“十一五”高等院校应用型规划教材

计算机系列

网络安全与维护

刘永华 主 编

李竹健 陈庆方 副主编

刘国英 年仁德 田 云 编 著

南京大学出版社

“十一五”高等院校应用型规划教材·计算机系列

网络安全与维护

刘永华　主　编

李竹健　陈庆方　副主编

刘国英　年仁德　田　云　编　著

南京大学出版社

内 容 简 介

本书涵盖了网络安全和管理的基本概念、原理和技术，主要包括操作系统安全、数字加密与认证、防火墙技术、入侵检测系统、网络病毒的防治技术、网络维护等内容。本书内容全面、取材新颖，既有网络安全和管理的理论知识，又有实用技术，反映了网络安全和管理技术的最新发展。

本书可作为大学本科及高职高专学校计算机、信息安全、网络工程、信息工程等专业信息安全课程的教材，也可供计算机爱好者、网络管理员及安全软件开发人员阅读和参考。

图书在版编目(CIP)数据

网络安全与维护/刘永华主编.—南京：南京大学出版社，2007.3

“十一五”高等院校应用型规划教材·计算机系列

ISBN 978-7-305-04948-4

Ⅰ. 网… Ⅱ. 刘… 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(2007)第 030690 号

出 版 者 南京大学出版社

社　　址 南京市汉口路 22 号　　邮编 210093

网　　址 http://press.nju.edu.cn

出 版 人 左　健

丛 书 名 “十一五”高等院校应用型规划教材·计算机系列

书　　名 网络安全与维护

主　　编 刘永华

副 主 编 李竹健　陈庆方

责任编辑 徐燕华　　编辑热线 83595844

照　　排 南京海洋电脑制版有限公司

印　　刷 南京大学印刷厂

开　　本 789×1092　1/16　　印张：19.5　　字数：392 千字

版　　次 2007 年 3 月第 1 版　2007 年 3 月第 1 次印刷

ISBN 978-7-305-04948-4

定　　价 29.80 元

发行热线 025-83592169　025-83592317

电子邮箱 sales@press.nju.edu.cn(销售部)

nupressl@publicl.ptt.js.cn

《“十一五”高等院校应用型规划教材》

编审委员会

丛书序

目前，我国高等教育正迎来一个前所未有的高速发展时期。社会的迫切需求是高等教育发展的最大动力，高等教育的发展已进入到一个新的阶段。高等本科院校也逐渐演变成“研究型、学术型”和“应用型、就业型”两大类。

而作为知识传承载体的教材，在“应用型”高等院校的教学活动中起着至关重要的作用。但目前教材建设却远远滞后于应用型人才培养的步伐，许多院校一直沿用偏重于研究型的教材，应用型教材比较缺乏，这势必影响应用型人才的培养。因此，我们顺应国家“十一五”规划的大局，在教育界相关专家的建议与指导下，坚持“以理论知识够用为前提，重点加强应用技能的培养”的原则，加大实验、实践的力度，由广大学校的老师结合本校的教学改革和精品课程建设，适时规划了这一系列教材，以顺应高等教育普及化迅速发展的趋势。

本套教材具有如下特色。

1. 理论知识以“够用”为前提，培养创新型的应用人才

本系列教材，以培养应用型人才为目标，确保理论知识的介绍够用，加大新知识、新技术的介绍，加强实验、实践的力度，以培养创新型的应用人才。

2. 注重现代教育技术在教学中的应用

本系列教材中的实验采用全程录像的方式，实例采用视频演示的方式讲授。每本书均配一张光盘，提供课堂实例的多媒体视频演示与实验的全程录像，以方便老师授课和学生自主学习。

3. 重视对学生应用能力的培养与训练

本系列教材的编写以“提高学生应用能力”为宗旨，按照企业对高校学生的实际需求，以“项目驱动法”来设计实例与实验，使学生能够在了解相关理论的基础上，具备相应的实际操作技能。

4. 立体化的教学资源网——提供网站优质服务与教学支持

面对“十一五”规划的新形势，为了继续深化课程与教学改革，更深入地解决课改与教改中的重点与难点问题，为中国高等教育的发展提供精工细做的食粮，我们不仅提供优秀的纸质主教材，还提供电子教案、教学大纲、实验录像、

视频演示、网络课程等教学配套资源，形成纸质出版物、电子音像与网络出版物等有机结合的立体化教学解决方案。

老师通过网络平台，可以获得更多、更好的教学资源；学生通过网络平台，可以随时随地进行学习。网络平台方便师生进行信息交流，实现资源共享。

前　言

《网络安全与维护》是高等学校普遍开设的一门计算机课程，是计算机及相关专业的重要的课程，在计算机素质教育方面发挥着重要作用。

本书是“十一五”高等院校应用型规划教材之一，本书作者是长期从事计算机网络和维护课程教学的一线教师，而且是高级网络管理人员，对计算机网络及相关课程的教学方法有较深的认识和系统的研究。本书作者在借鉴已有教材优点的基础上，针对大学本科、高职高专学生的特点，融入了多年的教学经验和网络维护经验编著完成。

随着网络应用的日益广泛，网络安全问题越来越受到关注。网络技术已被广泛应用于社会生活的各个方面，作为高等教育的教材，本书从网络安全的基本理论和技术出发，深入浅出、循序渐进地讲述了网络安全的基本原理、技术应用配置方法，内容全面，通俗易懂。全书分为 7 章，主要内容安排如下。

第 1 章具体介绍计算机网络安全的相关基础知识，包括网络安全的概念及影响网络安全的主要因素、网络安全的组成以及网络安全常用的技术。

第 2 章主要介绍操作系统安全，介绍了 Windows 和 Linux 操作系统的安全机制、安全漏洞和安全配置方案。

第 3 章介绍了网络安全中的密码技术，包括传统的加密方法、DES 加密标准、公开密钥体制和数字签名等技术。

第 4 章介绍了访问控制技术中的防火墙技术，包括防火墙的原理、种类和实现策略等。

第 5 章主要介绍了入侵检测的概念，对相关技术进行了全面介绍，并对入侵检测的未来发展进行了讨论。

第 6 章主要介绍了病毒的原理、病毒的类型和计算机网络病毒，同时介绍了几种影响较大的网络病毒，如 CIH 病毒、Word 宏病毒、Nimda 病毒和红色代码病毒等，并且介绍了病毒的清除及防护措施。

第 7 章主要介绍 Windows 自带的常用网络工具，讨论了网卡、集线器、交换机、路由器、网线和 RJ-45 接头等网络连接设备的维护，以及网络的性能优化等问题，并重点介绍了常用网络故障及排除方法。

由于网络安全的内容非常丰富，本书按理论教学以“必需、够用”为度，加

强实践性环节教学，以提高学生的实际技能的原则组织编写。讲究知识性、系统性、条理性、连贯性。本书力求激发学生的兴趣，注重提示各知识之间的内在联系，精心组织内容，做到由浅入深、由易到难、删繁就简、突出重点、循序渐进，使之适于课堂教学和实践教学。

全书由刘永华主编，李竹健、陈庆方副主编。其中第 1、3 章由刘永华编写，第 5、7 章由李竹健编写，第 2 章由陈庆方编写，第 4 章由刘国英、田云编写，第 6 章由年仁德编写，全书由刘永华统稿整理。另外，李凤慧、贾秀兰、黄忠义、张元国和李华英参加了本书编写大纲的讨论和制定，并参与编写了部分内容。本书在编写过程中参阅了大量国内外计算机网络安全书籍中的部分内容，并从 Internet 上参考了大量计算机网络安全、黑客技术与防范措施的资料。

本书的编写得到了许多友人的支持和帮助，在此表示衷心感谢。

由于编者能力有限，且时间匆忙，书中的不足之处，恳请专家及读者批评指正。

编　者

2006 年 10 月

目　　录

第 1 章　网络安全概述 …… 1
1.1　网络安全简介 …… 1
1.1.1　网络安全的概念 …… 2
1.1.2　网络安全模型 …… 3
1.1.3　计算机安全的分级 …… 4
1.1.4　网络安全的重要性 …… 5
1.2　网络安全现状 …… 5
1.3　网络安全威胁 …… 8
1.3.1　安全攻击 …… 8
1.3.2　基本的威胁 …… 10
1.3.3　主要的可实现的威胁 …… 11
1.3.4　病毒 …… 11
1.4　影响网络安全的因素 …… 12
1.4.1　计算机系统因素 …… 12
1.4.2　操作系统因素 …… 13
1.4.3　网络协议因素 …… 14
1.4.4　人为因素 …… 14
1.5　网络安全技术 …… 15
1.5.1　数据加密与认证 …… 15
1.5.2　防火墙 …… 16
1.5.3　入侵检测 …… 17
1.5.4　访问控制 …… 18
1.5.5　病毒防治 …… 22
复习思考题 …… 22

第 2 章　操作系统安全 …… 23
2.1　操作系统的漏洞 …… 24
2.1.1　系统漏洞的概念 …… 24
2.1.2　漏洞的类型 …… 25
2.1.3　漏洞对网络安全的影响 …… 28
2.2　Windows Server 2003 的安全 …… 29
2.2.1　Windows Server 2003 安全模型 …… 30

2.2.2 Windows Server 2003 安全隐患 ····· 35
2.2.3 Windows Server 2003 安全防范措施 ····· 36
2.3 Linux 网络操作系统的安全 ····· 50
2.3.1 Linux 网络操作系统的基本安全机制 ····· 51
2.3.2 Linux 网络操作系统可能受到的攻击 ····· 52
2.3.3 Linux 网络安全防范策略 ····· 53
2.3.4 加强 Linux 网络服务器的管理 ····· 55
复习思考题 ····· 58
第 3 章 数字加密与认证 ····· 59
3.1 密码学 ····· 60
3.1.1 加密的起源 ····· 60
3.1.2 密码学基本概念 ····· 61
3.1.3 传统加密技术 ····· 62
3.1.4 对称密钥算法 ····· 65
3.1.5 公开密钥算法 ····· 66
3.1.6 加密技术在网络中的应用 ····· 69
3.1.7 密码分析 ····· 70
3.2 密钥管理 ····· 71
3.2.1 密钥的分类和作用 ····· 71
3.2.2 密钥长度 ····· 72
3.2.3 密钥产生技术 ····· 74
3.2.4 密钥的组织结构 ····· 76
3.2.5 密钥分发 ····· 77
3.2.6 密钥的保护 ····· 80
3.3 数字签名与数字证书 ····· 82
3.3.1 电子签名 ····· 82
3.3.2 认证机构(CA) ····· 83
3.3.3 数字签名 ····· 84
3.3.4 公钥基础设施(PKI) ····· 87
3.3.5 数字证书 ····· 89
3.3.6 数字时间戳技术 ····· 93
3.4 认证技术 ····· 93
3.4.1 身份认证的重要性 ····· 94
3.4.2 身份认证的方式 ····· 94
3.4.3 消息认证 ····· 96

3.4.4 认证技术的实际应用 …… 101
3.5 数字证书应用实例 …… 103
3.5.1 获得及安装免费数字证书 …… 103
3.5.2 在 IE 中查看数字证书 …… 104
3.5.3 发送安全邮件 …… 106
3.5.4 检查 Windows 是否为微软正版 …… 112
复习思考题 …… 113

第 4 章 防火墙技术 …… 114
4.1 防火墙的基本概念与分类 …… 115
4.1.1 防火墙的基本概念 …… 115
4.1.2 防火墙的作用 …… 117
4.1.3 防火墙的优缺点 …… 118
4.1.4 防火墙的分类 …… 119
4.2 防火墙技术 …… 121
4.2.1 包过滤技术 …… 121
4.2.2 应用代理技术 …… 124
4.2.3 状态检测技术 …… 126
4.2.4 技术展望 …… 129
4.3 防火墙的体系结构 …… 131
4.3.1 双重宿主主机结构 …… 131
4.3.2 屏蔽主机结构 …… 133
4.3.3 屏蔽子网结构 …… 134
4.3.4 防火墙的组合结构 …… 136
4.4 选择防火墙的注意事项 …… 136
4.4.1 选型防火墙的基本原则 …… 136
4.4.2 选择防火墙的注意事项 …… 137
复习思考题 …… 144

第 5 章 入侵检测系统 …… 145
5.1 入侵检测概述 …… 146
5.1.1 入侵检测概念 …… 146
5.1.2 入侵检测系统组成 …… 146
5.1.3 入侵检测功能 …… 147
5.2 入侵检测系统分类 …… 149
5.2.1 根据数据源分类 …… 149
5.2.2 根据检测原理分类 …… 150

5.2.3 根据体系结构分类 ····· 151
5.2.4 根据工作方式分类 ····· 152
5.2.5 根据系统其他特征分类 ····· 152
5.3 入侵检测技术 ····· 153
5.3.1 误用检测技术 ····· 153
5.3.2 异常检测技术 ····· 155
5.3.3 高级检测技术 ····· 157
5.3.4 入侵诱骗技术 ····· 160
5.3.5 入侵响应技术 ····· 162
5.4 入侵检测体系 ····· 164
5.4.1 入侵检测模型 ····· 164
5.4.2 入侵检测体系结构 ····· 166
5.5 入侵检测系统与协同 ····· 172
5.5.1 数据采集协同 ····· 172
5.5.2 数据分析协同 ····· 173
5.5.3 响应协同 ····· 175
5.6 入侵检测分析 ····· 177
5.6.1 入侵检测特点分析 ····· 177
5.6.2 入侵检测与防火墙 ····· 178
5.6.3 入侵检测系统的缺陷 ····· 179
5.7 入侵检测的发展 ····· 180
5.7.1 入侵检测标准 ····· 180
5.7.2 入侵检测评测 ····· 181
5.7.3 入侵检测发展 ····· 183
复习思考题 ····· 186

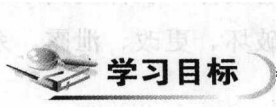
第 6 章 网络病毒的防治技术 ····· 187
6.1 计算机网络病毒的特点及危害 ····· 187
6.1.1 计算机病毒的概念 ····· 188
6.1.2 计算机病毒的特点 ····· 188
6.1.3 计算机病毒的分类 ····· 191
6.1.4 计算机网络病毒的概念 ····· 196
6.1.5 计算机网络病毒的特点 ····· 197
6.1.6 计算机网络病毒的分类 ····· 199
6.1.7 计算机网络病毒的危害 ····· 201
6.2 几种典型病毒的分析 ····· 203

6.2.1 CIH 病毒……203
6.2.2 宏病毒……205
6.2.3 蠕虫病毒……208
6.2.4 木马病毒……211
6.3 计算机病毒的症状……218
6.3.1 病毒发作前的症状……218
6.3.2 病毒发作时的症状……219
6.3.3 病毒发作后的症状……221
6.4 反病毒技术……223
6.4.1 预防病毒技术……224
6.4.2 检测病毒技术……228
6.4.3 杀毒技术……237
6.5 计算机病毒发展的新技术……240
6.5.1 抗分析病毒技术……240
6.5.2 隐蔽性病毒技术……241
6.5.3 多态性病毒技术……241
6.5.4 超级病毒技术……242
6.5.5 插入性病毒技术……242
6.5.6 破坏性感染病毒技术……243
6.5.7 病毒自动生产技术……243
6.5.8 Internet 病毒技术……244
6.6 防杀网络病毒的软件……244
6.6.1 防毒软件……244
6.6.2 反病毒软件……245
6.6.3 瑞星杀毒软件……245
6.6.4 金山毒霸……246
6.6.5 江民杀毒软件……246
复习思考题……246
第 7 章 网络维护……247
7.1 Windows 自带的网络工具……248
7.1.1 Ping 命令……248
7.1.2 Ipconfig/Winipcfg 命令……256
7.1.3 Netstat 命令……258
7.1.4 Tracert 命令……260

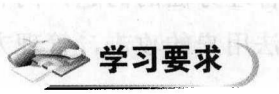
7.2 网络连接设备的维护 …… 261
7.2.1 网卡 …… 261
7.2.2 集线器和交换机 …… 262
7.2.3 路由器 …… 264
7.2.4 网线 …… 265
7.2.5 RJ-45 接头 …… 265
7.3 网络性能优化 …… 266
7.3.1 系统内存优化 …… 266
7.3.2 CPU 的优化 …… 268
7.3.3 硬盘优化 …… 269
7.3.4 网络接口优化 …… 271
7.4 网络故障和排除 …… 272
7.4.1 网络常见故障概述 …… 273
7.4.2 网络故障排除的思路 …… 274
7.4.3 局域网故障与排除 …… 277
7.4.4 Windows 局域网使用过程中的常见故障 …… 288
7.4.5 故障实例及排除方法 …… 292
复习思考题 …… 297
主要参考文献 …… 298

第1章

网络安全概述



系统学习网络安全的概念、网络面临的主要威胁、影响网络安全的因素以及保证网络安全的技术。



- **了解**：网络的安全威胁；影响网络安全的主要因素。
- **掌握**：网络安全的概念；网络安全的基本技术。

随着信息科技的迅速发展，网络已成为全球重要的信息传播工具。而随着因特网的飞速发展，网络安全问题已经越来越受到大家广泛的关注——各种病毒花样繁多、层出不穷；系统、程序、软件的安全漏洞越来越多；黑客们通过不正当手段侵入他人计算机，非法获得信息资料，给正常使用因特网的用户带来不可估量的损失。因此，网络安全越来越引起人们的重视。

1.1 网络安全简介

20世纪90年代中期以来，随着网络技术突飞猛进的发展，特别是Internet的迅猛发展，使各国的信息化进程急剧加快。我国的信息化热潮也随之高涨，信息的应用也从原来的军事、科技、文化和商业渗透到了社会生活的各个领域，在社会生产、生活中的作用日益显著。人们在享受信息化带来的众多好处的同时，也面临着日益突出的信息安全与保密的问题。网络信息安全技术经过近10年来的发展，在信息安全技术的研究上形成了两个完全不同的角度和方向：一个从正面防御考虑，研究加密、鉴别、认证、授权和访问控制等；另一个从反

面攻击考虑，研究漏洞扫描评估、入侵检测、紧急响应和防病毒。

1.1.1 网络安全的概念

网络安全从其本质上来讲就是网络上的信息安全。它涉及的领域相当广泛，这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。下面给出网络安全的一个通用定义：

网络安全就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统能连续可靠正常地运行，网络服务不中断。

广义来说，凡是涉及到网络上信息的保密性、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安全所要研究的领域。

网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两者相互补充，缺一不可。技术方面主要侧重于防范外部非法用户的攻击，管理方面则侧重于内部人为因素的管理。

网络安全要考虑以下几个方面的内容。

1. 网络系统的安全

主要包括以下几方面的问题。

- 网络操作系统的安全性：目前流行的操作系统(UNIX、Windows 98/2000/NT/XP 等)均存在网络安全漏洞。
- 来自外部的安全威胁。
- 来自内部用户的安全威胁。
- 通信协议软件本身缺乏安全性(如 TCP/IP 协议)。
- 计算机病毒感染。
- 应用服务的安全：许多应用服务系统在访问控制及安全通信方面考虑得不周全。

2. 局域网安全

局域网采用广播方式，在同一个广播域中可以侦听到在该局域网上传输的所有信息包，这是一个不安全的因素。

3. Internet 互联安全

非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒等都是在 Internet 上经常遇到的问题。

4. 数据安全

事实上，无论 Internet 还是其他专用网络，都必须注意数据的安全性问题，以保护本单位、本部门的信息资源不会受到外来的侵害。

从根本意义上讲，绝对安全的计算机是根本不存在的，绝对安全的网络也是不可能有的。只有存放在一个无人知晓的密室里，而又不插电的计算机才可以称之为安全。计算机只要投入使用，就或多或少地存在着安全问题，只是程度不同而已。因此，在探讨网络安全的时候，实际上指的是一定程度的网络安全。而到底需要多大的安全性，要依据实际需要及自身能力而定。网络安全性越高，同时也意味着网络管理越复杂。网络的安全性与网络管理便利性是一对矛盾。

1.1.2　网络安全模型

典型的网络安全模型如图 1-1 所示。信息需要从一方通过网络传送到另一方。在传送中居主体地位的双方必须合作以便进行交换。通过通信协议(如 TCP/IP)在两个主体之间可以建立一条逻辑信息通道。

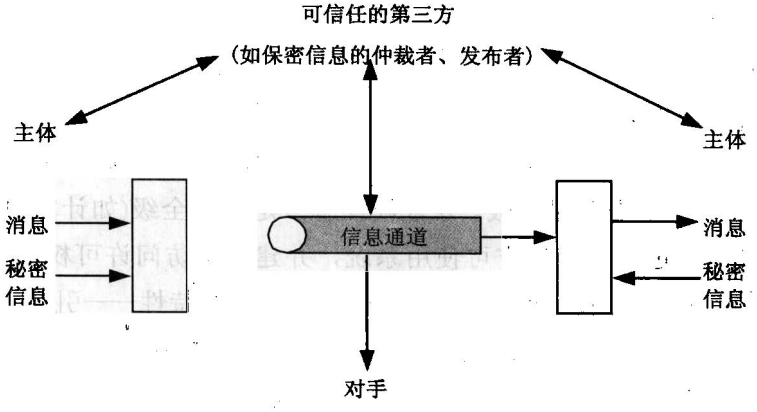


图 1-1　网络安全模型

为防止对手对信息机密性、可靠性等造成破坏，需要保护传送的信息。保证安全性的所有机制包括以下两部分：