

<<网络信息安全原理>>

图书基本信息

书名：<<网络信息安全原理>>

13位ISBN编号：9787030258618

10位ISBN编号：7030258614

出版时间：2009-10

出版时间：梅挺 科学出版社 (2009-10出版)

作者：梅挺

页数：220

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>

## <<网络信息安全原理>>

### 前言

随着Internet的迅猛发展和信息社会的到来，网络已经影响到社会的政治、经济、文化、军事和社会生活的各个方面。

以网络方式获取信息或交流信息已成为现代信息社会的一个重要特征。

同时，随着人们对网络信息系统依赖的日益增强，网络正在逐步改变人们的工作方式和生活方式，成为当今社会发展的一个主题。

在人类进入信息化时代的今天，人们对信息的安全传输、安全存储、安全处理的要求越来越显得十分迫切和重要，它不仅关系到战争的胜负、国家的安危、科技的进步、经济的发展，而且也关系到每个人的切身利益。

但是，网络作为一把双刃剑，在加速人类社会信息化的同时，也给信息安全保障带来了极大的挑战。

网络犯罪事件已屡见不鲜，且呈逐年上升趋势。

特别，随着电子商务、电子现金、数字货币、网络银行等业务的兴起以及各种专用网（如金融网）的建设，伴随着这些业务产生的互联网和网络信息的安全问题，也已成为人们关注的热点问题。

当前，我国的网络安全正面临着严峻的挑战：一方面随着电子政务工程的启动，电子商务的开展以及国家关键基础设施的网络化，使得现有的网络安全设施建设日益滞后；另一方面，黑客入侵、病毒传播以及形形色色的网络攻击事件日益增多，且成功率一直居高不下，从侧面反映出广大网民的网络防护意识和网络安全知识的欠缺。

针对这种现状，作者在总结多年的实践经验和从事网络安全研究成果的基础上编写了本书。

网络安全技术是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

因此，网络安全研究的内容十分广泛，它涉及密码学理论、安全体系结构、安全协议、网络信息分析、网络安全监控、应急处理等，其中密码学理论是网络安全的关键技术。

本书全面阐述了网络安全原理和实践技术，主要包括：网络安全技术知识、密码技术、访问控制和防火墙技术、入侵检测与安全审计技术、黑客与病毒防范技术、操作系统安全技术、数据库系统安全技术等诸多知识。

## <<网络信息安全原理>>

### 内容概要

《网络信息安全原理》具有科学严谨的体系结构，内容丰富，深入浅出，构思新颖，突出实用，系统性强，并利用通俗的语言全面阐述网络安全原理与实践技术。  
《网络信息安全原理》可作为网络安全领域的科技人员与信息系统安全管理的参考用书，也可作为高等院校研究生教材使用。

## &lt;&lt;网络信息安全原理&gt;&gt;

## 书籍目录

第1章 网络信息安全概述1.1 网络信息安全基础知识1.1.1 网络信息安全的内涵1.1.2 网络信息安全的特征1.1.3 网络信息安全的关键技术1.1.4 网络信息安全分类1.1.5 网络信息安全问题的根源1.1.6 网络信息安全策略1.2 网络信息安全体系结构与模型1.2.1 ISO / OSI安全体系结构1.2.2 网络信息安全解决方案1.2.3 网络信息安全等级与标准1.3 网络信息安全管理体系(NISMS)1.3.1 信息安全管理体系定义1.3.2 信息安全管理体系构建1.4 网络信息安全评测认证体系1.4.1 网络信息安全度量标准1.4.2 各国测评认证体系与发展现状1.4.3 我国网络信息安全评测认证体系1.5 网络信息安全与法律1.5.1 网络信息安全立法的现状与思考1.5.2 我国网络信息安全的相关政策法规第2章 密码技术2.1 密码技术概述2.1.1 密码技术的起源、发展与应用2.1.2 密码技术基础2.1.3 标准化及其组织机构2.2 对称密码技术2.2.1 对称密码技术概述2.2.2 古典密码技术2.2.3 序列密码技术2.2.4 DES(数据加密标准)2.2.5 IDEA(国际数据加密算法)2.2.6 AES(高级加密标准)2.3 非对称密码技术2.3.1 非对称密码技术概述2.3.2 RSA算法2.3.3 Diffie-Hellman密钥交换协议2.3.4 ElGamal公钥密码技术2.3.5 椭圆曲线密码算法2.4 密钥分配与管理技术2.4.1 密钥分配方案2.4.2 密钥管理技术2.4.3 密钥托管技术2.4.4 PKI(公钥基础设施)技术2.4.5 PMI(授权管理基础设施)技术2.5 数字签名2.5.1 数字签名及其原理2.5.2 数字证书2.5.3 数字签名标准与算法2.6 信息隐藏技术2.6.1 信息隐藏技术原理2.6.2 数据隐写术(Steganography)2.6.3 数字水印第3章 访问控制与防火墙技术3.1 访问控制技术3.1.1 访问控制技术概述3.1.2 访问控制策略3.1.3 访问控制的常用实现方法3.1.4 WindowsNT / 2K安全访问控制手段3.2 防火墙技术基础3.2.1 防火墙概述3.2.2 防火墙的类型3.3 防火墙安全设计策略3.3.1 防火墙体系结构3.3.2 网络服务访问权限策略3.3.3 防火墙设计策略及要求3.3.4 防火墙与加密机制3.4 防火墙攻击策略3.4.1 扫描防火墙策略3.4.2 通过防火墙认证机制策略3.4.3 利用防火墙漏洞策略3.5 第四代防火墙的主要技术3.5.1 第四代防火墙的主要技术与功能3.5.2 第四代防火墙技术的实现方法3.5.3 第四代防火墙抗攻击能力分析3.6 防火墙发展的新方向3.6.1 透明接入技术3.6.2 分布式防火墙技术3.6.3 以防火墙为核心的网络信息安全体系3.7 防火墙选择原则与常见产品3.7.1 防火墙选择原则3.7.2 常见产品第4章 入侵检测与安全审计4.1 入侵检测系统概述4.1.1 入侵检测定义4.1.2 入侵检测的发展及未来4.1.3 入侵检测系统的功能及分类4.1.4 入侵响应(IntrusionResponse)4.1.5 入侵跟踪技术4.2 入侵检测系统(IDS)的分析方法4.2.1 基于异常的人侵检测方法4.2.2 基于误用的入侵检测方法4.3 入侵检测系统(IDS)结构4.3.1 公共入侵检测框架(CIDF)模型4.3.2 简单的分布式入侵检测系统4.3.3 基于智能代理技术的分布式入侵检测系统4.3.4 自适应入侵检测系统4.3.5 智能卡式入侵检测系统实现4.3.6 典型入侵检测系统简介4.4 入侵检测工具简介4.4.1 日志审查(Swatch)4.4.2 访问控制(TCPwrapper)4.4.3 Watcher检测工具4.5 现代安全审计技术4.5.1 安全审计现状4.5.2 安全审计标准CC中的网络信息安全审计功能定义4.5.3 分布式入侵检测和安全审计系统S\_Audit简介第5章 黑客与病毒防范技术5.1 黑客及防范技术5.1.1 黑客原理5.1.2 黑客攻击过程5.1.3 黑客防范技术5.1.4 特洛伊木马简介5.2 病毒简介5.2.1 病毒的概念及发展史5.2.2 病毒的特征及分类5.3 病毒检测技术5.3.1 病毒的传播途径5.3.2 病毒检测方法5.4 病毒防范技术5.4.1 单机环境下的病毒防范技术5.4.2 小型局域网的病毒防范技术5.4.3 大型网络的病毒防范技术5.5 病毒防范产品介绍5.5.1 病毒防范产品的分类5.5.2 防杀计算机病毒软件的特点5.5.3 对计算机病毒防治产品的要求5.5.4 常见的计算机病毒防治产品第6章 操作系统安全技术6.1 操作系统安全概述6.1.1 操作系统安全的概念6.1.2 操作系统安全的评估6.1.3 操作系统的安全配置6.2 操作系统的安全设计6.2.1 操作系统的安全模型6.2.2 操作系统安全性的设计方法及原则6.2.3 对操作系统安全性认证6.3 Windows系统安全防护技术6.3.1 Windows2000Server操作系统安全性能概述6.3.2 Windows2000Server安全配置6.4 Unix / Linux操作系统安全防护技术6.4.1 Solaris系统安全管理6.4.2 Linux安全技术6.5 常见服务的安全防护技术6.5.1 WWW服务器的安全防护技术6.5.2 Xinetd超级防护程序配置6.5.3 SSH(SecureShell)程序第7章 数据库系统安全技术7.1 数据库系统安全概述7.1.1 数据库系统安全简介7.1.2 数据库系统的安全策略与安全评估7.1.3 数据库系统安全模型与控制7.2 数据库系统的安全技术7.2.1 口令保护技术7.2.2 数据库加密技术7.2.3 数据库备份与恢复技术7.3 数据库的保密程序及其应用7.3.1 Protect的保密功能7.3.2 Protect功能的应用7.4 Oracle数据库的安全7.4.1 Oracle的访问控制7.4.2 Oracle的完整性7.4.3 Oracle的并发控制7.4.4 Oracle的审计追踪

## &lt;&lt;网络信息安全原理&gt;&gt;

## 章节摘录

插图：安全策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则。实现网络安全，不但要靠先进的技术，而且也得靠严格的管理、法律约束和安全教育，主要包括以下内容： 威严的法律：安全的基石是社会法律、法规和手段，即通过建立与信息安全相关的法律和法规，使不法分子慑于法律，不敢轻举妄动。

先进的技术：先进的技术是信息安全的根本保障，用户对自身面临的威胁进行风险评估，决定其需要的安全服务种类。

选择相应的安全机制，然后集成先进的安全技术。

严格的管理：各网络使用机构、企业和单位应建立相应的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。

网络安全策略是一个系统的概念，它是网络安全系统的灵魂与核心，任何可靠的网络安全系统都是构架在各种安全技术集成的基础之上，而网络安全策略的提出，正是为了实现这种技术的集成。

可以说网络安全策略是我们为了保护网络安全而制定的一系列法律、法规和措施的总和。

当前制定的网络安全策略主要包含5个方面的策略。

1.物理安全策略物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件设备和通信链路免受自然灾害、人为破坏和搭线攻击；验证用户的身份和使用权限，防止用户越权操作；确保计算机系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非法进入计算机控制室和各种盗劫、破坏活动的发生。

2.访问控制策略访问控制策略是网络安全防范的主要策略，它的主要任务是保证网络资源不被非法使用和访问。

它也是维护网络系统安全、保护网络资源的重要手段。

各种安全策略必须相互配合才能真正起到安全保护作用，但访问控制可以说是保证网络安全最重要的核心策略之一。

它主要由入网访问控制、网络权限控制、目录级安全控制、属性安全控制、网络服务安全控制、网络检测和锁定控制及网络端口和节点的安全控制组成。

入网访问控制：入网访问控制为网络访问提供了第一层访问控制。

它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许他们在哪台工作站入网。

用户的入网访问控制可分为三个步骤：用户名的识别与验证；用户口令的识别与验证；用户帐号的缺省限制检查。

三个关卡中只要任何一关未过，该用户便不能进入该网络。

网络的权限控制：网络的权限控制是针对网络非法操作所提出的一种安全保护措施。

用户和用户组被赋予一定的权限。

网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源。

可以指定用户对这些文件、目录、设备能够执行哪些操作。

我们可以根据访问权将用户分为：特殊用户（系统管理员）、一般用户和审计用户。

## <<网络信息安全原理>>

### 编辑推荐

《网络信息安全原理》由科学出版社出版。

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>