

<<计算机网络安全导论>>

图书基本信息

书名：<<计算机网络安全导论>>

13位ISBN编号：9787564107932

10位ISBN编号：7564107936

出版时间：2007-9

出版时间：东南大学

作者：龚俭

页数：378

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>

## <<计算机网络安全导论>>

### 内容概要

本书从数据安全和网络安全两方面介绍了计算机网络安全的基本知识和常用的安全技术。

在数据安全方面介绍了目前主流的数据加密技术和密钥管理技术，支持数据完整性保护的信息摘录技术和多种数字签名技术，支持身份认证的各种数据鉴别技术，包括无否认、匿名通信等支持数据安全所需的一些基本公平服务。

在网络安全方面介绍了几种典型的访问控制技术和信任管理的基本内容，目前一些主要的网络威胁，网络安全监测技术以及包括防火墙技术在内的安全响应技术。

本书还介绍了计算机网络安全管理方面的基本内容和互联网网络基础设施安全的一些重点发展领域的现状，包括DNSSEC、IPsec和TLS过这些内容，可使读者掌握计算机网络(特别是计算机互联网络)安全的基本概念，了解设计和维护安全的网络及其应用系统的基本手段和常用方法。

本书可用作计算机专业本科生或研究生的教材，也可作为相关领域技术人员的参考书。

## &lt;&lt;计算机网络安全导论&gt;&gt;

## 书籍目录

第二版前言	第一章 计算机系统与网络的安全	1.1 计算机安全	1.1.1 基本概念	1.1.2 计算机系统的安全目标	1.1.3 计算机系统安全的主要内容	1.2 计算机系统的安全评估	1.2.1 安全保护等级	1.2.2 公共标准	1.2.3 风险评估	1.2.4 系统安全设计考虑	1.3 网络的安全威胁	1.3.1 网络的脆弱性	1.3.2 安全威胁分类	1.4 计算机网络的安全管理	1.4.1 系统的可生存性	1.4.2 网络安全管理的基本内容	1.4.3 网络安全规划	1.4.4 网络安全管理的实现	1.5 法律风险与规避	1.5.1 网络安全的法律风险	1.5.2 良好的行为规范	参考文献
习题	第二章 数据加密技术	2.1 概论	2.1.1 加密的概念	2.1.2 加密的基本方法	2.1.3 密码体制	2.1.4 加密系统的安全问题	2.2 分组加密	2.2.1 概述	2.2.2 DES	2.2.3 AES	2.2.4 大数据加密	2.3 序列加密	2.3.1 概述	2.3.2 序列密钥生成器	2.3.3 序列密码分析	2.4 非对称密码体制	2.4.1 概述	2.4.2 离散对数密码体制	2.4.3 RSA密码体制	2.4.4 椭圆曲线加密	参考文献	习题
	第三章 密钥管理技术	3.1 概论	3.1.1 密钥的组织结构	3.1.2 密钥管理的基本内容	3.2 密钥的分配技术	3.2.1 密钥分配中心(KDC)	3.2.2 Diffie-Hellman方法与桥接攻击问题	3.2.3 智能卡方法	3.2.4 组播密钥的分配	3.3 公开密钥的全局管理	3.3.1 基于X 509证书的公钥基础设施	3.3.2 X 509v3证书	3.3.3 X 509的证书撤销列表CRLv2	3.3.4 X509的存取操作	3.3.5 X 509的管理操作	3.3.6 PKI的实现	3.3.7 PGP的信任管理	参考文献	习题	第四章 数据完整性保护	4.1 信息摘录技术	4.1.1 概述.....
	第五章 数据鉴别保护	第六章 访问控制	第七章 网络入侵威胁	第八章 网络入侵检测	第九章 网络入侵防范	第十章 互联网的基础设施安全																

<<计算机网络安全导论>>

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>