

<<网络安全>>

图书基本信息

书名：<<网络安全>>

13位ISBN编号：9787302105862

10位ISBN编号：7302105863

出版时间：2005-6

出版时间：清华大学出版社

作者：刘建伟/王育民编

页数：578

字数：781000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<网络安全>>

内容概要

全书共分3篇15章。

第1篇为网络安全基础，共3章，主要讨论了网络安全的基础知识，并从网络协议安全性的角度出发，阐述了当今计算机网络中存在的安全威胁；第2篇为保密学基础，共5章，较详细地讨论了网络安全中涉及的各种密码技术；第3篇为网络安全实践，共7章，主要介绍了网络安全实践中一些比较重要的产品及其技术应用。

本书内容丰富，概念清楚，语言精练。

在网络安全基本知识和保密学理论方面，力求深入浅出，通俗易懂；在网络安全产品方面，力求理论与实践相结合，具有很强的实用性。

特别是每章的后面提供了很多习题，在书末也提供了大量的参考文献，便于有兴趣的读者继续深入地学习有关内容。

本书可作为高等院校信息安全、通信、计算机等专业的研究生和本科生教材，也可以作为网络安全工程师、网络管理员和计算机用户的参考用书，或作为网络安全培训教材。

作者简介

刘建伟，山东大学学士、硕士、西安电子科技大学博士，山东大学、中国海洋大学、北京航空航天大学兼职教授，中国电子学会高级会员。

曾任海信集团技术中心副主任等职务，现任北京海信数码科技有限公司的总经理。

长期从事通信、信息安全的教学和科研工作，获海信集团“科技

<<网络安全>>

书籍目录

第1章 网络安全概论	1.1 对网络安全的需求	1.1.1 网络安全发展态势	1.1.2 敏感信息对安全的需求
	1.1.3 网络应用对安全的需求	1.2 安全威胁与防护措施	1.2.1 基本概念
	1.2.2 安全威胁的来源	1.2.3 安全防护措施	1.3 网络安全策略
	1.3.1 授权	1.3.2 访问控制策略	1.3.3 责任
	1.4 安全攻击的分类	1.4.1 被动攻击	1.4.2 主动攻击
	1.5 网络攻击的常见形式	1.5.1 口令窃取	1.5.2 欺骗攻击
	1.5.3 缺陷和后门攻击	1.5.4 认证失效	1.5.5 协议缺陷
	1.5.6 信息泄露	1.5.7 指数攻击——病毒和蠕虫	1.5.8 拒绝服务攻击
	1.6 开放系统互联安全体系结构	1.6.1 安全服务	1.6.2 安全机制
	1.6.3 安全服务与安全机制的关系	1.6.4 在OSI层中的服务配置	习题第2章 低层协议的安全性
	2.1 基本协议	2.1.1 IP	2.1.2 ARP
	2.1.3 TCP	2.1.4 SCTP	2.1.5 UDP
	2.1.6 ICMP	2.2 地址和域名管理	2.2.1 路由协议
	2.2.2 域名系统	2.2.3 BOOTP和DHCP	2.3 IPv6
	2.3.1 IPv6简介	2.3.2 IPv6地址	2.3.3 IPv6地址配置
	2.3.4 邻居发现协议	2.3.5 移动IPv6	2.3.6 IPv6的安全性
	2.4 网络地址转换器	2.5 无线网的安全	习题第3章 高层协议的安全性
	3.1 消息发送	3.1.1 SMTP	3.1.2 MIME
	3.1.3 POP3	3.1.4 IMAP4	3.1.5 即时消息
	3.2 互联网电话	3.2.1 H.323	3.2.2 SIP
	3.3 基于RPC的协议	3.3.1 RPC	与Rpcbnd
	3.3.2 NIS	3.3.3 NFS	3.3.4 AFS
	3.4 TFTP和FTP	3.4.1 TFTP	3.4.2 FTP
	3.4.3 SMB协议	3.5 远程登录协议	3.5.1 Telnet
	3.5.2 “r”命令	3.5.3 SSH	3.6 SNMP
	3.7 NTP	3.8 信息服务	3.8.1 Finger——用户查询服务
	3.8.2 Whois——数据库查询服务	3.8.3 LDAP	3.8.4 WWW服务
	3.8.5 NNTP——网络消息传输协议	3.8.6 多播及MBone	3.9 专有协议
	3.9.1 RealAudio	3.9.2 Oracle的SQL*Net	3.9.3 其他专用服务
	3.10 对等实体联网	3.11 X11	视窗系统
	3.12 其他小的服务	习题第4章 单(私)钥加密体制	4.1 密码体制的定义
	4.2 古典密码	4.2.1 代换密码	4.2.2 换位密码
	4.2.3 古典密码的安全性	4.3 流密码的基本概念	4.3.1 流密码框图和分类
	4.3.2 密钥流生成器的结构和分类	4.3.3 密钥流的局部统计检验	4.3.4 随机数与密钥流
	4.4 快速软、硬件实现的流密码算法	4.4.1 A5	4.4.2 加法流密码生成器
	4.4.3 RC4	4.4.4 SEAL	4.4.5 PKZIP
	4.5 分组密码概述	4.6 数据加密标准	4.6.1 DES介绍
	4.6.2 DES的核心作用：消息的随机非线性分布	4.6.3 DES的安全性	4.7 高级加密标准
	4.7.1 Rijndael密码概述	4.7.2 Rijndael密码的内部函数	4.7.3 Rijndael内部函数的功能小结
	4.7.4 AES对应用密码学的积极影响	4.8 其他重要的分组密码算法	4.8.1 IDEA
	4.8.2 SAFER K ⁶⁴	4.8.3 RC5	4.9 分组密码的工作模式
	4.9.1 电码本模式	4.9.2 密码分组链接模式	4.9.3 密码反馈模式
	4.9.4 输出反馈模式	4.9.5 计数器模式	习题第5章 双(公)钥密码体制
	5.1 双钥密码体制的基本概念	5.1.1 单向函数	5.1.2 陷门单向函数
	5.1.3 公钥系统	5.1.4 用于构造双钥密码的单向函数	5.2 RSA密码体制
	5.2.1 体制	5.2.2 RSA的安全性	5.2.3 RSA的参数选择
	5.2.4 RSA体制实用中的其他问题	5.2.5 RSA的实现	5.2.6 RSA体制的推广
	5.3 背包密码体制	5.3.1 背包问题	5.3.2 简单背包
	5.3.3 Merkle-Hellman陷门背包	5.3.4 M-H体制的安全性	5.3.5 背包体制的缺陷
	5.3.6 其他背包体制	5.4 Rabin密码体制	5.4.1 Rabin体制
	5.4.2 Williams体制	5.5 ElGamal密码体制	5.5.1 方案
	5.5.2 加密	5.5.3 安全性	5.6 椭圆曲线密码体制
	5.6.1 实数域上的椭圆曲线	5.6.2 有限域Z _p 上的椭圆曲线	5.6.3 GF(2 ^m)上的椭圆曲线
	5.6.4 椭圆曲线密码	5.6.5 椭圆曲线的安全性	5.6.6 ECC的实现
	5.6.7 当前ECC的标准化工作	5.6.8 椭圆曲线上的RSA密码体制	5.6.9 用圆锥曲线构造双钥密码体制
	5.7 其他双钥密码体制	5.7.1 McEliece密码体制	5.7.2 LUC密码体制
	5.7.3 有限自动机体制	5.7.4 概率加密体制	5.7.5 秘密共享密码体制
	5.7.6 多密钥公钥密码体制	5.8 公钥密码体制的分析	习题第6章 消息认证与杂凑函数
	6.1 认证函数	6.1.1 消息加密	6.1.2 消息认证码
	6.1.3 杂凑函数	6.1.4 杂凑函数的性质	6.2 消息认证码
	6.2.1 对MAC的要求	6.2.2 基于密钥杂凑函数的MAC	6.2.3 基于分组加密算法的MAC
	6.3 杂凑函数	6.3.1 单向杂凑函数	6.3.2 杂凑函数在密码学中的应用
	6.3.3 分组迭代单向杂凑算法的层次结构	6.3.4 迭代杂凑函数的构造方法	6.3.5 基本迭代函数的选择
	6.3.6 应用杂凑函数的基本方式	6.4 MD-4和MD-5	6.4.1 算法步骤
	6.4.2 MD-5的安全性	6.4.3 MD-5的实现	6.4.4 MD-4与MD-5算法差别
	6.4.5 MD-2和MD-3	6.5 安全杂凑算法	6.5.1 算法
	6.5.2 SHA的安全性		

<<网络安全>>

6.5.3 SHA与MD-4, MD-5的比较 6.6 其他杂凑算法 6.6.1 RIPEMD?160 6.6.2 SNEFRU算法
6.6.3 GOST杂凑算法 6.6.4 HAVAL算法 6.6.5 RIPE?MAC 6.6.6 其他 6.7 HMAC 习题第7
章 数字签名 7.1 数字签名基本概念 7.2 RSA签名体制 7.3 Rabin签名体制 7.4 ElGamal签名体制 7.5
Schnorr签名体制 7.6 DSS签名标准 7.6.1 概况 7.6.2 签名和验证签名的基本框图 7.6.3 算法描
述 7.6.4 DSS签名、验证框图 7.6.5 公众反应 7.6.6 实现速度 7.7 GOST签名标准 7.8 ESIGN
签名体制 7.9 Okamoto签名体制 7.10 OSS签名体制 7.11 其他数字签名体制 7.11.1 离散对数签名
体制 7.11.2 不可否认签名 7.11.3 防失败签名 7.11.4 盲签名 7.11.5 群签名 7.11.6 代理
签名 7.11.7 指定证实人的签名 7.11.8 一次性数字签名 7.11.9 双有理签名方案 7.11.10 数
字签名的应用 习题第8章 密码协议 8.1 协议的基本概念 8.1.1 仲裁协议 8.1.2 裁决协议
8.1.3 自动执行协议 8.2 安全协议分类及基本密码协议 8.2.1 密钥建立协议 8.2.2 认证建立协
议 8.2.3 认证的密钥建立协议 8.3 秘密分拆协议 8.4 秘密广播协议和会议密钥分配 8.4.1 秘密
广播协议 8.4.2 会议密钥分配协议 8.4.3 Tatebayashi?Matsuzaki?Newman协议 8.5 密码协议的安全
性 8.5.1 对协议的攻击 8.5.2 密码协议的安全性分析习题第9章 PKI与PMI 9.1 PKI的组成
9.1.1 实施PKI服务的实体 9.1.2 认证中心 9.1.3 注册中心 9.2 证书 9.2.1 X.509证书 9.2.2
证书扩展项 9.3 属性证书和漫游证书 9.3.1 属性证书 9.3.2 漫游证书 9.4 PKI/CA认证系统实例
9.5 PMI介绍 9.5.1 PMI概况 9.5.2 权限管理基础设施 9.5.3 属性权威 9.5.4 权限管理
9.5.5 访问控制框架 9.5.6 策略规则 9.5.7 基于PMI建立安全应用 习题第10章 网络加密与密钥
管理 10.1 网络加密的方式及实现 10.2 硬件加密、软件加密及有关问题 10.2.1 硬件加密的优点
10.2.2 硬件种类 10.2.3 软件加密 10.2.4 存储数据加密的特点 10.2.5 文件删除 10.3 密钥管
理基本概念 10.3.1 密钥管理 10.3.2 密钥的种类 10.4 密钥的长度与安全性 10.4.1 密钥必须
足够长 10.4.2 密钥长度与穷举破译时间和成本估计 10.4.3 软件攻击 10.4.4 密钥多长合适
10.4.5 双钥体制的密钥长度 10.5 密钥生成 10.5.1 选择密钥方式不当会影响安全性 10.5.2 好
的密钥 10.5.3 不同等级的密钥产生的方式不同 10.5.4 双钥体制下的密钥生成 10.6 密钥分配
10.6.1 基本方法 10.6.2 密钥分配的基本工具 10.6.3 密钥分配系统的基本模式 10.6.4 TTP
10.6.5 协议的选用 10.6.6 密钥注入 10.7 密钥的证实 10.7.1 单钥证书 10.7.2 公钥的证实技
术 10.7.3 公钥认证树 10.7.4 公钥证书 10.7.5 基于身份的公钥系统 10.7.6 隐式证实公钥
10.8 密钥的保护、存储与备份 10.8.1 密钥的保护 10.8.2 密钥的存储 10.8.3 密钥的备份
10.9 密钥的泄露、吊销、过期与销毁 10.9.1 泄露与吊销 10.9.2 密钥的有效期 10.9.3 密钥
销毁 10.10 密钥控制 10.11 多个管区的密钥管理 10.12 密钥托管和密钥恢复 10.12.1 密钥托管体
制的基本组成 10.12.2 密钥托管体制实例——EES 10.12.3 其他密钥托管体制 10.13 密钥管理系
统 习题第11章 无线网络安全 11.1 无线蜂窝网络技术 11.1.1 无线传输系统 11.1.2 高级移动电
话系统 11.1.3 时分多址 11.1.4 全球移动通信系统 11.1.5 蜂窝式数字分组数据 11.1.6 个人
数字蜂窝 11.1.7 码分多址 11.1.8 第2.5代技术 11.1.9 第3代技术 11.2 无线数据网络技术
11.2.1 扩谱技术 11.2.2 正交频分复用 11.2.3 IEEE制定的无线局域网标准 11.2.4 802.11无线
网络的工作模式 11.2.5 IEEE制定的无线城域网标准 11.2.6 蓝牙 11.2.7 HomeRF技术
11.2.8 无线应用协议 11.3 无线蜂窝网络的安全性 11.3.1 GSM安全性分析 11.3.2 CDMA的安
全性分析 11.3.3 第3代移动通信系统的安全性分析 11.4 无线数据网络的安全性 11.4.1 有线同等
保密协议 11.4.2 802.1x协议介绍 11.4.3 802.11i标准介绍 11.4.4 802.16标准的安全性 11.4.5
WAP协议的安全性 11.5 无线网络面临的安全威胁 11.6 针对安全威胁的解决方案 11.6.1 采用安全
策略 11.6.2 用户安全教育 11.6.3 采用802.1x认证协议 11.6.4 MAC地址过滤 11.6.5 SSID问
题解决方案 11.6.6 天线的选择 11.6.7 VLAN和防火墙的使用 11.6.8 使用RADIUS认证服务器
11.6.9 虚拟专用网 11.6.10 WEP使用动态生成密钥 11.6.11 利用入侵检测系统监测网络
11.6.12 采用安全的路由协议习题第12章 防火墙原理与设计 12.1 防火墙概述 12.2 防火墙的类型和
结构 12.2.1 防火墙分类 12.2.2 网络地址翻译(NAT) 12.3 静态包过滤器 12.3.1 工作原理
12.3.2 设计与实现 12.3.3 静态包过滤器的优缺点 12.4 电路级网关 12.4.1 工作原理
12.4.2 电路级网关的优缺点 12.5 应用层网关 12.5.1 工作原理 12.5.2 应用网关的优缺点 12.6
动态包过滤防火墙 12.6.1 动态包过滤防火墙原理 12.6.2 设计实现 12.6.3 动态包过滤防火墙

<<网络安全>>

的优缺点 12.7 状态检测防火墙 12.7.1 工作原理 12.7.2 设计与实现 12.7.3 状态检测防火墙
 的优缺点 12.8 切换代理 (Cutoff Proxy) 12.8.1 工作原理 12.8.2 设计与实现 12.8.3 切换代
 理的优缺点 12.9 空气隙防火墙 (Air Gap) 12.9.1 工作原理 12.9.2 空气隙防火墙的优缺点
 12.10 分布式防火墙 12.10.1 工作原理 12.10.2 分布式防火墙的优缺点 12.11 关于防火墙其他
 问题的思考 12.11.1 硬件化 12.11.2 多功能化 12.11.3 安全性 习题第13章 入侵检测系统
 13.1 IDS的概述 13.1.1 IDS的历史 13.1.2 IDS的分类 13.1.3 IDS的作用 13.1.4 IDS的任务
 13.1.5 IDS的主要功能 13.1.6 IDS的评价标准 13.1.7 IDS的典型部署 13.2 IDS的设计
 13.2.1 CIDF的模型 13.2.2 NIDS的设计 13.2.3 NIDS的关键技术 13.2.4 HIDS的设计
 13.2.5 HIDS的关键技术 13.2.6 控制台的设计 13.2.7 自身安全设计 13.3 IDS的发展方向 习题
 第14章 VPN的设计与实现 14.1 VPN概述 14.1.1 VPN概念 14.1.2 VPN的特点 14.1.3 VPN的
 分类 14.2 VPN关键技术 14.2.1 隧道封装技术 14.2.2 密码技术 14.2.3 身份鉴别和认证技术
 14.2.4 QoS 技术 14.3 隧道协议与VPN实现 14.3.1 PPTP 14.3.2 L2F 14.3.3 L2TP 14.3.4
 MPLS 14.3.5 IPSec 14.3.6 SSL 14.3.7 SOCKs 14.4 VPN 网络的配置与实现 14.4.1 Win 2000
 系统中VPN连接的设置 14.4.2 Linux系统中VPN连接的设置 14.5 VPN安全性分析 习题第15章 身
 份认证 15.1 身份证明 15.1.1 身份欺诈 15.1.2 身份证明系统的组成和要求 15.1.3 身份证明
 的基本分类 15.1.4 实现身份证明的基本途径 15.2 通行字认证系统 15.2.1 概述 15.2.2 通行
 字的控制措施 15.2.3 通行字的检验 15.2.4 通行字的安全存储 15.3 个人特征的身份证明技术
 15.3.1 手书签字验证 15.3.2 指纹验证 15.3.3 语音验证 15.3.4 视网膜图样验证 15.3.5 虹
 膜图样验证 15.3.6 脸型验证 15.3.7 身份证实系统的设计 15.4 零知识证明的基本概念 15.4.1
 概述 15.4.2 零知识证明的基本协议 15.4.3 并行零知识证明 15.4.4 使第三者相信的协议(零知
 识) 15.4.5 非交互式零知识证明 15.4.6 一般化理论结果 15.5 零知识身份证明的密码体制
 15.5.1 Feige?Fiat?Shamir体制 15.5.2 GQ识别体制 15.5.3 Schnorr识别体制 15.5.4 Fiat?Shamir
 , GQ和Schnorr体制的比较 15.5.5 离散对数的零知识证明体制 15.5.6 公钥密码体制破译的零知
 识证明 15.6 身份认证协议实践 15.6.1 安全壳远程登录协议 15.6.2 Kerberos协议及其在Windows
 2000系统中的实现 15.6.3 SSL和TLS 15.7 智能卡技术及其应用 习题参考文献

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>