

<<网络安全要素>>

图书基本信息

书名：<<网络安全要素>>

13位ISBN编号：9787115087911

10位ISBN编号：7115087911

出版时间：2000-11

出版时间：人民邮电出版社

作者：William Stallings

页数：287

字数：462000

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>

## <<网络安全要素>>

### 内容概要

本书分四部分介绍网络安全的应用和标准：第一部分是概述；第二部分简要说明作为网络安全应用基础的加密算法和协议，如加密、哈希函数、数字签名和密钥交换等内容；第三部分介绍重要的网络安全工具和应用，包括Kerberos、X.509v3证书、PGP、S/MIME、IP安全、SSL/TLS、SET和SNMPv3等；第四部分介绍系统级的安全问题，包括入侵者和病毒的威胁及对策、防火墙和可信系统的使用等。

本书适用于计算机及相关专业的大中专学生，以及网络安全技术人员。

## &lt;&lt;网络安全要素&gt;&gt;

## 书籍目录

第一部分 概述	第1章 网络安全简介	1.1 攻击、服务和机制	1.1.1 服务	1.1.2 机制
1.1.3 攻击	1.2 安全攻击	1.2.1 被动攻击	1.2.2 主动攻击	1.3 安全服务
1.3.1 保密性	1.3.2 验证	1.3.3 完整性	1.3.4 不可否认性	1.3.5 访问控制
1.3.6 可用性	1.4 网络安全模型	1.5 Internet标准和RFC	1.5.1 Internet社团	1.5.2 RFC的发布
1.5.3 标准化进程	1.5.4 非标准跟踪文档	1.6 Internet和Web资源	1.6.1 本书的Web站点	1.6.2 其他网络站点
1.6.3 UNENET新闻组	1.6.4 推荐读物	第二部分 密码术	第2章 常规加密和消息的保密性	2.1 常规加密原则
2.1.1 密码术	2.1.2 密码分析	2.1.3 Feistel的密码结构	2.2 常规加密算法	2.2.1 数据加密标准
2.2.2 三重DEA	2.2.3 高级加密标准	2.2.4 其他对称分组密码	2.3 密码分组操作方式	2.3.1 加密分组的链方式
2.3.2 密码反馈方式	2.4 加密设备的位置	2.5 密钥分布	2.6 习题	第3章 公钥密码和消息验证
3.1 消息验证的方法	3.1.1 使用常规加密方法的验证	3.1.2 没有加密的消息验证	3.1.3 消息验证码	3.1.4 单向哈希函数
3.2 安全哈希函数和HMAC	3.2.1 哈希函数的需求	3.2.2 简单哈希函数	3.2.3 SHA-1安全哈希函数	3.2.4 其他安全哈希函数
3.2.5 HMAC	3.3 公钥密码术规则	3.3.1 公钥加密的结构	3.3.2 公钥密码系统的应用	3.3.3 公钥密码的要求
3.4 公钥密码算法	3.4.1 RSA公钥加密算法	3.4.2 Diffie-Hellman密钥交换	3.4.3 其他公钥密码算法	3.5 数字签名
3.6 密钥管理	3.6.1 数字证书	3.6.2 公钥密码的保密密钥分发	3.7 习题	3.8 背景知识--素数和模运算
3.8.1 素数和相对素数	3.8.2 模运算	第三部分 网络安全应用	第4章 身份验证应用	4.1 Kerberos
4.1.1 动机	4.1.2 Kerberos 版本4	4.1.3 Kerberos 版本5	4.2 X.509身份验证服务	4.2.1 证书
4.2.2 身份验证过程	4.2.3 X.509版本3	4.3 习题	4.4 背景知识--Kerberos加密技术	4.4.1 口令到密钥的转换
4.4.2 传播密码分组链模式	第5章 电子邮件安全	5.1 PGP	5.1.1 表示法	5.1.2 操作说明
5.1.3 密钥和密钥环	5.1.4 公钥管理	5.2 S/MIME	5.2.1 RFC 822	5.2.2 多用Internet邮件扩展
5.2.3 S/MIME的功能	5.2.4 S/MIME的消息	5.2.5 S/MIME证书处理	5.2.6 增强的安全服务	5.3 使用ZIP压缩数据
5.3.1 压缩算法	5.3.2 解压缩算法	5.4 基数64转换	5.5 PGP随机数生成	5.5.1 真随机数
5.5.2 伪随机数	5.6 习题	第6章 IP安全	6.1 IP安全概况	6.1.1 IPSec的应用
6.1.2 IPSec的优势	6.1.3 路由应用	6.2 IP安全体系结构	6.2.1 IPSec文档	6.2.2 IPSec服务
6.2.3 安全关联	6.2.4 传输和隧道模式	6.3 验证报头	6.3.1 反重放服务	6.3.2 完整性检查值
6.3.3 传输和隧道模式	6.4 封装安全有效载荷	6.4.1 ESP格式	6.4.2 加密和验证算法	6.4.3 填充
6.4.4 传输和隧道模式	6.5 组合式安全关联	6.5.1 验证加保密性	6.5.2 SA的基本组合	6.6 密钥管理
6.6.1 Oakley密钥确定协议	6.6.2 ISAKMP	6.7 习题	6.8 背景知识--网络互连和Internet协议	6.8.1 IP的作用
6.8.2 IPv4	6.8.3 IPv6	6.8.4 IPv6报头	第7章 Web安全	7.1 Web安全问题
7.1.1 Web安全威胁	7.1.2 Web通信流安全的实现	7.2 安全套接层和传输层安全	7.2.1 SSL体系结构	7.2.2 SSL记录协议
7.2.3 改变密码规格协议	7.2.4 警告协议	7.2.5 握手协议	7.2.6 密码计算	7.2.7 传输层安全
7.3 安全电子交易	7.3.1 SET 概述	7.3.2 双重签名	7.3.3 支付过程	7.4 习题
第8章 网络管理安全	8.1 SNMP的基本概念	8.1.1 网络管理体系结构	8.1.2 网络管理协议体系结构	8.1.3 代理
8.1.4 SNMPv2	8.2 SNMPv1的共同体机制	8.2.1 共同体和共同体名称	8.2.2 验证服务	8.2.3 访问策略
8.2.4 代理服务	8.3 SNMPv3	8.3.1 SNMP体系结构	8.3.2 消息处理和用户安全模型	8.3.3 基于视图的访问控制
8.4 习题	第四部分 系统安全	第9章 入侵者和病毒	9.1 入侵者	9.1.1 入侵技术
9.1.2 口令保护	9.1.3 口令的弱点	9.1.4 访问控制	9.1.5 口令选择策略	9.1.6 入侵检测
9.2 病毒和相关威胁	9.2.1 恶意程序	9.2.2 病毒的性质	9.2.3 病毒的类型	9.2.4 宏病毒
9.2.5 反病毒方法	9.2.6 反病毒高级技术	9.3 习题	第10章 防火墙	10.1 防火墙设计原则
10.1.1 防火墙的特点	10.1.2 防火墙的种类	10.1.3 防火墙配置	10.2 可信系统	10.2.1 数据访

<<网络安全要素>>

问控制      10.2.2 可信系统的概念      10.2.3 防御特洛伊木马程序      10.3 习题附录A 本书引用的RFC附录B 网络安全课程教学计划      B.1 研究计划      B.2 编程计划      B.3 读书/报告作业附录C 术语表附录D 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>