

目 录:

第一部分网络安全基础

第 1 章网络安全概述/

1.1 网络安全的概念及目标

1.2 网络安全现状

1.3 ISO/OSI 网络安全体系

1.3.1 安全策略

1.3.2 安全服务

1.3.3 安全机制

1.3.4 安全管理

1.4 典型网络安全模型

1.4.1 动态自适应网络模型

1.4.2 APPDRR 模型

1.4.3 分层的网络安全解决方案

1.5 网络安全评估规范

1.5.1 可信计算机系统评估准则

1.5.2 通用准则

1.5.3 信息安全保障技术框架

1.5.4 计算机信息系统安全保护等级划分准则

本章实验

思考题

第 2 章密码学基础/

2.1 密码学概述

2.1.1 密码算法和密钥

2.1.2 密码算法分类

2.1.3 密码分析与计算复杂性

2.2 对称密钥算法

2.2.1 DES

2.2.2 3DES

2.2.3 其他对称密钥算法

2.3 公钥算法

2.3.1 RSA

2.3.2 Diffie Hellman

2.4 哈希算法

2.4.1 MD5

2.4.2 SHA

2.5 密码协议

本章实验

思考题

第3章 数字认证技术/

3.1 认证技术概述

3.1.1 报文鉴别

3.1.2 身份鉴别

3.2 密码鉴别

3.2.1 密码与密码攻击

3.2.2 验证码

3.2.3 一次一密密码

3.2.4 基于挑战/应答的鉴别

3.3 基于密钥的鉴别

3.3.1 基于对称密钥的鉴别

3.3.2 基于非对称密钥的鉴别

3.3.3 基于第三方的鉴别

3.4 数字签名

3.5 认证技术的应用

3.5.1 PPP 中的认证

3.5.2 AAA 协议及其应用

3.5.3 Kerberos 鉴别

3.5.4 S/KEY 一次性密码鉴别

本章实验

思考题

第4章 公钥基础设施/

4.1 PKI 概述

4.2 PKI 技术发展及应用现状

4.3 PKI 体系结构——PKIX 模型

4.4 X.509 证书

- 4.5 PKI 信任模型
- 4.6 密钥和证书的生命周期
 - 4.6.1 密钥/证书生命周期管理
 - 4.6.2 密钥生命周期
 - 4.6.3 证书生命周期
- 4.7 PKI 相关标准
- 4.8 成熟 PKI 系统简介
 - 4.8.1 商业应用
 - 4.8.2 政府应用
- 4.9 PKI 实施与应用案例
 - 4.9.1 小型 PKI 和 CA 设计案例
 - 4.9.2 大型 PKI 系统设计案例
 - 4.9.3 PKI 应用简介
- 本章实验
- 思考题

第二部分 TCP/IP 网络安全协议

第 5 章网络层安全协议/

- 5.1 IPSec 概述
- 5.2 IPSec 体系结构
- 5.3 Ipsec 的操作模式
- 5.4 安全策略与安全协议
- 5.5 密钥交换协议
 - 5.5.1 ISAKMP
 - 5.5.2 IKE
 - 5.5.3 IKE 在 IPSec 中的应用
- 5.6 验证头 AH
 - 5.6.1 AH 报文格式
 - 5.6.2 AH 操作模式
 - 5.6.3 AH 协议处理过程
- 5.7 封装安全载荷 ESP
 - 5.7.1 ESP 报文格式
 - 5.7.2 ESP 操作模式
 - 5.7.3 ESP 协议处理及 AH 嵌套

5.8 IPSec 的应用

本章实验

思考题

第 6 章传输层安全协议/

6.1 SSL 协议

6.1.1 SSL 概述

6.1.2 SSL 连接与会话

6.1.3 SSL 握手协议

6.1.4 SSL 记录集协议

6.1.5 SSL 密码计算

6.1.6 SSL 协议的应用

6.2 SSH 协议

6.2.1 SSH 概述

6.2.2 SSH 协议体系结构

6.2.3 SSH 协议分析

6.2.4 SSH 协议的通信过程

6.2.5 SSH 协议的应用

6.3 SOCKS 协议

6.3.1 SOCKS 协议概述

6.3.2 SOCKS 协议通信过程

本章实验

思考题

第 7 章应用层安全协议/

7.1 Internet 的应用层安全隐患

7.2 WWW 安全

7.2.1 WWW 安全保障体系

7.2.2 HTTP 安全协议

7.3 电子邮件安全协议

7.3.1 电子邮件及其安全性概述

7.3.2 S/MIME

7.3.3 PGP

7.3.4 垃圾邮件防御技术介绍

- 7.4 DNS 安全协议
 - 7.4.1 DNS 脆弱性分析
 - 7.4.2 DNS 安全防护策略
 - 7.4.3 DNSSEC 协议概述
 - 7.4.4 DNSSEC 密钥管理
 - 7.4.5 DNSSEC 签名验证及公钥信任机制
 - 7.4.6 TSIG 和 TKEY
 - 7.5 SNMP 安全协议
 - 7.5.1 SNMP 及其安全性概述
 - 7.5.2 SNMPv3 的体系结构
 - 7.5.3 SNMPv3 安全服务的实现
- 本章实验
- 思考题

第三部分网络安全技术与应用

第8章企业级安全技术/

- 8.1 虚拟专用网
 - 8.1.1 VPN 概述
 - 8.1.2 VPN 分类
 - 8.1.3 PPTP
 - 8.1.4 L2F/L2TP
 - 8.1.5 MPLS VPN
 - 8.1.6 VPN 实施示例
- 8.2 访问控制与安全审计
 - 8.2.1 访问控制策略
 - 8.2.2 访问控制实施模型
 - 8.2.3 访问控制实施策略
 - 8.2.4 访问控制语言
 - 8.2.5 安全审计
- 8.3 防火墙技术
 - 8.3.1 防火墙概述
 - 8.3.2 防火墙分类
 - 8.3.3 防火墙相关技术
 - 8.3.4 防火墙应用模式

- 8.4 入侵检测系统
 - 8.4.1 入侵检测概述
 - 8.4.2 入侵检测系统的分类
 - 8.4.3 入侵检测系统模型
 - 8.4.4 分布式入侵检测系统
 - 8.4.5 SNORT 入侵检测系统
 - 8.4.6 入侵检测的发展趋势

本章实验

思考题

第9章无线网络及移动 IP 安全/

- 9.1 无线网络安全概述
 - 9.1.1 无线网络及其分类
 - 9.1.2 无线网络安全性分析
- 9.2 常用无线局域网安全技术
 - 9.2.1 传统安全措施
 - 9.2.2 增强安全机制
- 9.3 802.11X 认证机制
 - 9.3.1 802.1x 框架结构
 - 9.3.2 802.1x 安全性分析
 - 9.3.3 高层认证协议
 - 9.3.4 802.1x 协议技术特点
- 9.4 WAPI
 - 9.4.1 WAPI 的工作原理
 - 9.4.2 WAPI 的特点
- 9.5 移动 IP 安全概述
 - 9.5.1 移动 IP 概述
 - 9.5.2 移动 IP 的工作原理
 - 9.5.3 移动 IP 面临的安全威胁及对策
- 9.6 移动 IP 安全机制
 - 9.6.1 基于 AAA 的移动 IP 认证机制
 - 9.6.2 基于公钥的移动 IP 安全构架
 - 9.6.3 移动 IPSec 方案
 - 9.6.4 穿越防火墙的 IP 移动方案

思考题

第 10 章 Web Service 与网络安全/

10.1 Web Service 及其安全性概述

10.1.1 Web Service 简介

10.1.2 Web Service 的安全性需求

10.2 Web Service 安全技术概述

10.2.1 XML 签名

10.2.2 XML 加密

10.2.3 Soap 消息安全保护

10.3 WS Security

10.3.1 WS Security 消息模型

10.3.2 WS Security 基本语法要素

10.3.3 WS Security 安全令牌信任机制

10.4 网格及其安全性概述

10.4.1 网格体系结构及其特性

10.4.2 网格环境中的安全挑战

10.4.3 网格的安全性需求及其安全架构

10.5 网络安全基础设施

10.5.1 GSI 概述

10.5.2 GSI 关键技术