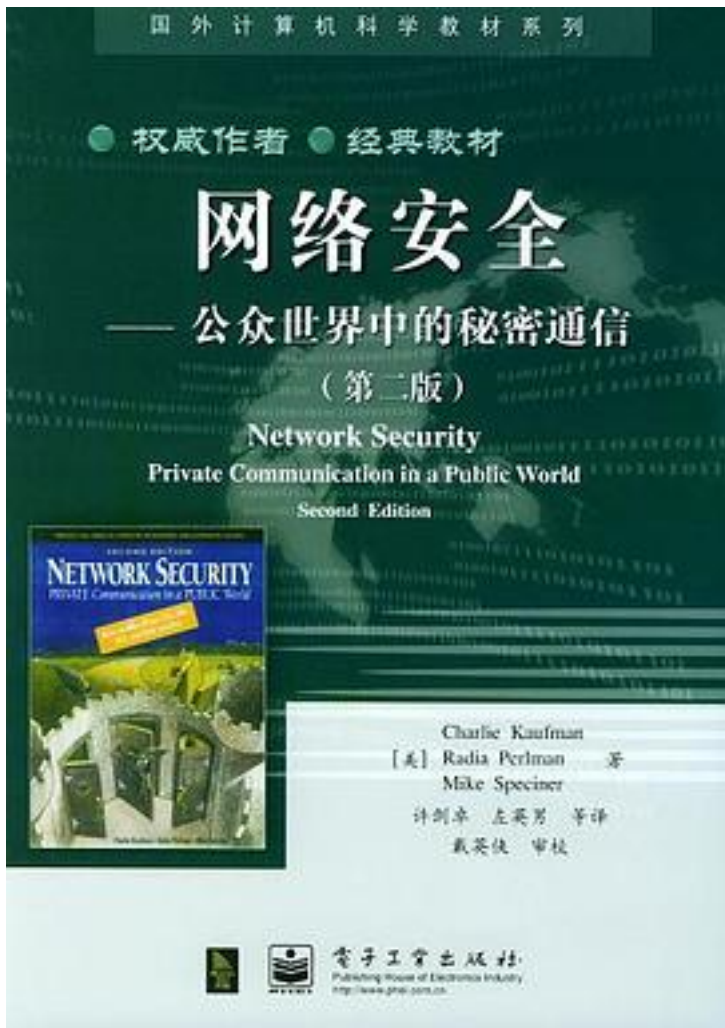


网络安全



[网络安全_下载链接1](#)

著者:刘建伟

出版者:清华大学出版社

出版时间:2005-01-01

装帧:简装本

isbn:9787302105862

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。

作者介绍:

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“科技标兵”称号。主持研制的海信防火墙获山东省科技进步二等奖,海信Netkey身份认证系统获山东省计算机应用新成果二等奖。在国内外学术刊物和会议上发表论文30篇,出版著作多部,合写著作曾获教育部全国普通高校优秀教材一等奖。

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

1.5.4 认证失效

1.5.5 协议缺陷

1.5.6 信息泄露

1.5.7 拒绝服务攻击——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

目录第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

- 2.1.5UDP
- 2.1.6ICMP
- 2.2地址和域名管理
 - 2.2.1路由协议
 - 2.2.2域名系统
 - 2.2.3BOOTP和DHCP
- 2.3IPv6
 - 2.3.1IPv6简介
 - 2.3.2IPv6地址
 - 2.3.3IPv6地址配置
 - 2.3.4邻居发现协议
 - 2.3.5移动IPv6
 - 2.3.6IPv6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
 - 3.1.1SMTP
 - 3.1.2MIME
 - 3.1.3POP3
 - 3.1.4IMAP4
 - 3.1.5即时消息
 - 3.2互联网电话
 - 3.2.1H.323
 - 3.2.2SIP
 - 3.3基于RPC的协议
 - 3.3.1RPC与Rpcbind
 - 3.3.2NIS
 - 3.3.3NFS
 - 3.3.4AFS
 - 3.4TFTP和FTP
 - 3.4.1TFTP
 - 3.4.2FTP
 - 3.4.3SMB协议
 - 3.5远程登录协议
 - 3.5.1Telnet
 - 3.5.2“r”命令
 - 3.5.3SSH
 - 3.6SNMP
 - 3.7NTP
 - 3.8信息服务
 - 3.8.1Finger——用户查询服务
 - 3.8.2Whois——数据库查询服务
 - 3.8.3LDAP
 - 3.8.4WWW服务
 - 3.8.5NNTP——网络消息传输协议
 - 3.8.6多播及MBone
 - 3.9专有协议
 - 3.9.1RealAudio
 - 3.9.2Oracle的SQL*Net
 - 3.9.3其他专用服务
 - 3.10对等实体联网
 - 3.11X11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

4.4.1A5

4.4.2加法流密码生成器

4.4.3RC4

4.4.4SEAL

4.4.5PKZIP

4.5分组密码概述

4.6数据加密标准

4.6.1DES介绍

4.6.2DES的核心作用：消息的随机非线性分布

4.6.3DES的安全性

4.7高级加密标准

4.7.1Rijndael密码概述

4.7.2Rijndael密码的内部函数

4.7.3Rijndael内部函数的功能小结

4.7.4AES对应用密码学的积极影响

4.8其他重要的分组密码算法

4.8.1IDEA

4.8.2SAFERK64

4.8.3RC5

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 [2]

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

5.2RSA密码体制

5.2.1体制

5.2.2RSA的安全性

5.2.3RSA的参数选择

5.2.4RSA体制实用中的其他问题

5.2.5RSA的实现

5.2.6RSA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
- 5.3.3MerkleHellman陷门背包
- 5.3.4MH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
- 5.4Rabin密码体制
- 5.4.1Rabin体制
- 5.4.2Williams体制
- 5.5ElGamal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
- 5.6.6ECC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
- 5.7.1McEliece密码体制
- 5.7.2LUC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
- 6.4MD4和MD5
- 6.4.1算法步骤
- 6.4.2MD5的安全性
- 6.4.3MD5的实现
- 6.4.4MD4与MD5算法差别

- 6.4.5MD2和MD3
- 6.5安全杂凑算法
 - 6.5.1算法
 - 6.5.2SHA的安全性
 - 6.5.3SHA与MD4，MD5的比较
- 6.6其他杂凑算法
 - 6.6.1RIPEMD160
 - 6.6.2SNEFRU算法
 - 6.6.3GOST杂凑算法
 - 6.6.4HAVAL算法
 - 6.6.5RIPEMAC
 - 6.6.6其他
- 6.7HMAC

习题

第7章数字签名

- 7.1数字签名基本概念
- 7.2RSA签名体制
- 7.3Rabin签名体制
- 7.4ElGamal签名体制
- 7.5Schnorr签名体制
- 7.6DSS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
 - 7.6.4DSS签名、验证框图
 - 7.6.5公众反应
 - 7.6.6实现速度
- 7.7GOST签名标准
- 7.8ESIGN签名体制
- 7.9Okamoto签名体制
- 7.10OSS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 [2]
 - 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
- 8.4.3TatebayashiMatsuzakiNewman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

9.1PKI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

9.2.1X.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

9.4PKI/CA认证系统实例

9.5PMI介绍

9.5.1PMI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

- 10.6.4TTP
- 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 [2]
 - 11.2.1扩谱技术
 - 11.2.2正交频分复用
 - 11.2.3IEEE制定的无线局域网标准
 - 11.2.4802.11无线网络的工作模式
 - 11.2.5IEEE制定的无线城域网络标准
 - 11.2.6蓝牙
 - 11.2.7HomeRF技术
 - 11.2.8无线应用协议
- 11.3无线蜂窝网络的安全性
 - 11.3.1GSM安全性分析
 - 11.3.2CDMA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
 - 11.4.2802.1x协议介绍
 - 11.4.3802.11i标准介绍

- 11.4.4802.16标准的安全性
- 11.4.5WAP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
 - 11.6.4MAC地址过滤
 - 11.6.5SSID问题解决方案
 - 11.6.6天线的选择
 - 11.6.7VLAN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
 - 11.6.10WEP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 (CutoffProxy)
 - 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 (AirGap)
 - 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

13.1IDS的概述

13.1.1IDS的历史

13.1.2IDS的分类

13.1.3IDS的作用

13.1.4IDS的任务

13.1.5IDS的主要功能

13.1.6IDS的评价标准

13.1.7IDS的典型部署

13.2IDS的设计

13.2.1CIDF的模型

13.2.2NIDS的设计

13.2.3NIDS的关键技术

13.2.4HIDS的设计

13.2.5HIDS的关键技术

13.2.6控制台的设计

13.2.7自身安全设计

13.3IDS的发展方向

习题

第14章VPN的设计与实现

14.1VPN概述

14.1.1VPN概念

14.1.2VPN的特点

14.1.3VPN的分类

14.2VPN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

14.2.4QoS技术

14.3隧道协议与VPN实现

14.3.1PPTP

14.3.2L2F

14.3.3L2TP

14.3.4MPLS

14.3.5IPSec

14.3.6SSL

14.3.7SOCKs

14.4VPN网络的配置与实现

14.4.1Win2000系统中VPN连接的设置

14.4.2Linux系统中VPN连接的设置

14.5VPN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
 - 15.5.1FeigeFiatShamir体制
 - 15.5.2GQ识别体制
 - 15.5.3Schnorr识别体制
 - 15.5.4FiatShamir，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
 - 15.6.2Kerberos协议及其在Windows2000系统中的实现
 - 15.6.3SSL和TLS
- 15.7智能卡技术及其应用
- 习题
- 参考文献
 - • • • • (收起)

[网络安全_下载链接1](#)

标签

评论

[网络安全_下载链接1](#)

[网络安全_下载链接1](#)