 黑洞过滤.....	317
16.3.6 LAN 交换机安全.....	318
16.3.7 防火墙的设置.....	319
16.3.8 IDS 设置.....	319
16.3.9 远程访问设置.....	319
16.3.10 网络设备远程管理安全.....	320
16.3.11 服务器和终端安全设置.....	320
16.3.12 数据备份.....	321
参考文献.....	322

第1章 概述

1.1 网络安全形势

网络日益普及的今天,互联网已逐步成为人们生活和工作中必不可少的组成部分。网络涉及国家的政府、军事、文教等诸多领域。其中,存储、传输和处理的信息有许多是重要的政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要信息。通过网上的协同和交流,人的智能和计算机快速运行的能力汇集并融合起来,创造了新的社会生产力,交流、学习、医疗、消费、娱乐、安全感、安全环境、电子商务、网上购物等满足着人们的各种社会需要。然而,与此同时,网络社会与生俱来的不安全因素,如信息泄漏、信息窃取、数据篡改、数据删添、计算机病毒等各种人为攻击也无时无刻不在威胁着网络的健康发展。基于网络的威胁潜伏在每一个角落。

互联网自21世纪初,在世界各国都得到了前所未有的发展,尤其在中国,可谓是突飞猛进。我们可以看到随着互联网的快速发展,虚拟与现实生活越来越难以割裂,政府、企业发展都与互联网的发展息息相关,个人的生活、工作也越来越依赖于计算机网络,互联网的发展给整个世界的发展带来了一次伟大的革命。人与人、国与国之间距离在不断缩小,从“地球村”到“世界是平的”一说,都意味着人类越来越意识到互联网的含义。越来越多的人发现,随着互联网的发展,他们能够找到更多的合作对象和竞争对手,地球上的各个知识中心都将被统一到了单一的全球网络中。但不幸的是,随着网络发展而衍生出来的网络安全问题也时刻威胁着“地球村”的“村民”们,例如计算机病毒、流氓软件、间谍软件等。由于Internet的开放性和超越组织与无国界等特点,使它在安全性上也同样存在着开放性和无国界性,因此,给网民带来了严重的安全隐患问题。那么,何为网络安全威胁,网络安全威胁到底会给社会带来怎样的后果呢?

网络安全关系政治、经济、军事、科技和文化等国家信息安全。据有关报道,2000年美国发生网上恐怖事件,短短几天内电子商务网站、股市网站等损失达12亿美元;2001年日本东京国际机场航管由于红色代码病毒导致的系统失灵,影响巨大,造成几百架飞机无法起降、千人行程受阻;2003年,美国银行的ATM网络遭到入侵,损失惨重,2005年的4000多万张卡用户信息被盗,并被植入特洛伊木马,假冒消费,由此导致用户巨大的财产损失,这是美国最大的窃密事件……由于这些事件的不断发生,人们对网络安全的认识也在不断深入,对信息安全防护能力、隐患发现能力、网络应急反应能力以及对抗能力的要求也在不断提升。因此,网络的安全问题就显得更加关键和重要。

据统计,在全球范围内,由于信息系统的脆弱性而导致的经济损失,每年达数亿美元,并且呈逐年上升的趋势。据美国《金融时报》报道,现在平均每20秒就发生一次入侵计算

机网络的事件；超过 1/3 的互联网防火墙被攻破。中国工商银行、中国银行、中国建设银行等金融机构先后成为黑客们模仿的对象，设计了类似的网页，通过网络钓鱼的形式获取利益，而这一现象正在以每个月 73% 的数字增长，使很多用户对网络交易的信心大减。在历史上，由于网络的不安全而给军队带来损失的案例也是不计其数。海湾战争前，美军将带有“病毒”的计算机通过法国卖给伊拉克军队。海湾战争初期，美军就对伊军实施了“病毒”战，使其防空指挥控制系统失灵，指挥文书只能靠汽车传递，在整个战争中都处于被动挨打的局面。同样，网络的不安全也影响了人们的生活，对构建和谐社产生了阻碍。尊重隐私权是每个公民应有的权利，但侵犯信息隐私权的事件在网络上大量存在。网络一旦遭到非法攻击，网络操作系统中的用户全称、电话号码和办公地点等信息，就可能被复制或篡改，网民的基本信息就得不到保障。

1.2 我国网络安全形势

我国互联网基础设施和重要信息系统整体上运行基本正常，没有出现造成严重影响或后果的大规模网络安全事件。但是，网络攻击的频次、种类和复杂性均比往年大幅增加，遭入侵和受控计算机数量增多，潜在威胁和攻击力继续增长，信息数据安全问题日益突出，网络安全形势依旧严峻。

2008年 国家互联网应急中心（CNCERT）接收和自主监测的各种网络安全事件数量与 2007年上半年同期相比有较为显著的增加。其中，垃圾邮件事件和网页恶意代码事件增长较快，网页恶意代码同比增长近一倍；网页篡改事件和网络仿冒事件也有大幅增长，同比增长分别是 23.7% 和 38%，其中，涉及国内政府机构和重要信息系统部门的网页篡改事件、涉及国内外商业机构的网络仿冒事件是 2008年上半年事件监测和处置的重点。

网页篡改事件特别是我国大陆地区政府网页被篡改事件呈现大幅增长趋势。统计显示，2008年上半年我国大陆地区被篡改的 .gov.cn 网站数量比 2007年上半年增加 41%，共计 2 242 个，占被篡改网站总数的比例达到 7%，而 .gov.cn 域名仅占 .cn 域名总数的 2.3%，这说明 .gov.cn 网站遭受黑客攻击的可能性相对较高。2008年 5月 1日，我国颁布施行《政府信息公开条例》，该《条例》的推行对政府信息化建设提出了新的要求，同时也对电子政务信息系统的网络安全提出更高的要求。由于政府网站整体安全水平较低，往往是黑客攻击的重要目标，因此，作为政府对外形象的窗口、发布权威信息和与公众开放交流的平台，电子政务信息系统的网络安全管理成为各级部门必须高度重视的问题。

我国大陆地区感染木马和僵尸网络的主机数量巨大。据 CNCERT 的监测数据显示，2008年前 5个月监测到的感染木马和僵尸网络的主机数量缓慢波动上涨，但在 6月份出现跳跃式增长。这一现象跟 CNCERT 加强监测力度和扩大监测范围有关，但更令人担忧的原因则是攻击者似乎在北京奥运会前夕加紧活动，图谋通过网络攻击干扰数字奥运的顺利举行。

造成木马和僵尸网络产生和扩散的一大途径是恶意代码的肆虐传播。2008年上半年，CNCERT 通过技术平台共捕获约 90万个恶意代码，比 2007年同期增长 62.5%。其中，新的恶意代码样本 8.9万个，与 2007年同期基本相近；通过国内外合作渠道接收到恶意代码样本 49.6万个。综合各种来源数据并从中去掉重复的恶意代码样本，2008年上半年实际新增恶意代码样本数达 52.9万个。数据合作方包括国内外主要的反病毒厂商、CERT 组织和安全机构。