

<<网络安全>>

图书基本信息

书名：<<网络安全>>

13位ISBN编号：9787505399457

10位ISBN编号：7505399454

出版时间：2004-9

出版时间：电子工业出版社

作者：(美国)考夫曼等著、许剑卓等译

页数：463

字数：845000

译者：考夫曼

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

本书全面阐述了信息安全理论，全书共分五个部分，即密码学、认证、标准、电子邮件以及其他安全机制。

其中，第一部分阐述了密码算法的基本原理以及各种经典的和现代的加密算法。

第二部分介绍了如何在网络中证明身份、人在向设备证明自己的身份时可能碰到的问题、认证握手协议的细节以及协议可能存在的多种缺陷。

第三部分讲述了一系列安全协议（如Kerberos，IPSec和SSL等）以及PKI的一些标准。

第四部分讲述了电子邮件安全中的若干问题，列出了与电子邮件相关的几个安全特性，并描述了这些安全特性的具体实现方式。

第五部分介绍了防火墙、各种操作系统的安全性问题、浏览网站时所涉及的协议以及对安全实践经验的总结。

本书提供了章后习题，书后还给出了大量参考文献。

本书从日常应用入手，以简单易懂的方式阐述了深奥的理论，加之原作者文笔生动幽默，堪称风格独特。

本书可作为相关专业高年级本科生和研究生的教学用书以及相关领域专业人员的参考用书。

作者简介

Sun Microsystems的资深工程师,她因在桥接、路由、以及安全方面的贡献而亨而享誉世界。Perlman是“ Interconnections:Bridges,Ridges,Routers,Switches,and Internetworking Protocols ”一书的作者,还是Data Cmmunications ”杂志评选出的网络界最有影响力的25人之一。

书籍目录

第1章 简介 1.1 本书内容 1.2 本书所属类型 1.3 术语 1.4 符号 1.5 网络基础知识 1.6 积极攻击和被动攻击 1.7 分层和密码学 1.8 授权 1.9 风暴 1.10 为执法部门实施密钥托管 1.11 为粗心的用户实施密钥托管 1.12 病毒、蠕虫和特洛伊木马 1.13 安全的多层模型 1.14 法律问题第一部分 密码学 第2章 密码学简介 2.1 什么是密码学 2.2 破解密码算法 2.3 密码算法函数 2.4 秘密密钥算法 2.5 公开密钥算法 2.6 哈希算法 2.7 习题 第3章 秘密密钥算法 3.1 简介 3.2 分组密码算法 3.3 数据加密标准 3.4 IDEA算法 3.5 AES算法 3.6 RC4算法 3.7 习题 第4章 运算模式 4.1 简介 4.2 加密长消息 4.3 生成MAC 4.4 使用DES算法实施多次加密 4.5 习题 第5章 哈希和消息摘要 5.1 简介 5.2 哈希算法的一些有趣的应用 5.3 MD2 5.4 MD4 5.5 MD5 5.6 SHA-1 5.7 HMAC 5.8 习题 第6章 公钥算法 6.1 简介 6.2 模运算 6.3 RSA 6.4 Diffie-Hellman 6.5 数字签名标准 6.6 RSA和Diffie-Hellman的安全性 6.7 椭圆曲线算法 6.8 零知识证明系统 6.9 习题 第7章 数论 7.1 简介 7.2 模运算 7.3 素数 7.4 欧几里得算法 7.5 中国余数定理 7.6 Z_n^* 7.7 欧拉的totient函数 7.8 欧拉定理 7.9 习题 第8章 AES和椭圆曲线的数学基础 8.1 简介 8.2 符号 8.3 群 8.4 域 8.5 Rijndael算法的数学基础 8.6 椭圆曲线算法 8.7 习题第二部分 认证 第9章 认证系统概述 9.1 基于口令的认证 9.2 基于地址的认证 9.3 密码认证协议 9.4 正在接受认证的人是谁 9.5 使用口令作为密钥 9.6 窃听及数据库读取 9.7 可信的第三方 9.8 会话密钥协商 9.9 代理 9.10 习题 第10章 认证人的身份 10.1 口令 10.2 在线口令猜解 10.3 离线口令猜解 10.4 应该使用多大数量的秘密 10.5 侦听 10.6 口令及粗心的用户 10.7 分发初始口令 10.8 认证令牌 10.9 物理接触 10.10 生物特征 10.11 习题 第11章 安全握手协议的缺陷 11.1 只进行登录 11.2 双向认证 11.3 加密数据和保护数据完整性 11.4 受干预的认证 11.5 Nonce类型 11.6 选择随机数 11.7 性能 11.8 认证协议核对表 11.9 习题 第12章 强口令协议 12.1 简介 12.2 Lamport哈希 12.3 强口令协议 12.4 强口令证明书下载协议 12.5 习题第三部分 标准 第13章 Kerberos V4 13.1 简介 13.2 门票和门票分发门票 13.3 配置 13.4 登录网络 13.5 备份KDC 13.6 域 13.7 域间认证 13.8 密钥版本号 13.9 加密以保证保密性和完整性 13.10 过加密只保护完整性 13.11 门票中的网络层地址 13.12 消息格式 13.13 习题 第14章 Kerberos V5 14.1 ASN.1 14.2 名称 14.3 权限代理 14.4 门票生存时间 14.5 密钥版本 14.6 在不同的域中使用不同的主密钥 14.7 优化 14.8 密码算法 14.9 域的层次结构 14.10 避免离线口令猜解 14.11 认证值中的密钥 14.12 双TGT认证 14.13 PKINIT: 用户的公开密钥 14.14 KDC数据库 14.15 Kerberos V5消息 14.16 习题 第15章 公钥基础设施 15.1 引言 15.2 一些技术 15.3 PKI信任模型 15.4 证书撤销 15.5 目录服务与PKI 15.6 PKIX和X.509 15.7 X.509和PKIX证书 15.8 授权的前景 15.9 习题 第16章 实时通信安全 16.1 协议应当实现在哪一层 16.2 会话密钥的建立 16.3 完美的前向保密性 16.4 PFS挫败 16.5 拒绝服务/防阻塞 16.6 端点识别符隐藏 16.7 通信双方的实时确认 16.8 并行计算 16.9 会话重用 16.10 似是而非的否认 16.11 数据流保护 16.12 协商密码参数 16.13 简单问题 16.14 习题 第17章 IPSec: AH和ESP 17.1 IPSec概述 17.2 IP和IPv6 17.3 AH 17.4 ESP 17.5 我们是否需要AH 17.6 编码方式的比较 17.7 问答题 17.8 习题 第18章 IPSec: IKE 18.1 Photuris 18.2 SKIP 18.3 IKE的历史 18.4 IKE的阶段 18.5 IKE的阶段1 18.6 IKE的阶段2 18.7 ISAKMP/IKE编码 18.8 习题..... 第19章 SSL/TLS第四部分 电子邮件 第20章 电子邮件安全 第21章 PEM和S/MIME 第22章 PGP第五部分 其他安全机制 第23章 防火墙 第24章 更多的安全系统 第25章 Web安全问题 第26章 实践经验术语表参考文献

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>