

# 信息系统安全技术

黄继海  
杨 凯 等编著  
杨建国



河南科学技术出版社

• 郑州 •

## 内 容 简 介

本书从计算机泄密途径和我国网络信息安全现状入手,介绍了信息安全和网络安全技术的基本知识,涉及身份认证技术、常用加密算法、访问控制技术、入侵检测技术、防病毒技术、网络隔离、防火墙技术、安全扫描技术和安全审计技术等网络信息安全体系,并详细讲解了指纹和声纹等高科技加密手段。实际指导架设 Linux 下的 VPN 安全系统,分析黑客常用的网上攻击方法针对性采用先进的防护手段保障网络安全,同时对操作系统的安全和网站建设的安全问题进行系统地研究和方案设计。以实际案例较为全面地介绍了现代流行的信息安全技术。

本书注重理论和实践相结合,内容实用、层次分明、语言流畅,所涵盖的内容对大家提高网络安全意识和主动进行网络安全防护是不可或缺的。

阅读本书的读者应具备基本的计算机网络知识。本书可以作为计算机类专业或信息类相关专业的本科或专科教材,也可供从事计算机网络开发和安全研究的科研人员参考,同时可以作为一本网络安全手册。

### 图书在版编目(CIP)数据

信息系统安全技术/黄继海等编著. —郑州:河南科学技术出版社, 2006. 2

ISBN 7-5349-3455-9

I. 信… II. 黄… III. 信息系统-安全技术 IV. TP309

中国版本图书馆CIP数据核字(2006)第005649号

---

出版发行:河南科学技术出版社

地址:郑州市经五路66号 邮编:450002

电话:(0371) 65737028

责任编辑:张晓东

责任校对:柯姣

封面设计:张伟

版式设计:栾亚平

印刷:河南第一新华印刷厂

经销:全国新华书店

幅面尺寸:185 mm×260 mm 印张:13.75 字数:400千字

版次:2006年2月第1版 2006年2月第1次印刷

印数:1—3 100

定价:28.00元

---

如发现印、装质量问题,影响阅读,请与出版社联系。

## 《信息系统安全技术》编写人员

编  
著

黄继海      杨    凯      杨建国      于政庆

郎士宁      孟    军      李宝林      王    辉

审  
稿

左    军

# 前 言

当今时代，因特网将全球的无数台计算机联网，形成了由计算机、光纤、电缆和卫星构成的另一个地球、另一个世界、另一个村落。表面看似平静的信息网络，其内部信息流无时不是汹涌澎湃，人们在享受便利的同时，也面临各种威胁，黑客、病毒、信息窃取等网络犯罪无时不在。小到个人隐私，大到国家机密无时不受到侵犯。这使得我们不得不研究网络信息系统安全。

与政治霸权、经济霸权和军事霸权相对应，网络又催生出了文化霸权和文化侵略。网络安全又成为国家继领土、领海和领空之后的第四维领地。信息系统安全严重影响着国家的文化安全。何谓“文化安全”？文化安全，是指一个国家或一个民族的文化受到外来消极思想文化的影响，使本国或本民族文化受到侵害，出现衰落或消亡。保护本国或本民族的文化安全已经成为人们关注的重点。何谓“文化霸权”？文化霸权，亦称文化强权，是指国与国之间、民族与民族之间的文化价值观的强加行为。以往一种文化渗入另一种文化需要用几年甚至几十年的时间，而今天，在经济和信息全球化的时代里，现代传播技术的发展大大加速了思想、文化传播的速度和进程。掌握有先进科学技术的发达国家，因为拥有强大的综合国力，特别是拥有先进的网络等传播技术和手段，正在竭力拓展世界思想文化市场，控制思想文化资源，把建立文化霸权作为谋求世界霸权的全球战略的重要组成部分。20世纪80年代末至90年代初苏联和东欧的演变，就被认为是思想文化渗透成功。他们把这种做法称之为“静悄悄的文化输出”，是对社会主义国家的“软化战争”。中国是社会主义国家，又是发展中国家，历来是西方发达国家思想文化渗透的重点目标。为了我们的文化安全，我们也不得不研究网络信息系统安全。

网络战，是以计算机和计算机网络为目标，以信息技术为手段，在整个网络空间所进行的各类信息攻防作战的总称。网络战已悄悄走上战争舞台，信息网络已成为新的战场和作战平台。在未来信息时代的信息化战争中，军队不再被陆地、高山、海洋阻隔，战场将被智能的、无缝的信息网络连成一体，使战场上每一个战斗员及与战场有关的人员战斗在一个虚拟而又客观存在的“信息球”之中。网络提供一体化信息支持能力，即通过数字化、网络化、自动化、智能化的信息系统，以通信网络为纽带，以信息处理为核心，将遍布陆海空天的战场感知系统、指挥自动化系统、火力打击武器平台和信息攻击武器平台等作战体系各要素联结成为一个有机的整体，实现全维信息感知、实时信息传输和智能信息处理，为联合作战提供一体化信息支持。在信息化战场上，信息获取、信息传输和信息处理，三者实时互动，有机联结，密不可分，形成一体化信息支持能力。军事斗争的需求更要研究网络信息系统安全。

由于作者水平有限，错误之处难免，敬请指正。对于本书引用的文献和案例，在此向原创者表示谢意。

作 者

2006年1月于郑州

# 目 录

---

---

第 1 章 网络信息安全概论 .....	1
1.1 计算机泄密的主要途径 .....	1
1.1.1 计算机电磁波辐射泄漏 .....	1
1.1.2 计算机网络化造成的泄密 .....	2
1.1.3 计算机媒体泄密 .....	2
1.1.4 内部工作人员泄密 .....	3
1.2 我国网络信息安全现状 .....	3
1.2.1 软件和硬件设备上严重依赖国外, 安全技术有待研究 .....	3
1.2.2 网络安全管理存在漏洞 .....	4
1.2.3 研究项目和网络安全基础设施 .....	5
第 2 章 信息安全的基本要素 .....	7
2.1 网络与信息安全的概念 .....	7
2.1.1 网络信息安全的定义 .....	7
2.1.2 网络信息安全问题研究 .....	7
2.1.3 网络安全和信息安全基本要素 .....	8
2.1.4 案例: Jump® (捷普) 内网综合审计监管系统 .....	9
2.2 安全策略 .....	12
2.2.1 什么是安全策略 .....	12
2.2.2 安全策略方案 .....	14
2.2.3 案例: 天和信息技术全面、动态的安全策略 .....	15
2.2.4 网络安全策略实施过程 .....	16
第 3 章 网络信息安全技术体系 .....	18
3.1 身份认证技术 .....	18
3.1.1 用户-机器的用户验证 .....	18
3.1.2 主机-主机用户验证 .....	20
3.1.3 内网身份认证 .....	20
3.1.4 案例: 应用在 Linux 上的指纹识别系统 .....	22
3.1.5 案例: USB 声纹锁 .....	23
3.2 密码技术 .....	24

3.2.1	密码学要实现的基本功能	24
3.2.2	加密算法	25
3.2.3	案例: RSA 算法实践	30
3.2.4	单向散列算法	34
3.2.5	密钥的管理	37
3.2.6	密码学大事记	38
3.3	访问控制技术	39
3.3.1	入网访问控制	39
3.3.2	网络权限控制	40
3.3.3	目录级安全控制	40
3.3.4	属性安全控制	41
3.3.5	服务器安全控制	41
3.3.6	案例: 访问控制产品	41
3.4	防病毒技术	43
3.4.1	蠕虫病毒及其防范	44
3.4.2	特洛伊木马、逻辑炸弹及其防范	48
3.4.3	防病毒技术的发展	50
3.5	网络隔离技术	51
3.5.1	隔离技术的发展历程	51
3.5.2	隔离技术需具备的安全要点	52
3.5.3	案例: 物理隔离技术斩断网上黑手	53
3.6	防火墙技术	56
3.6.1	防火墙的概念	56
3.6.2	防火墙的分类	58
3.6.3	防火墙的主要功能	62
3.6.4	防火墙策略	64
3.6.5	防火墙技术的发展	69
3.6.6	第四代防火墙的技术与功能	71
3.6.7	案例: 天网防火墙个人版	73
3.6.8	案例: 2004 年度中国市场主流防火墙产品评测技术报告	74
3.7	入侵检测技术	82
3.7.1	入侵检测的概念	82
3.7.2	入侵检测系统的分类及其主要功能	82
3.7.3	入侵检测系统的关键技术	82
3.7.4	入侵检测过程	83
3.7.5	案例: 免费 NIDS 系统——snort	85
3.7.6	案例: 天阍入侵检测与管理系统	92

3.8	安全扫描技术	93
3.8.1	网络安全扫描技术简介	93
3.8.2	案例：常见网络安全漏洞扫描器	96
3.9	审计技术	97
3.9.1	与审计有关的概念	98
3.9.2	需要重点审计的几个方面	99
3.9.3	构建安全审计系统的关键点	99
3.9.4	案例：电子数据安全审计	100
3.10	虚拟专用网（VPN）技术	102
3.10.1	VPN 的基本概念	102
3.10.2	VPN 使用的协议	103
3.10.3	VPN 的身份验证方法	104
3.10.4	VPN 的加密技术	105
3.10.5	案例：Windows 2000 VPN 的安装	105
3.10.6	案例：架设 Linux 下最简单的 VPN 系统	108
第 4 章	黑客与网络攻击技术	113
4.1	黑客	113
4.2	黑客攻击的主要方式	114
4.2.1	拒绝服务攻击	114
4.2.2	典型 DoS 攻击原理及抵御措施	115
4.2.3	非授权访问尝试	120
4.2.4	预探测攻击	120
4.2.5	特洛伊木马攻击	122
4.2.6	案例：偷拍电影网站藏木马	123
4.2.7	案例：查杀 P3 木马病毒	124
4.2.8	案例：预防震荡波蠕虫病毒	125
4.3	黑客攻击方法和途径	128
4.3.1	攻击途径	128
4.3.2	攻击方法	129
4.3.3	防护手段	130
4.3.4	案例：攻破天网的几种方法	130
第 5 章	操作系统安全	135
5.1	Windows 2000 安全	135
5.1.1	Windows 2000/NT 安全检查	135
5.1.2	Windows 2000 安全配置	136
5.1.3	案例：Windows 2000 中通过本地安全策略封杀端口	146
5.1.4	案例：修改注册表加强 Windows 2000 安全	149

---

---

5.1.5	案例: Microsoft ISA Server 2004 .....	152
5.2	Linux 安全 .....	157
5.2.1	Linux 病毒 .....	157
5.2.2	Linux 的安全措施 .....	158
第6章	应用服务安全 .....	164
6.1	DNS 服务安全 .....	164
6.1.1	名字欺骗 .....	164
6.1.2	隐藏信息 .....	165
6.2	域控制器 .....	166
6.2.1	域控制器简介 .....	166
6.2.2	案例: 保障 Windows Server 2003 域控制器的安全性 .....	166
6.3	DHCP 服务 .....	168
6.3.1	DHCP 服务简介 .....	168
6.3.2	案例: Windows 2000 DHCP 服务器的设置 .....	168
6.4	Web 服务 .....	170
6.4.1	Web 服务简介 .....	170
6.4.2	案例: Windows 2000 Web 站点的内容分级访问控制 .....	173
6.4.3	案例: Windows 2000 安全与权限设置 .....	174
6.4.4	安全认证 .....	176
6.4.5	IP 地址及域名限制 .....	177
6.4.6	停止、启动和暂定站点服务 .....	179
6.5	FTP 服务 .....	179
6.5.1	案例: 在 IIS 上架构的 FTP 站点 .....	179
6.5.2	案例: Linux 平台 FTP 的安全配置与应用 .....	182
6.5.3	案例: 构建中小企业或个人 E-mail 服务器指南 .....	189
6.6	数据库服务 .....	194
6.6.1	数据库服务简介 .....	194
6.6.2	案例: 保证 Oracle 数据库安全性的策略和方法 .....	198
6.7	Telnet .....	202
6.7.1	远程登录的基本概念 .....	202
6.7.2	Telnet 的作用 .....	203
6.7.3	案例: Windows 2000 的 Telnet 服务 .....	204
6.8	应用程序服务器 .....	207
6.8.1	应用程序服务器简介 .....	207
6.8.2	案例: Windows 2000 Internet 服务器安全构建指南 .....	208

# 网络信息安全概论

21

## 1.1 计算机泄密的主要途径

1.1.1

1 000

100

10

1 000

6.5

1. 1. 2

1

2

3 Internet

Internet

Internet

BBS

Internet

Internet

Internet

Internet

4

Internet

Internet

BO BO2000

5

1. 1. 3

1

2

3

4

5

6

7

1. 1. 4

1.

Internet

2.

Internet

Internet

3.

## 1.2 我国网络信息安全现状

1.2.1

CPU

" "

1.2.2

" " ( )

( )

90%

10%

" "

1. 2 3

" " " "  
20 90

15  
1998

" " UNIX  
UNIX B1

ATM

1 000

100

" "

UNIX

2004 12 26  
2

3 200

"

"

CPU

# 信息安全的基本要素

## 2.1 网络与信息安全的概念

ISO

CPU

CPU

CPU

CPU

CPU



IP

1.

2.

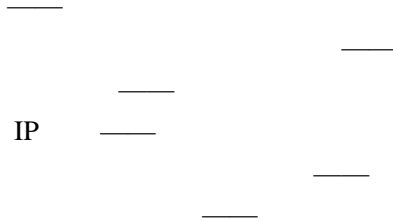
3.

4.



- 1
- 2
- 3
- 4
- 5
- 6

®



- 1
- 2 JOS
- 3
- 4
- 5
- 6 USB
- 7
- 8