



高等院校信息与通信工程系列教材

通信网的安全理论与技术

戴逸民 王培康 陈巍 编著

清华大学出版社

TN915.08

4

高等院校信息与通信工程系列教材

通信网的安全理论与技术

戴逸民 王培康 陈巍 编著

清华大学出版社
北 京

内 容 简 介

本书主要阐述网络可能存在的 13 种信息安全隐患(窃听、修改、重放、伪装、哄骗、渗透、抵赖、拒绝服务、计算机病毒、因特网蠕虫、特洛伊木马、黑客后门、黑客入侵),以及为了克服安全隐患,在网络上实现网上通信、网上无纸办公、网上使用信用卡、网上签订合同、网上购物、电子现金转移时,网络需要解决的 6 类信息安全策略或安全机制(信息的隐蔽、信息的完整性、信息的认证、信息的访问控制、信息的电磁泄露控制、网络的防御策略)和 6 种信息安全技术(信息加密、信息认证、抵御计算机病毒、被动的网络防御、主动的网络防御、数字产品版权保护)。

本书的特点是:内容新颖,概念清晰,实践性强,突出新技术,许多内容,特别是安全可靠的防火墙攻防模型、计算机资源保护模型、主动的网络防御技术、抵御已知攻击能力的分析方法和双层数字水印算法等,都是信息与通信工程领域的基础理论与较为前沿的专业知识,具有广泛的应用前景。

本书可作为高等院校通信工程、信息安全及计算机专业本科生和硕士研究生的教材,也可作为计算机和通信领域专业技术人员的参考书。

版权所有,翻印必究。举报电话:010-62782989 13501256678 13801310933

图书在版编目(CIP)数据

通信网的安全理论与技术/戴逸民,王培康,陈巍编著. —北京:清华大学出版社,2006.7
(高等院校信息与通信工程系列教材)

ISBN 7-302-12624-0

I. 通… II. ①戴… ②王… ③陈… III. 通信网—安全技术—高等学校—教材 IV. TN915.08

中国版本图书馆 CIP 数据核字(2006)第 016208 号

出 版 者:清华大学出版社

<http://www.tup.com.cn>

社 总 机:010-62770175

地 址:北京清华大学学研大厦

邮 编:100084

客户服务:010-62776969

组稿编辑:陈国新

特邀编辑:魏艳春 曾德斌

印 装 者:清华大学印刷厂

发 行 者:新华书店总店北京发行所

开 本:185×260 印张:29.75 字数:701 千字

版 次:2006 年 7 月第 1 版 2006 年 7 月第 1 次印刷

书 号:ISBN 7-302-12624-0/TN·311

印 数:1~3000

定 价:39.00 元

高等院校信息与通信工程系列教材编委会

主 编：陈俊亮

副 主 编：李乐民 张乃通 邬江兴

编 委（排名不分先后）：

王 京 韦 岗 朱近康 朱世华

邬江兴 李乐民 李建东 张乃通

张中兆 张思东 严国萍 刘兴钊

陈俊亮 郑宝玉 范平志 孟洛明

袁东风 程时昕 雷维礼 谢希仁

责任编辑：陈国新

出版说明

信息与通信工程学科是信息科学与技术的重要组成部分。改革开放以来,我国在发展通信系统与信息系统方面取得了长足的进步,形成了巨大的产业与市场,如我国的电话网络规模已占世界首位,同时该领域的一些分支学科出现了为国际认可的技术创新,得到了迅猛的发展。为满足国家对高层次人才的迫切需求,当前国内大量高等学校设有信息与通信工程学科的院系或专业,培养大量的本科生与研究生。为适应学科知识不断更新的发展态势,他们迫切需要内容新颖又符合教改要求的教材和教学参考书。此外,大量的科研人员与工程技术人员也迫切需要学习、了解、掌握信息与通信工程学科领域的基础理论与较为系统的前沿专业知识。为了满足这些读者对高质量图书的渴求,清华大学出版社组织国内信息与通信工程国家级重点学科的教学与科研骨干以及本领域的一些知名学者、学术带头人编写了这套高等院校信息与通信工程系列教材。

该套教材以本科电子信息工程、通信工程专业的专业必修课程教材为主,同时包含一些反映学科发展前沿的本科选修课程教材和研究生教学用书。为了保证教材的出版质量,清华大学出版社不仅约请国内一流专家参与了丛书的选题规划,而且每本书在出版前都组织全国重点高校的骨干教师对作者的编写大纲和书稿进行了认真审核。

祝愿《高等院校信息与通信工程系列教材》为我国培养与造就信息与通信工程领域的高素质科技人才,推动信息科学的发展与进步做出贡献。

北京邮电大学

陈俊亮

前 言

自从 1956 年第一个计算机网络建立以来,网络技术得到了极其迅速的发展,使我们的生活方式和工作方式发生了巨大变化。这些新的变化主要包括网上通信、网上无纸办公、网上使用信用卡、网上签订合同、网上购物、电子现金转移等。

因特网核心协议(TCP/IP)是按照自由开放和彼此信任的群体使用来设计的,在当前的现实环境下却表现出内在缺陷。它们虽然能很好地完成互联层(IP 层)和传输层的功能,但也存在不少可被攻击者利用来进行攻击的“漏洞”。

本书概述网络可能存在的 13 种信息安全隐患和在网络上实现网上通信、网上无纸办公、网上使用信用卡、网上签订合同、网上购物、电子现金转移时,为了克服安全隐患网络需要解决的 6 类信息安全策略或安全机制和 6 种信息安全技术。

(1) 网络可能存在的 13 种信息安全隐患是:窃听、修改、重放、伪装、哄骗、渗透、抵赖、拒绝服务、计算机病毒、因特网蠕虫、特洛伊木马、黑客后门、黑客入侵。

(2) 网络需要解决的 6 类信息安全策略或安全机制是:信息的隐蔽、信息的完整性、信息的认证、信息的访问控制、信息的电磁泄露控制、网络的防御策略。

(3) 网络常用的 6 种信息安全技术是:信息加密、信息认证、抵御计算机病毒、被动的网络防御、主动的网络防御、数字产品版权保护。

本书是作者在中国科学技术大学研讨班(Seminar)课程——“通信网的安全理论与技术”4 年的教学实践的基础上编写而成。

本书可作为高等院校通信工程、信息安全及计算机专业本科生和硕士研究生的教材,也可作为计算机和通信领域专业技术人员的参考书。

全书分为 11 章,下面概括介绍每章的内容。

第 1 章扼要介绍网络的组网原理及可能存在的 13 种信息安全隐患。

第 2 章从信息安全原理的层次结构、物理概念、数学方法、实际应用和实现技巧等角度阐述 6 类信息安全对策或安全机制。

第 3 章给出 5 个信息加密范例和 7 个密文破译范例,以此说明信息加密与密文破译的重要概念和通用原理。

第 4 章概述密钥流产生原理、技术和实例。

第 5 章以高级加密标准 AES 为例,概述分组密码设计原理、技术和抵御已知攻击的强度。

第 6 章概述双密钥思想的优势和缺陷,指出弥补缺陷的途径;简介广义数字签名的概念和算法。

第 7 章阐述通信网安全认证协议、网络安全认证协议和用于认证的典型算法。

第 8 章简介网络分层结构、控制报文协议(ICMP)和 TCP 连接规程,分别叙述它们的漏洞和对策,最后构造一个安全可靠的防火墙攻防模型,并概括叙述网络防御技术的发展方向。

第 9 章简介计算机安全等级、操作系统发展与恶意代码的演化关系,分别叙述 4 种恶意代码的入侵机制和防御措施,最后构造一个安全可靠的计算机资源保护模型。

第 10 章从密码算法的选择、操作模式的选择、使用环境的考虑、不同品牌安全设备的互连等方面,叙述网上安全通信系统设计的指导思想,并给出 3 个实例。

第 11 章简介空间和频谱数字水印嵌入原理及提取技术,分别叙述它们的优势和漏洞,最后构造一个安全可靠的双层数字水印算法,适用于“可信赖的”数码相机和摄像机等。

本书的第 1 章、第 2 章(2.1~2.3 节)、第 7 章由王培康编写,第 2 章(2.4~2.7 节)、第 3 章~第 6 章、第 8 章~第 10 章由戴逸民编写,第 11 章由陈巍编写。张曦、杨婧和储元麟参与 11.5 节“用于数码相机的双层数字水印算法”的实验工作。戴逸民负责全书的统稿。

作者于合肥中国科学技术大学

2005 年 10 月

daiym@ustc.edu.cn

目 录

第 1 章 通信网面临的安全威胁	1
1.1 因特网的安全隐患与安全处理方法	1
1.1.1 资源保护	1
1.1.2 安全威胁	2
1.1.3 安全系统特征	4
1.1.4 安全策略	5
1.1.5 安全系统密级层次划分法	6
1.2 电子邮件及其安全	7
1.2.1 电子邮件的优点	7
1.2.2 电子邮件服务的组成	7
1.2.3 电子邮件系统所面临的主要安全威胁	8
1.3 局域网的安全	10
1.3.1 基于客户机/服务器应用的安全问题	10
1.3.2 商务旅行中笔记本式计算机的安全问题	12
1.4 公众交换电话网络和卫星通信的安全	12
1.4.1 公众交换电话网络的优点	12
1.4.2 公众交换电话网的主要安全威胁	12
1.4.3 保密电话呼叫协议	13
1.4.4 卫星通信	14
1.5 无线通信网的安全	17
1.5.1 无线通信网的主要安全威胁	17
1.5.2 移动通信网的通信体制	18
1.5.3 移动通信网的组成	20
1.5.4 移动通信网的现有安全措施	22
1.5.5 移动通信网所面临的主要安全威胁	24
第 2 章 通信网信息安全理论概述	27
2.1 安全原理简介	27
2.1.1 信息安全原理的层次结构	27
2.1.2 当前使用的安全标准	28
2.1.3 密码术的强度和类型	29

2.1.4 实用的密码术处理	30
2.2 用户认证	31
2.2.1 认证方法概述	31
2.2.2 口令认证	31
2.2.3 身份认证	36
2.2.4 生物学认证	40
2.3 访问控制	41
2.3.1 访问控制概述	41
2.3.2 访问控制列表	41
2.3.3 执行控制列表	41
2.3.4 访问控制策略	42
2.4 信息的隐蔽原理	42
2.4.1 消息的信息量和冗余度	42
2.4.2 信息加密和信息隐藏技术	43
2.4.3 密码算法、密钥和安全协议	46
2.4.4 对称算法	52
2.4.5 非对称算法	59
2.4.6 对称算法与非对称算法的性能比较	63
2.5 消息的完整性原理	64
2.5.1 消息完整性原理的作用	64
2.5.2 消息完整性威胁的解决机制	64
2.5.3 数字签名与认证的关系	68
2.5.4 数字签名算法的应用	68
2.6 消息的认证原理	70
2.6.1 语音消息认证	70
2.6.2 时间认证	71
2.6.3 文本/数据消息认证	71
2.7 消息的电磁泄露原理	73
2.7.1 危及安全辐射的定义	73
2.7.2 危及安全辐射的产生机理	74
2.7.3 机密信息如何通过电磁辐射泄露	74
2.7.4 电子耦合	76
2.7.5 电子设备结构设计中的预防措施	77
第3章 信息加密和密文破译范例	80
3.1 凯撒密码及其破译	80
3.1.1 加密范例一:凯撒密码和自然序标准单表密码	80
3.1.2 破译范例一:凯撒密码和自然序标准单表密码的破译	81

3.2	多表密码及其破译	85
3.2.1	加密范例二:多表密码	85
3.2.2	破译范例二:多表密码的破译	89
3.3	置换密码及其破译	99
3.3.1	置换密码的常用形式	99
3.3.2	加密范例三:列置换密码	100
3.3.3	破译范例三:列置换密码的破译	102
3.4	乘积密码及其破译	104
3.4.1	加密范例四:乘积密码	105
3.4.2	破译范例四:乘积密码的破译	106
3.5	比特级加密及其破译	113
3.5.1	加密范例五:比特级加密	113
3.5.2	破译范例五:综合法破译	114
3.5.3	破译范例六:相关法破译	117
3.5.4	破译范例七:字典法破译计算机用户口令	121
第4章	密钥流产生技术	122
4.1	流密码体制概述	122
4.1.1	一次一密密带体制的工作原理	122
4.1.2	一次一密密带体制的安全性	123
4.1.3	同步序列密码原理	124
4.1.4	真随机序列的三大特征	125
4.2	流密码设计方法	126
4.2.1	系统理论法	127
4.2.2	信息理论法	129
4.2.3	复杂性理论法	129
4.2.4	随机法	130
4.3	线性反馈移位寄存器	131
4.3.1	反馈移位寄存器	131
4.3.2	线性反馈移位寄存器	132
4.3.3	线性反馈移位寄存器的特点	132
4.4	流密码安全性分析	136
4.4.1	线性复杂性	136
4.4.2	相关免疫	137
4.5	密钥流产生器的构造	137
4.5.1	基于线性移位寄存器设计密钥流产生器	137
4.5.2	基于置换盒设计密钥流产生器	140

第 5 章 高级加密标准	142
5.1 概述	142
5.1.1 AES 的产生背景	142
5.1.2 AES 的优势和限制	143
5.2 定义	144
5.2.1 术语和缩写词表	144
5.2.2 算法参数、符号和函数	144
5.3 符号和约定	145
5.3.1 输入和输出	145
5.3.2 字节	146
5.3.3 字节的数组	146
5.3.4 状态	147
5.3.5 作为列数组的状态	147
5.4 数学预备知识	148
5.4.1 加法	148
5.4.2 乘法	148
5.4.3 使用有限域 $GF(2^8)$ 元素系数的多项式	150
5.5 算法描述	151
5.5.1 密码	152
5.5.2 密钥扩充	161
5.5.3 逆向密码	168
5.6 实现问题	178
5.6.1 密钥长度的需求	178
5.6.2 密钥约束	179
5.6.3 密钥长度、分组大小和循环次数的参数化	179
5.6.4 关于不同平台的执行建议	179
5.7 AES 加密算法设计的基本原理	179
5.7.1 设计的基本标准	179
5.7.2 约简多项式 $m(x)$	180
5.7.3 用于字节置换的 S 盒	180
5.7.4 列字节混合变换	181
5.7.5 行字节移位的偏移量	181
5.7.6 密钥扩充	181
5.7.7 循环数目	182
5.8 AES 加密算法抵御已知攻击的强度	183
5.8.1 DES 类型的对称特性和弱密钥	183
5.8.2 差分和线性密码分析	183

5.8.3	截尾差分	187
5.8.4	平方攻击	187
5.8.5	内插攻击	190
5.8.6	相对密钥攻击	190
5.8.7	IDEA 类型的弱密钥	190
5.9	安全目标和预期的强度	190
5.9.1	安全目标	190
5.9.2	预期的强度	192
5.10	AES 的其他应用	192
第 6 章	公开密钥加密机制和数字签名算法	194
6.1	公开密钥加密机制的优势和缺陷	194
6.1.1	公开密钥加密解密过程	194
6.1.2	公开密钥算法的创新性	195
6.1.3	公开密钥算法的实现原理	195
6.1.4	公开密钥的安全性	199
6.1.5	使用概率加密的公开密钥	200
6.1.6	提高公开密钥算法运算速度的途径	201
6.2	RSA 算法	203
6.2.1	RSA 算法组成	203
6.2.2	RSA 算法实例	204
6.2.3	RSA 算法速度	205
6.2.4	RSA 算法的安全性	205
6.3	公开密钥数字签名原理	206
6.3.1	广义的数字签名的算法	206
6.3.2	数字签名的特性	206
6.3.3	数字签名的实施协议	207
6.4	公开密钥数字签名算法	209
6.4.1	DSA 数字签名算法	209
6.4.2	零知识证明的数字签名算法	211
6.5	Diffie Hellman 密钥交换算法	212
6.5.1	数学背景	213
6.5.2	算法协议	213
6.5.3	算法组成	214
6.5.4	算法的数学解释	215
6.5.5	算法特点	215

第 7 章 通信网认证协议和认证算法	218
7.1 通信安全认证协议	218
7.1.1 基于对称密钥的相互认证和密钥交换	219
7.1.2 能阻止重放攻击的相互认证和密钥交换	221
7.1.3 基于对称密钥和可信赖的第三方的通信安全认证	224
7.1.4 分布式认证安全服务	227
7.1.5 基于公开密钥的相互认证和密钥交换	228
7.2 网络安全认证协议	232
7.2.1 基于客户机/服务器模式的网络安全认证	232
7.2.2 基于对等网络模式的网络安全认证	233
7.2.3 基于 TCP/IP 通信协议的网络安全认证	233
7.3 认证算法	238
7.3.1 MD5 单向散列函数的算法	238
7.3.2 安全的散列算法	241
7.3.3 消息认证码算法	243
7.3.4 基于散列值的消息认证码	243
7.3.5 零知识证明的认证算法	244
第 8 章 网络攻击和防御原理	247
8.1 网络分层结构和安全性简介	247
8.1.1 概述	247
8.1.2 网络接入层	248
8.1.3 互联网层	249
8.1.4 传输层	250
8.1.5 应用层	252
8.1.6 TCP/IP 信息包	253
8.2 基于控制报文协议的网络攻击和防御	255
8.2.1 控制报文协议简要介绍	255
8.2.2 假冒源 IP 地址和对路由信息进行欺诈和邻机嗅探	257
8.2.3 邻机侦听	268
8.2.4 ICMP 诊断、ICMP 查询和 ICMP 隧道的远程控制攻击	270
8.2.5 带宽耗尽攻击	274
8.3 基于 TCP 连接规程的网络攻击和防御	276
8.3.1 端口重定向	276
8.3.2 TCP 同步淹没和 IP 地址伪装攻击	280
8.3.3 TCP 连接规程与端口扫描	286
8.3.4 TCP 数据传输与 TCP 会话劫持	291

8.4	基于 TCP 与 ICMP 分组组合的网络攻击和防御	292
8.4.1	网络的路径跟踪原理	292
8.4.2	分布式拒绝服务攻击	299
8.5	基于网络防御设备的网络攻防模型	300
8.5.1	防火墙防御机制简介	301
8.5.2	简化的网络攻防模型	307
8.5.3	改进的网络攻防模型	310
8.5.4	比较完整的网络攻防模型	312
8.5.5	完整的网络攻防模型	316
8.5.6	无线局域网攻防模型	316
8.6	网络防御技术的新进展	318
8.6.1	入侵检测系统	318
8.6.2	入侵防护系统	321
8.6.3	网络异常流量与系统性能的实时监控技术	323
8.6.4	数字免疫原理	326
第 9 章	计算机安全	328
9.1	计算机安全概述	328
9.1.1	计算机安全等级	328
9.1.2	恶意代码的演化和传播趋势	329
9.1.3	恶意代码类型	330
9.2	计算机病毒	331
9.2.1	病毒的传染机制	331
9.2.2	病毒蔓延和传播的途径	332
9.2.3	抗病毒程序的主要检测算法	334
9.2.4	加密病毒的主要特征及其检测算法	336
9.2.5	多形病毒的主要特征及其检测困难	338
9.2.6	多形病毒检测方案	339
9.3	因特网“蠕虫”	342
9.3.1	因特网的第一次“蠕虫”危机和后果	342
9.3.2	“蠕虫”传染机制的基础知识	343
9.3.3	“蠕虫”传染机制的定性描述	350
9.3.4	“蠕虫”传染机制的详细描述	351
9.3.5	“蠕虫”的检测和防御	355
9.4	特洛伊木马	358
9.4.1	特洛伊木马的特点	358
9.4.2	特洛伊木马的发展历史	359
9.4.3	网络传播型特洛伊木马的工作机制	360

9.4.4	特洛伊木马的客户端与服务端通信如何隐藏	360
9.4.5	特洛伊木马的分类	362
9.4.6	特洛伊木马的检测和防御	367
9.5	黑客后门	370
9.5.1	黑客后门的特点	370
9.5.2	黑客创建后门的主流机制	370
9.5.3	发现黑客后门的方法	371
9.6	保护资源	373
9.6.1	保护资源和服务的方法	373
9.6.2	操作系统安全	374
9.6.3	保护 TCP/IP 服务	375
9.6.4	公共网关接口脚本	376
第 10 章	网上安全通信系统设计举例	378
10.1	密码算法的选择	378
10.1.1	公开密钥和对称密钥算法	378
10.1.2	流密码和分组密码算法	379
10.1.3	密钥一致协议和数字信封算法	380
10.2	密码操作模式的选择	380
10.2.1	流密码的操作模式	380
10.2.2	分组密码的操作模式	384
10.2.3	密码操作模式性能比较	392
10.3	密码使用工作环境的选择	393
10.3.1	链接加密和端到端加密	393
10.3.2	文件水平加密和驱动器水平加密	396
10.3.3	硬件加密和软件加密	397
10.3.4	压缩、编码和加密	398
10.4	不同品牌安全设备的互连	398
10.5	安全性考虑	399
10.5.1	处理秘密密钥	399
10.5.2	暂时缓冲器	400
10.5.3	伪随机数和种子的产生	400
10.5.4	选择口令	400
10.5.5	初始化矢量和掺杂	400
10.5.6	密钥大小	401
10.6	PEM 电子邮件安全保密系统	402
10.6.1	PEM 文件	403
10.6.2	证书管理	403

10.6.3	PEM 消息格式	404
10.6.4	PEM 的安全性	407
10.7	通用电子付款系统	407
10.7.1	smart 卡	407
10.7.2	通用电子付款系统	407
10.8	网上安全通信系统	409
10.8.1	发送过程	409
10.8.2	接收过程	410
10.8.3	系统安全性分析	410
第 11 章	数字产品版权保护原理	412
11.1	版权保护与数字水印	412
11.1.1	数字水印的重要性和用途	412
11.1.2	数字水印的基本性质	413
11.2	空间数字水印原理	414
11.2.1	空间数字水印的嵌入原理	414
11.2.2	空间数字水印的提取原理	414
11.2.3	空间数字水印的检测原理	415
11.2.4	空间数字水印性能实验分析	416
11.3	频谱数字水印原理	419
11.3.1	频谱数字水印概述	419
11.3.2	频谱数字水印的嵌入原理	419
11.3.3	频谱数字水印的提取原理	420
11.3.4	频谱数字水印的检测原理	421
11.3.5	频谱数字水印性能的实验分析	422
11.4	用于数码相机的双层数字水印算法	423
11.4.1	现有数字水印算法的性能和不足	423
11.4.2	硬件实现的双层水印算法的基本要求	424
11.4.3	第一层水印:版权保护	426
11.4.4	第二层水印:完整性和可信性鉴定	431
11.4.5	双层水印算法的总体结构	436
11.4.6	算法在 DSP 硬件平台上的实现	439
11.4.7	双层数字水印算法的实现效果	442
11.4.8	算法的改进和展望	450
参考文献		452

第 1 章 通信网面临的安全威胁

首先简介因特网的安全目标(资源保护)、安全威胁、安全系统特征、安全策略和安全系统密级层次划分方法,然后仔细分析因特网两项应用服务所面临的安全威胁,并扼要介绍其他通信网的组网工作原理和面临的安全威胁。

1.1 因特网的安全隐患与安全处理方法

越来越多的单位、团体、公司开始依赖因特网完成办公、管理、商务、通信和协作。与过去相比,现在敏感信息的完整性和在线通信日臻重要。对病毒和黑客作出反应是任何网络管理工作的一个主要职责。本节将简介因特网的安全隐患与安全处理方法。

1.1.1 资源保护

在计算机网络中,安全可以定义为由网络管理员进行的一系列处理,以保证信息只在经认证的用户之间共享。当设计和执行一项安全计划时,首先需要了解所要保护的资源。

1. 保护资源的重要性

因特网是一个开放的网络,因此,内置的保护信息的能力是非常差的。从安全观点看,因特网天生就不安全。保护敏感的数据,只允许经过授权的人员使用它,这是使用因特网所面临的挑战。

2. 用户或单位需要保护的资源

用户或单位需要保护的资源,由以下四部分组成,如图 1-1 所示。

(1) 本地资源

基于口令保护的屏幕保护程序能阻止侦听。当从因特网下载任何文件时,需要每一个使用者使用病毒检验程序,并观察有关警告。

(2) 网络资源

用于整个单位的主要通信媒体是网络和它的资源。如果一个黑客得到某个网络访问和控制权,那么他便能访问该单位的大部分网络数据。

(3) 数据库和信息资源

任何单位的主要资源是组织起来的或分散的信息。黑客的最终目标是发现这些信