

<<网络安全基础>>

图书基本信息

书名：<<网络安全基础>>

13位ISBN编号：9787302154358

10位ISBN编号：730215435X

出版时间：2007-7

出版时间：清华大学出版社

作者：斯托林斯

页数：321

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>

## &lt;&lt;网络安全基础&gt;&gt;

## 内容概要

本书由著名作者William Stallings编写，完全从实用的角度出发，用较小的篇幅对当前网络安全解决方案中使用的主要算法、重要协议和系统管理方法等方面内容做了全面而详细的介绍。

全书共分为三部分：(1)密码算法和协议，包括网络安全应用中最常用的密码算法和协议；(2)网络安全应用，介绍了网络安全解决方案中使用的各种安全协议，如Kerberos、PGP、S/MIME、IPSec、SSL/TLS和SET等；(3)系统安全，介绍了一些系统级的安全问题，如网络入侵、恶意软件和防火墙等。

每章后面都提供了一定数量的推荐读物、网址、思考题和习题等。

全书最后还提供了一定数量的项目作业。

为方便作为教材使用的教师搞好教学，该书原出版社还提供了较为完整的配套服务。

与该书的前两版相比，第3版除在语言和叙述方面做进一步加工提高外，主要增加的内容包括RC4算法、公钥基础设施(PKI)、分布式拒绝服务攻击(DDoS)和信息技术安全评估通用准则等。

本书既可作为我国高校相关课程的教材使用，又是满足普通网络安全爱好者学习和了解网络安全基本知识的一本难得好书。

## 作者简介

作者：(美国)斯托林斯 译者：白国强 王海欣 陈弘毅 William Stallings：计算机网络与体系结构方面成就卓著。

他六次荣获由“教材与大学作者协会”颁发的“年度最佳计算机科学与工程教材”奖，作品包括《操作系统——精髓与设计原理》、《计算机组成与体系结构》、《数据与计算机通信》等。

他是致力于密码学各个方面的学术期刊Cryptologia的编委会成员之一。

目前他作为独立顾问为计算机硬件制造商、软件开发商和政府研究机构提供咨询服务。

## 书籍目录

第1章 引言 1.1 安全趋势 1.2 OSI安全体系结构 1.3安全攻击 1.3.1 被动攻击 1.3.2 主动攻击 1.4 安全服务 1.4.1 认证 1.4.2 访问控制 1.4.3 数据机密性 1.4.4 数据完整性 1.4.5 不可抵赖性 1.4.6 可用性服务 1.5 安全机制 1.6 网络安全模型 1.7 互联网标准与互联网协会 1.7.1 互联网组织和RFC发布 1.7.2 标准化过程 1.7.3 互联网标准分类 1.7.4 其他RFC类型 1.8 本书概览 1.9 推荐读物 1.10 互联网资源 1.10.1 本书网址 1.10.2 其他网址 1.10.3 USENET新闻组 1.11 关键词、思考题和习题 1.11.1 关键词 1.11.2 思考题 1.11.3 习题 第1部分 密码编码学 第2章 对称加密和消息机密性 2.1 对称加密原理 2.1.1 密码体制 2.1.2 密码分析 2.1.3 Feistel密码结构 2.2 对称分组加密算法 2.2.1 数据加密标准 2.2.2 三重DES 2.2.3 高级加密算法 2.3 流密码和RC4 2.3.1 流密码结构 2.3.2 RC4算法 2.4 分组密码的工作模式 2.4.1 密码分组链接模式 2.4.2 密码反馈模式 2.5 加密设备的位置 2.6 密钥分发 2.7 推荐读物和网址 推荐网址 2.8 关键词、思考题和习题 2.8.1 关键词 2.8.2 思考题 2.8.3 习题 第3章 公钥密码和消息认证 3.1 消息认证方法 3.1.1 利用常规加密的认证 3.1.2 非加密的消息认证 3.2 安全散列函数和HMAC 3.2.1 散列函数的要求 3.2.2 简单散列函数 3.2.3 安全散列函数SHA-1 3.2.4 其他安全散列函数 3.2.5 HMAC 3.3 公钥加密原理 3.3.1 公钥加密思想 3.3.2 公钥密码系统的应用 3.3.3 公钥加密的要求 3.4 公钥加密算法 3.4.1 RSA公钥加密算法 3.4.2 Diffie-Hellman密钥交换 3.4.3 其他公钥加密算法 3.5 数字签名 3.6 密钥管理 3.6.1 公钥证书 3.6.2 利用公钥分发密钥 3.7 推荐读物和网址 推荐网址 3.8 关键词、思考题和习题 3.8.1 关键词 3.8.2 思考题 3.8.3 习题 第2部分 网络安全应用 第4章 认证的应用 4.1 Kerberos 4.1.1 动机 4.1.2 Kerberos版本4 4.2 X.509认证服务 4.2.1 证书 4.2.2 认证过程 4.2.3 X.509版本3 4.3 公钥基础设施 4.3.1 PKIX管理功能 4.3.2 PKIX管理协议 4.4 推荐读物和网址 推荐网址 4.5 关键词、思考题和习题 4.5.1 关键词 4.5.2 思考题 4.5.3 习题 附录4A Kerberos加密技术 从口令到密钥的变换 PCBC模式 第5章 电子邮件安全 5.1 PGP 5.1.1 符号约定 5.1.2 操作描述 5.1.3 加密密钥和密钥环 5.1.4 公钥管理 5.2 S/MIME 5.2.1 RFC 822 5.2.2 多用途网际邮件扩展 5.2.3 S/MIME的功能 5.2.4 S/MIME的消息 5.2.5 S/MIME证书处理过程 5.2.6 增强的安全性服务 5.2.7 推荐网址 5.3 关键词、思考题和习题 5.3.1 关键词 5.3.2 思考题 5.3.3 习题 附录5A 使用ZIP的数据压缩 压缩算法 解压缩算法 附录5B 基-64转换 附录5C PGP随机数生成 真随机数 伪随机数 第6章 IP安全 6.1 IP安全概述 6.1.1 IPSec的应用 6.1.2 IPSec的好处 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 传输模式和隧道模式 6.3 认证报头 6.3.1 反重放服务 6.3.2 完整性校验值 6.3.3 传输模式和隧道模式 6.4 封装安全载荷 6.4.1 ESP格式 6.4.2 加密和认证算法 6.4.3 填充 6.4.4 传输模式和隧道模式 6.5 安全关联组合 6.5.1 认证加保密 6.5.2 安全关联的基本组合 6.6 密钥管理 6.6.1 Oakley密钥确定协议 6.6.2 ISAKMP 6.7 推荐读物和网址 推荐网址 6.8 关键词、思考题和习题 6.8.1 关键词 6.8.2 思考题 6.8.3 习题 附录6A 互联网与互联网协议 互联网协议的作用 IPv4 IPv6 第7章 Web安全 7.1 Web安全需求 7.1.1 Web安全威胁 7.1.2 Web流量安全方法 7.2 安全套接字层(SSL)和传输层安全(TLS) 7.2.1 SSL体系结构 7.2.2 SSL记录协议 7.2.3 密码变更规格协议 7.2.4 报警协议 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 推荐读物和网址 推荐网址 7.5 关键词、思考题和习题 7.5.1 关键词 7.5.2 思考题 7.5.3 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 委托代理 8.1.4 SNMPv2 8.2 SNMPv1共同体功能 8.2.1 共同体和共同体名称 8.2.2 认证服务 8.2.3 访问策略 8.2.4 委托代理服务 8.3 SNMPv3 8.3.1 SNMP体系结构 8.3.2 消息处理和用户安全模式 8.3.3 基于视图的访问控制 8.4 推荐读物和网址 推荐网址 8.5 关键词、思考题和习题 8.5.1 关键词 8.5.2 思考题 8.5.3 习题 第3部分 系统安全 第9章 入侵者 9.1 入侵者 9.1.1 入侵技术 9.2 入侵检测 9.2.1 审计记录 9.2.2 统计异常检测 9.2.3 基于规则的入侵检测 9.2.4 基率谬误 9.2.5 分布式入侵检测 9.2.6 蜜罐 9.2.7 入侵检测交换格式 9.3 口令管理 9.3.1 口令保护 9.3.2 口令选择策略 9.4 推荐读物和网址 推荐网站 9.5 关键词、思考题和习题 9.5.1 关键词 9.5.2 思考题 9.5.3 习题 附录9A 基率谬误 条件概率和独立性 贝叶斯定理 基率谬误示例 第10章 恶意软件 10.1 病毒及相关威胁 10.1.1 恶意程序 10.1.2 病毒的性质 10.1.3 病毒的类型 10.1.4 宏病毒 10.1.5 电子邮件病毒 10.1.6 蠕虫 10.1.7 蠕虫技术的现状 10.2 病毒对策 10.2.1 反病毒方法 10.2.2 高级反病毒技术 10.2.3 行为阻断软件 10.3 分布式拒绝服务攻击 10.3.1 DDoS攻击描述 10.3.2 构造攻击网络 10.3.3 DDoS防范 10.4 推荐读物和网址 推荐网址 10.5 关键词、思考题和习题 10.5.1 关键词 10.5.2 思考

题 10.5.3 习题 第11章 防火墙 11.1 防火墙设计原则 11.1.1 防火墙特征 11.1.2 防火墙类型 11.1.3 防火墙配置 11.2 可信系统 11.2.1 数据访问控制 11.2.2 可信系统的概念 11.2.3 特洛伊木马防护 11.3 信息技术安全评估通用准则 11.3.1 需求 11.3.2 大纲和目标 11.4 推荐读物和网址 推荐网址 11.5 关键词、思考题和习题 11.5.1 关键词 11.5.2 思考题 11.5.3 习题 附录A 数论知识 A.1 素数和互为素数 A.1.1 约数 A.1.2 素数 A.1.3 互为素数 A.2 模运算 附录B 网络安全教学项目 B.1 研究项目 B.2 编程项目 B.3 实验训练 B.4 写作作业 B.5 阅读报告作业 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>