

# 《网络安全》

## 图书基本信息

书名：《网络安全》

13位ISBN编号：9787030319234

10位ISBN编号：7030319230

出版时间：2011-7

出版社：科学出版社

作者：胡建伟

页数：276

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)

# 《网络安全》

## 内容概要

《普通高等教育信息安全类国家级特色专业系列规划教材:网络安全》系统地介绍了网络安全问题。《普通高等教育信息安全类国家级特色专业系列规划教材:网络安全》共14章,内容包括网络安全综述、对称密码学、单向散列函数、公钥密码系统、因特网与TCP/IP安全、VPN和IPSec、SSL和TLS、身份认证及其应用、访问控制与系统审计、防火墙技术、入侵检测系统、安全编程、恶意代码安全和无线局域网安全。《普通高等教育信息安全类国家级特色专业系列规划教材:网络安全》内容新颖、丰富,各章节都提供了参考资料和思考题,以供进一步学习研究。网络安全和密码学是当今通信与计算机领域的热门课题。

《普通高等教育信息安全类国家级特色专业系列规划教材:网络安全》可作为信息对抗、通信、电子或计算机相关专业的教材,也可作为相关领域的研究人员和专业技术人员的参考书。

## 书籍目录

丛书序

前言

### 第1章 网络安全综述

1.1 安全概念和术语

1.2 网络安全威胁

1.2.1 脆弱性、威胁和风险

1.2.2 网络威胁的类型

1.3 网络攻击

1.3.1 网络攻击的定义

1.3.2 攻击的一般过程

1.3.3 攻击的主要方式

1.4 X.800安全体系结构

1.4.1 安全攻击、安全机制和安全服务

1.4.2 安全服务

1.4.3 安全机制

1.4.4 服务和机制之间的关系

1.5 X.805安全体系框架

1.6 网络安全模型

1.7 安全评估与风险管理

1.7.1 评估方法

1.7.2 评估标准

1.7.3 评估的作用

1.7.4 安全风险的管理

思考题

### 第2章 对称密码学

2.1 密码系统模型

2.2 古典密码

2.2.1 替代密码

2.2.2 置换密码

2.3 数据加密标准

2.3.1 分组密码简介

2.3.2 DES算法的描述

2.3.3 DES密码分析

2.3.4 DES工作模式

2.3.5 三重DES

2.4 高级加密标准

2.4.1 代数基础

2.4.2 AES算法描述

2.4.3 字节代替

2.4.4 行移位

2.4.5 列混淆

2.4.6 轮密钥加

2.4.7 密钥调度

2.4.8 AES安全性分析

2.5 流密码算法

2.5.1 列密码简介

2.5.2 A5算法

## 思考题

### 第3章 单向散列函数

#### 3.1 MD5算法

##### 3.1.1 算法

##### 3.1.2 举例

#### 3.2 安全散列函数

##### 3.2.1 算法

##### 3.2.2 SHA-1与MD5的比较

##### 3.2.3 举例

#### 3.3 消息认证码

## 思考题

### 第4章 公钥密码系统

#### 4.1 数论基础

##### 4.1.1 素数

##### 4.1.2 费马小定理

##### 4.1.3 欧拉定理

#### 4.2 RSA密码系统

#### 4.3 Diffie-Hellman密钥交换

##### 4.3.1 Diffie-Hellman算法

##### 4.3.2 中间人攻击

##### 4.3.3 认证的Diffie-Hellman密钥交换

##### 4.3.4 三方或多方Diffie-Hellman

#### 4.4 数字签名

##### 4.4.1 基本概念

##### 4.4.2 数字签名算法

##### 4.4.3 RSA签名方案

##### 4.4.4 其他数字签名方案

## 思考题

### 第5章 因特网与TCP/IP安全

#### 5.1 TCP/IP协议栈

#### 5.2 协议封装

#### 5.3 IP协议

#### 5.4 TCP协议

##### 5.4.1 TCP安全缺陷

##### 5.4.2 IP欺骗攻击

#### 5.5 UDP协议

#### 5.6 ARP/RARP协议

#### 5.7 网络服务的安全性

##### 5.7.1 文件传输协议

##### 5.7.2 域名系统

## 思考题

### 第6章 VPN和IPSec

#### 6.1 VPN定义

#### 6.2 VPN优势

#### 6.3 VPN的安全考虑

#### 6.4 常见VPN应用环境

#### 6.5 VPN安全策略

#### 6.6 VPN数据安全性

##### 6.6.1 认证

- 6.6.2 加密
- 6.6.3 完整性
- 6.7 VPN协议
  - 6.7.1 PPTP
  - 6.7.2 L2TP
  - 6.7.3 IPSec
- 6.8 IPSec协议
  - 6.8.1 安全关联
  - 6.8.2 SA管理、创建、删除
  - 6.8.3 SA参数
  - 6.8.4 安全策略
  - 6.8.5 选择符
  - 6.8.6 IPSec模式
- 6.9 IPSec数据包信息格式
  - 6.9.1 认证报头
  - 6.9.2 AH模式
  - 6.9.3 封装安全有效载荷
  - 6.9.4 SA组合
- 6.10 因特网密钥管理协议
  - 6.10.1 IPSec的密钥管理需求
  - 6.10.2 认证方法
  - 6.10.3 密钥交换
  - 6.10.4 IKE阶段综述
  - 6.10.5 ISAKMP消息结构
  - 6.10.6 IPSec/IKE系统处理

## 思考题

## 第7章 SSL和TLS

- 7.1 SSL协议体系结构
- 7.2 SSL/TLS记录协议
  - 7.2.1 SSL 3.0的MAC计算
  - 7.2.2 TLS1.2的MAC计算
- 7.3 改变密码规范协议
- 7.4 告警协议
- 7.5 握手协议
  - 7.5.1 常规握手过程
  - 7.5.2 支持客户认证的握手过程
  - 7.5.3 恢复SSL/TLS会话
  - 7.5.4 SSL 2.0握手过程
- 7.6 密钥计算
  - 7.6.1 计算主密钥
  - 7.6.2 伪随机函数
  - 7.6.3 计算其他密钥参数
  - 7.6.4 安全HTTP通信

## 思考题

## 第8章 身份认证及其应用

- 8.1 引言
- 8.2 身份认证的方法
  - 8.2.1 基于用户知道什么的身份认证
  - 8.2.2 基于用户拥有什么的身份认证

- 8.2.3 基于用户是谁的身份认证
- 8.2.4 指纹识别技术
- 8.2.5 击键特征识别
- 8.3 第三方认证
  - 8.3.1 Kerberos概述
  - 8.3.2 Kerberos版本4认证消息对话
  - 8.3.3 Kerberos基础结构和交叉领域认证
  - 8.3.4 Kerberos版本5
- 8.4 X.509
  - 8.4.1 认证协议——简单认证过程
  - 8.4.2 认证协议——强认证程序
- 8.5 数字证书
  - 8.5.1 证书的获取
  - 8.5.2 证书的吊销
- 8.6 验证证书
  - 8.6.1 单向认证
  - 8.6.2 双向认证
  - 8.6.3 三向认证
- 8.7 CA系统结构
  - 8.7.1 CA服务器
  - 8.7.2 RA服务器
  - 8.7.3 证书目录服务器
  - 8.7.4 CA操作步骤
  - 8.7.5 证书链构造
  - 8.7.6 证书验证过程
  - 8.7.7 小结
- 思考题
- 附录A:CA证书样本——PEM格式
- 附录B:CA证书样本——TXT格式
- 第9章 访问控制与系统审计
  - 9.1 访问控制
    - 9.1.1 基本概念
    - 9.1.2 自主访问控制
    - 9.1.3 强制访问控制
    - 9.1.4 访问控制模型
    - 9.1.5 基于角色的访问控制
    - 9.1.6 RBAC标准模型
    - 9.1.7 总结
  - 9.2 计算机安全等级的划分
  - 9.3 系统审计
    - 9.3.1 审计及审计跟踪
    - 9.3.2 安全审计
- 思考题
- 第10章 防火墙技术
  - 10.1 防火墙的基本概念
  - 10.2 防火墙技术层次
    - 10.2.1 包过滤防火墙
    - 10.2.2 应用代理防火墙
    - 10.2.3 电路级网关型防火墙

- 10.2.4 状态包检测
- 10.3 防火墙体系结构
  - 10.3.1 双重宿主主机体系结构
  - 10.3.2 屏蔽主机体系结构
  - 10.3.3 屏蔽子网结构
- 10.4 包过滤技术
  - 10.4.1 创建包过滤规则
  - 10.4.2 IP头信息
  - 10.4.3 TCP头信息
  - 10.4.4 UDP端口过滤
  - 10.4.5 无状态操作和有状态检查
- 10.5 堡垒主机
- 10.6 应用网关和代理服务器
  - 10.6.1 网络地址转换器
  - 10.6.2 内容屏蔽和阻塞
  - 10.6.3 日志和报警措施
- 思考题
- 第11章 入侵检测系统
  - 11.1 引言
  - 11.2 入侵检测基本原理
    - 11.2.1 入侵检测的基本概念
    - 11.2.2 入侵检测系统
  - 11.3 入侵检测系统分类
    - 11.3.1 按数据来源的分类
    - 11.3.2 按分析技术的分类
    - 11.3.3 其他的分类
  - 11.4 入侵检测系统模型
    - 11.4.1 入侵检测系统的CIDF模型
    - 11.4.2 Denning的通用入侵检测系统模型
  - 11.5 分布式入侵检测系统
  - 11.6 小结
- 第12章 安全编程
  - 12.1 缓冲区溢出
    - 12.1.1 背景知识
    - 12.1.2 缓冲区溢出基本原理
    - 12.1.3 缓冲区溢出攻击方式
    - 12.1.4 有关Shellcode
    - 12.1.5 安全建议
  - 12.2 格式化字符串
    - 12.2.1 格式化函数和格式化字符串
    - 12.2.2 格式化字符串漏洞基本原理
    - 12.2.3 格式化字符串攻击
    - 12.2.4 安全建议
  - 12.3 整数安全
    - 12.3.1 整数
    - 12.3.2 整数类型转换
    - 12.3.3 整数溢出漏洞
    - 12.3.4 安全建议
  - 12.4 条件竞争

- 12.4.1 用户ID
- 12.4.2 条件竞争
- 12.4.3 安全建议
- 12.5 临时文件
- 12.6 动态内存分配和释放
- 12.6.1 背景知识
- 12.6.2 安全隐患

## 思考题

## 第13章 恶意代码安全

- 13.1 恶意代码
- 13.2 恶意代码的命名规则
- 13.3 恶意代码工作机理
- 13.3.1 恶意代码自我保护技术
- 13.3.2 恶意代码入侵技术
- 13.3.3 恶意代码隐藏技术
- 13.3.4 恶意代码防范
- 13.4 恶意代码分析技术
- 13.4.1 静态分析技术
- 13.4.2 文件类型分析
- 13.4.3 字符串提取分析
- 13.5 动态分析
- 13.5.1 注册表监视
- 13.5.2 监控文件变动
- 13.5.3 网络行为分析

## 思考题

## 第14章 无线局域网安全

- 14.1 无线和有线的区别
- 14.1.1 物理安全
- 14.1.2 设备局限性
- 14.2 安全威胁
- 14.2.1 窃听和网络通信流分析
- 14.2.2 信任传递
- 14.2.3 基础结构
- 14.2.4 拒绝服务
- 14.3 WLAN概述
- 14.3.1 协议堆栈
- 14.3.2 无线拓扑结构
- 14.3.3 基本和扩展服务集
- 14.3.4 WLAN网络服务
- 14.4 无线局域网的安全机制
- 14.4.1 SSID匹配
- 14.4.2 MAC地址过滤
- 14.4.3 认证和关联
- 14.4.4 WEP协议
- 14.4.5 WEP加密机制存在的安全问题
- 14.5 IEEE 802.1x协议
- 14.6 WPA规范
- 14.6.1 WPA认证
- 14.6.2 WPA加密



14.6.3 WPA完整性

14.7 IEEE 802.11i

14.8 WAPI——中国的WLAN安全标准

思考题

参考文献

## 章节摘录

版权页：插图：威胁可能是主动性的（当系统状态可被改变时），也可能是被动性的（不改变系统状态但非法泄露信息）。伪装成合法主体和拒绝服务是主动性威胁的例子，窃听获取口令是被动性威胁的例子。威胁可能是由黑客、恐怖分子、破坏分子、有组织犯罪或政府发起的，但相当数量的威胁来自组织内部人员。安全风险来源于安全脆弱性与安全威胁的结合。例如，操作系统应用的溢出漏洞（即脆弱性）加上黑客的知识、合适的工具和访问（即威胁）可产生万维网服务器攻击的风险。安全风险的后果是数据丢失、数据损坏、隐私失窃、诈骗、宕机及失去公共信任。1.2.2 网络威胁的类型威胁定义为对脆弱性的潜在利用，这些脆弱性可能导致非授权访问、信息泄露、资源耗尽、资源被盗或者被破坏。网络安全与保密所面临的威胁可以来自很多方面，并且是随着时间的变化而变化。网络安全的威胁可以是来自内部网或者外部网的，根据不同的研究结果表明，有80%-95%的安全事故来自内部网。显然只有少数网络攻击来自互联网。一般而言，主要的威胁种类有以下10种。

# 《网络安全》

## 编辑推荐

《普通高等教育信息安全类国家级特色专业系列规划教材:网络安全》以实践能力为培养目标，以安全缺陷为教学实例，系统阐述网络安全的核心概念及关键技术。以开放系统安全协议体系为框架，由浅入深，层层展开。概念阐述直观，叙述简练，图文并茂，实例丰富。内容攻防兼备，理论实践并重。可赠送电子课件给任课教师。

## 精彩短评

1、很好，给满分，推荐给大家

## 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：[www.tushu000.com](http://www.tushu000.com)