

<<网络信息安全>>

图书基本信息

书名：<<网络信息安全>>

13位ISBN编号：9787562922032

10位ISBN编号：7562922039

出版时间：2005-1

出版时间：机械工业出版社

作者：陈月波 编

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>

## 前言

随着网络的开放性、共享性和互连程度的扩大，网络的重要性和对社会的影响也越来越大，同时网络上各种新业务的兴起，比如电子商务、电子现金、数字货币、网络银行、网上证券、网上理财以及网上保险等等，使得网络与信息系统的安全与保密问题显得越来越重要，成了关键之所在。

进入21世纪以来，我国的网络信息安全形势更加严峻，研究和解决我国的网络信息安全问题刻不容缓。

各个高校纷纷开设信息安全专业和有关课程，培养紧缺的信息安全专业人才。

本书针对当前高校开设的“网络信息安全”课程编写，可以用作本科以及高职高专信息安全、计算机和电子商务等相关专业的教材。

本书的总参考学时数控制在72课时范围内。

## <<网络信息安全>>

### 内容概要

《网络信息安全》分为9章，介绍了网络信息安全概述，网络安全技术，信息加密技术，数字签名与CA认证技术，防火墙技术，Internet安全技术，网络信息安全协议与安全标准，网络信息安全防范策略，最后介绍了网络信息安全法律等。

该书遵从高职高专教学规律，从网络信息安全基础出发，重点介绍了信息加密技术、数字签名与CA认证技术、防火墙技术、Internet安全技术，同时每章配有针对性的实验，具有较强的可操作性。

《网络信息安全》可以用作本科以及高职高专信息安全、计算机、电子商务等相关专业的教材，同样适合广大计算机网络与信息安全爱好者阅读参考。

## 书籍目录

1 网络信息安全概述1.1 信息安全基本概念1.1.1 信息安全1.1.2 信息安全技术1.2 网络信息安全及其体系结构1.2.1 网络信息安全概况1.2.2 网络信息安全概念1.2.3 网络信息安全的体系结构1.3 网络信息安全威胁1.3.1 网络信息安全威胁种类1.3.2 网络信息安全威胁的表现形式1.4 网络信息安全的基本要素1.5 网络信息安全技术1.6 网络信息安全的工作目的1.7 信息安全模型及其主要评价准则1.7.1 信息安全模型1.7.2 信息安全的主要评价准则2 网络安全技术2.1 网络安全概述2.1.1 计算机网络安全的概念2.1.2 计算机网络系统面临的威胁2.1.3 计算机网络系统的脆弱性2.1.4 计算机网络安全技术的研究内容和发展过程2.2 网络操作系统安全2.2.1 典型的网络操作系统2.2.2 网络操作系统安全的脆弱性2.2.3 网络操作系统的网络安全服务2.2.4 Unix / Linux操作系统安全2.3 防火墙技术2.3.1 概述2.3.2 防火墙的基本思想2.3.3 防火墙的种类及其采用的技术2.4 虚拟专用网 (VPN) 技术2.4.1 虚拟专用网概念及常识2.4.2 虚拟专用网工作原理2.4.3 虚拟专用网的功能及其分类2.4.4 VPN的基本要求和实现技术2.4.5 VPN技术的发展2.5 网络入侵检测2.5.1 入侵检测技术简介2.5.2 入侵检测技术应用2.5.3 构建一个入侵检测系统2.5.4 入侵检测系统的功能2.5.5 入侵检测系统的性能检测和分析2.5.6 入侵检测系统发展方向3 信息加密技术3.1 信息加密技术概述3.2 密码技术3.2.1 密码学基础知识3.2.2 传统密码技术3.2.3 数据加密标准DES3.2.4 RSA密码体制3.2.5 单向散列函数Hash3.2.6 密码技术的未来3.3 密钥管理3.3.1 密钥管理基础知识3.3.2 密钥生成3.3.3 密钥分配3.3.4 密钥托管3.4 网络加密技术3.4.1 网络加密的重要性3.4.2 网络加密的形式4 数字签名与CA认证技术4.1 数字签名的原理、种类与方法4.1.1 数字签名的概念4.1.2 数字签名的原理4.1.3 基于公钥密码数字签名的种类4.1.4 数字签名的方法与种类4.2 数字证书4.2.1 数字证书的工作原理4.2.2 证书的获取与管理4.2.3 验证证书4.3 身份认证技术4.3.1 身份认证的方法4.3.2 CA认证中心4.4 数字证书的申请4.4.1 上海市电子商务安全证书的数字证书的申请4.4.2 广东省交通行业虚拟CA数字证书办理流程4.5 PKI基础4.5.1 PKI概述4.5.2 PKI基础设施4.5.3 PKI的功能与性能4.5.4 PKI的基本组成4.5.5 PKI加密与签名原理4.5.6 PKI的应用4.5.7 Windows2000的PKI结构5 防火墙技术5.1 防火墙概述5.2 防火墙的设计和实现5.2.1 防火墙的主要设计思想5.2.2 防火墙的分类5.3 防火墙的安全体系结构5.3.1 防火墙与网络结构5.3.2 防火墙的选择原则5.3.3 防火墙安全体系的功能评估及维护5.4 防火墙的组合变化5.4.1 完整的防火墙应具备的功能5.4.2 防火墙的组合变化5.4.3 防火墙的安全策略5.5 典型防火墙产品与防火墙技术发展5.5.1 典型防火墙产品5.5.2 防火墙的发展趋势6 Internet安全技术6.1 Internet安全概述6.1.1 Internet的安全状况6.1.2 TCP / IP协议6.1.3 Internet服务的安全隐患6.1.4 Internet的安全问题及其原因6.2 FTP安全6.2.1 FTP概述6.2.2 FTP协议的安全问题6.2.3 FTP协议安全功能的扩展6.2.4 FTP服务器的安全实现6.2.5 匿名FTP安全漏洞及检查6.3 E-Mail安全6.3.1 E-Mail概述6.3.2 电子邮件服务的协议6.3.3 电子邮件攻击及安全防范6.3.4 电子邮件的保密方式6.3.5 E-Mail欺骗6.4 web安全6.4.1 Web站点的安全6.4.2 攻击Web站点的目的6.4.3 安全策略制定原则6.4.4 配置Web服务器的安全特性6.4.5 排除站点中的安全漏洞6.4.6 监视控制Web站点出入情况6.5 Proxy技术6.5.1 Proxy概述6.5.2 代理服务器的功能6.5.3 架设代理服务器7 网络信息安全协议与安全标准7.1 安全协议概述7.1.1 网络信息安全协议7.1.2 网络信息安全协议的种类7.1.3 网络信息安全协议的特点7.2 安全套接层协议 (SSL) 7.2.1 SSL安全协议概述7.2.2 SSL记录协议7.2.3 改变密码规范协议7.2.4 告警协议7.2.5 握手协议7.2.6 SSL协议的安全网络支付实践示例7.3 安全电子支付7.3.1 电子支付的安全问题7.3.2 网络支付的安全需求7.3.3 电子支付的安全策略及解决方法7.3.4 电子支付安全内容7.4 安全电子交易 (SET) 7.4.1 SET协议简介7.4.2 SET安全支付参与方及应用系统框架7.4.3 SET协议的安全电子支付流程7.4.4 SET协议机制的应用实例7.4.5 SET协议和SSL协议的比较8 网络信息安全防范策略8.1 信息安全策略8.2 安全防范策略概述8.2.1 制订安全防范策略的目的8.2.2 安全防范策略制订原则8.2.3 安全防范策略制订步骤8.2.4 安全防范策略的基本内容8.2.5 安全管理体系建设8.3 网络信息安全防范体系8.3.1 网络信息安全防范体系模型8.3.2 网络信息安全防范体系模型流程8.3.3 网络信息安全防范体系模型组成部分8.4 常见的网络攻击与防范8.4.1 网络攻击的具体步骤8.4.2 网络攻击的工作原理和手法8.4.3 攻击者常用的攻击工具8.4.4 针对网络攻击的防范和应对策略8.5 物理安全防范策略8.5.1 机房环境安全8.5.2 电磁防护8.5.3 硬件防护8.6 访问权限控制8.6.1 访问控制概述8.6.2 访问控制策略8.7 黑客攻击防范策略8.7.1 黑客攻击概述8.7.2 黑客攻击行为的特征分析与反攻击技术8.7.3 黑客攻击防范策略8.8 灾难恢复8.8.1 灾难恢复的概念8.8.2 制定灾难恢复计划的目的、目标与要求8.8.3 拟定灾难恢复计划的步骤9 网络信息安全

法律与法规9.1 网络信息安全法律概述9.1.1 互联网引起的法律问题9.1.2 网络犯罪的形式9.1.3 网络犯罪的特点9.2 我国网络信息安全立法状况附录1 中华人民共和国电子签名法附录2 计算机病毒防治管理办法附录3 中华人民共和国计算机信息系统安全保护条例参考文献

## 章节摘录

(1) 数字证书的格式数字证书作为网上身份证明的依据，其内容与格式遵循国际流行的x.509标准，由基本数据信息和发行数据证书的CA签名与签名算法两部分组成，主要包括以下内容： 版本信息（Version），用来区分x.509证书格式的版本； 数字证书序列号，每个证书的序列号是唯一的； 有效使用期限，包括起始和结束日期； 证书颁发者信息，包括颁发数字证书的单位及其数字签名； 证书与公钥的使用者的相关信息，包括证书拥有者的姓名和证书拥有者的公钥； 公钥信息，包括公开密钥加密体制的算法名称和公钥的有效期； 发行数字证书的CA签名与签名算法，用以验证数字证书是否是由该CA的签名密钥签署的，以保证证书的真实性与内容的真实性。

插图：

#### 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>