

《信息安全理论、技术与应用基础》

图书基本信息

书名：《信息安全理论、技术与应用基础》

13位ISBN编号：9787111245124

10位ISBN编号：7111245121

出版时间：2008-8

出版社：傅予力,向友君,徐向民、傅予力、向友君、徐向民 机械工业出版社 (2008-08出版)

页数：154

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

前言

信息社会的兴起，给全球带来了信息技术飞速发展的契机；信息技术的应用，引起了人们生产方式、生活方式和思想观念的巨大变化，极大地推动了人类社会的发展和人类文明的进步。今天随着人类进入知识经济时代，网络和信息已逐渐成为人们从事社会活动的基本工具。但是，由于计算机和网络系统的开放性带来的信息与网络的安全问题也拓展到前所未有的程度。日益增多的对以计算机网络为载体的信息系统的非法入侵和破坏活动正以惊人的速度在全世界蔓延，给各国信息系统带来巨大的经济损失和安全威胁。面对严重的网络与信息安全隐患，迫切要求提高全民的安全防范意识，加大信息化安全保障体系，加速培养网络与信息安全的专门人才。重视信息安全已成为全社会的共识，研究网络信息安全的现状、规律和发展，研究信息安全基本理论、安全基础设施、安全技术与应用以及安全政策和管理，正是编写本书的出发点。本书具有如下特点：1.内容涵盖更全面完善的知识体系结构本书主要内容涵盖信息安全理论、安全技术、安全管理以及安全应用实践几个主体部分，整体内容的组织参考了目前国内外主流信息安全教育知识体系框架（如CISSP、CISP等），注重整体内容体系的完整性和系统性，更加适合于在校本科生的信息安全基础教学。2.注重信息安全理论、技术与实践的有机结合考虑到信息安全自身是一个不断实践不断发展的领域，因此本书在内容组织上非常注重信息安全理论、技术和相关应用实践的相结合，分别从理论、技术、应用三个层面来介绍信息安全。除了介绍各种密码学编解码理论算法、风险管理理论等信息安全基础理论外，还介绍了防火墙技术、病毒检测防护技术、入侵检测技术、漏洞扫描技术、VPN技术、身份认证技术等主流安全技术领域，进而结合现阶段国内外信息安全领域的实际发展现状，对各种安全设备产品、安全技术应用、安全管理实践等信息安全应用情况以及发展趋势进行介绍。因此，本教材非常便于初入门者从理论、技术和实践多个层面去学习和理解信息安全，有助于达到理论与实践有效结合的良好效果。3.将安全技术和安全管理相结合“三分技术七分管理”是信息安全领域的一个重要原则，因此，将安全技术与安全管理两方面内容进行结合也是本书特色。本书除了对目前各种主流安全技术手段的实现原理、实现方式以及应用实施等内容从技术的角度进行重点介绍外，还对各种安全管理理论、信息安全保障模型，以及风险评估、安全管理最佳实践等近年来的一些安全管理领域热点进行介绍，有助于读者更全面地理解信息安全，从而更好地帮助读者在入门阶段就对信息安全学科树立正确的认识观点。4.内容紧密结合信息安全领域发展现状考虑到信息安全“动态性”的特点，本书在内容选材方面紧密结合信息安全领域现阶段的发展状况，尤其对某些热门技术领域的技术发展和实施手段、对一些最新的主流信息安全实践、对现阶段一些主流安全厂商的安全产品发展现状等方面内容进行了介绍，从而使得读者对当前国内外信息安全领域的现状以及今后的发展趋势有一个全面的了解和清晰的把握。本书得以出版是众多人员的努力和支撑的结果。这里首先感谢王金炜、沈文超、彭超、王崇波、韩雨、任永杰、黎瑞瑜、陈敏聪等同学，他们对本书的完稿做了大量工作。本书由傅予力负责修改和定稿，并编写第1 - 5章，向友君负责本书第6 - 12章的编写，徐向民负责第13 - 16章的编写。在本书的策划和编写过程中，参阅了国内外诸多专家学者的文献和资料，对他们表示由衷的感谢。

前言 信息安全理论、技术与应用基础本书可作为高等院校信息安全、通信、计算机等专业本科生和研究生的教材，也可供从事网络信息安全技术工作的广大科技人员和计算机用户参考。由于网络与信息安全是一门发展很快的学科，新的理论、技术和方法、新的应用不断出现，本书的选材还有一些不尽如人意的地方，加上笔者学识水平和时间所限，书中难免存在各种错误和疏漏，敬请广大读者给予批评指正，以便进一步完善提高。编者

《信息安全理论、技术与应用基础》

内容概要

《信息安全理论.技术与应用基础》共16章。第1-4章为理论基础，主要讨论了网络信息安全的基础知识，包括信息安全概论、密码学理论基础、信息网络基础理论等内容；第5-15章为技术基础，较详细地讨论了网络信息安全中涉及的各种技术，包括加解密、防火墙、病毒防护、反垃圾邮件、入侵检测、漏洞扫描、虚拟专用网、身份认证、数据备份、安全审计、操作系统安全等内容；第16章，简单介绍了网络安全实践中当前主流的一些产品及其技术特点。《信息安全理论.技术与应用基础》可作为高等院校信息安全、通信、信号处理、计算机等专业本科生和研究生的教材，也可供从事网络信息安全技术工作的广大科技人员和计算机用户参考。

前言第1章 信息安全概述 1.1 信息安全背景 1.2 信息中的各种安全隐患 1.3 信息安全威胁分析 1.3.1 网络安全面临的威胁 1.3.2 来自外部的安全威胁分析 1.3.3 来自内部的安全威胁分析 1.3.4 信息病毒威胁 1.4 安全策略 1.5 信息安全保障体系 1.5.1 安全保障体系的组成 1.5.2 ISO/OSI安全体系结构 1.6 信息安全的主要技术概述 1.6.1 加解密与PKI技术 1.6.2 防火墙技术 1.6.3 病毒防护技术 1.6.4 反垃圾邮件技术 1.6.5 漏洞扫描技术 1.6.6 身份认证技术 1.6.7 数据备份技术 第2章 密码学基础理论 2.1 密码学基础 2.1.1 安全原则 2.1.2 基本概念 2.1.3 对称密码与非对称密码体制 2.1.4 密码分析的攻击类型 2.2 对称密码体制 2.2.1 概述 2.2.2 数据加密标准DES 2.2.3 国际数据加密算法IDEA 2.2.4 高级数据加密标准AES算法 2.2.5 对称密码体制的密钥交换问题 2.3 非对称（公钥）密码 2.3.1 公钥密码思想 2.3.2 RSA公钥密码体制 2.3.3 椭圆曲线密码体制 2.3.4 对称与非对称密钥加密 2.4 认证理论与技术 2.4.1 概述 2.4.2 单向Hash函数 2.4.3 数字签名 2.5 应用密码学的应用实例 2.5.1 PGP简介 2.5.2 SSL简介 2.5.3 Kerberos简介 2.5.4 IPSec简介 第3章 信息安全管理基础理论 3.1 信息安全管理概述 3.2 信息安全管理的重要性 3.3 如何实现信息安全管理 3.4 信息安全管理体系BS7799 3.5 风险评估 第4章 信息网络基础理论 4.1 信息网络 4.1.1 通信网络 4.1.2 计算机网络 4.1.3 网络应用 4.2 信息系统开发 4.2.1 目标系统分析与信息分析 4.2.2 系统设计与系统建设 4.3 多媒体通信 4.3.1 多媒体概念 4.3.2 多媒体通信的特点 4.3.3 多媒体通信网络 4.4 信息产业化 第5章 加解密与PKI技术 5.1 PKI概述 5.2 PKI的标准及体系结构 5.2.1 PKI的标准 5.2.2 PKI的体系结构 5.2.3 数字证书 5.3 PKI的应用与发展 5.3.1 PKI的应用 5.3.2 PKI的发展 第6章 防火墙技术 6.1 防火墙的简介 6.2 防火墙的体系结构及工作原理 6.3 防火墙的安全控制技术 6.4 防火墙的工作模式 6.5 防火墙的应用与发展 6.6 防火墙的技术指标 第7章 病毒防护技术 7.1 概述 7.1.1 计算机病毒的定义及其特点 7.1.2 计算机病毒的种类 7.1.3 计算机病毒的发展 7.2 计算机病毒的工作机理 7.2.1 引导型病毒 7.2.2 文件型病毒 7.2.3 混合型病毒 7.2.4 宏病毒 7.2.5 网络病毒 7.3 计算机病毒的防范 7.3.1 计算机病毒的传播途径 7.3.2 计算机病毒检测技术 7.3.3 计算机病毒的技术预防措施 7.4 企业构建防病毒体系 7.4.1 企业网络病毒感染及传播途径 7.4.2 企业网络防病毒解决方案 7.4.3 防病毒产品选择依据 7.5 防病毒技术展望 第8章 反垃圾邮件技术 8.1 垃圾邮件的概述 8.2 电子邮件的工作原理 8.3 垃圾邮件的生命周期 8.4 当前主要的反垃圾邮件技术 8.5 反垃圾邮件的管理 第9章 入侵检测技术 9.1 入侵检测系统概述 9.1.1 入侵检测系统定义 9.1.2 入侵检测系统的功能 9.2 入侵检测系统工作原理 9.2.1 入侵检测系统分类 9.2.2 入侵检测系统工作原理分析 9.2.3 主要的入侵检测技术 9.3 入侵检测技术的应用——防火墙与入侵检测技术的结合 9.4 入侵检测系统技术展望 第10章 漏洞扫描技术 10.1 漏洞扫描技术原理概述 10.2 漏洞的危害和产生原因 10.3 基于网络的漏洞扫描 10.4 基于主机的漏洞扫描 10.5 基于网络的漏洞扫描与基于主机的漏洞扫描的优缺点 10.6 漏洞扫描工具简介 10.7 漏洞扫描技术中存在的问题 第11章 VPN技术 11.1 VPN概述 11.2 VPN的主要技术 11.3 与VPN有关的几种主要协议 11.4 VPN组网方式和实现方式 11.5 VPN服务的特点 11.6 选用VPN方案时应注意的问题 11.7 VPN发展状况及趋势 第12章 身份认证技术 12.1 身份认证技术概述 12.2 传统身份认证体系 12.2.1 实例理解 12.2.2 几种主要的身份鉴别模型 12.3 常见身份鉴别技术 12.3.1 Kerberos认证技术 12.3.2 PAP&CHAP认证 12.3.3 一次性口令认证 12.3.4 RADIUS认证 12.3.5 X.509数字证书 12.3.6 生物特征识别技术 12.4 身份鉴别技术展望 第13章 数据备份与恢复技术 13.1 数据备份与恢复技术概述 13.2 数据备份技术 13.2.1 数据备份体系结构 13.2.2 备份策略 13.2.3 备份方式 13.2.4 备份管理 13.3 数据复制与恢复技术 13.3.1 数据复制方式 13.3.2 数据复制的形式 13.3.3 数据复制的模式 13.3.4 复制选择 第14章 网络安全审计 14.1 网络安全审计概述 14.2 安全审计系统组成 14.3 安全审计系统功能 14.4 安全审计当前面临的威胁 14.5 安全审计实例 14.5.1 系统安全审计——Windows的安全审计 14.5.2 网络系统安全审计 14.6 基于信息融合的安全审计 14.7 网络安全审计的创新 14.7.1 网络环境下的审计数据采集技术 14.7.2 审计分析技术 14.7.3 实时审计报告 第15章 操作系统安全技术 15.1 操作系统安全概述 15.1.1 操作系统安全的重要性 15.1.2 操作系统安全性设计的一般原则 15.1.3 操作系统安全的几个常用术语 15.2 Windows系统安全技术 15.2.1 Windows NT/2000的安全模型 15.2.2 Windows NT/2000的登录、访问控制 15.2.3 Windows NT/2000的安全管理 15.2.4 Windows注册表 15.2.5 Windows 2000/XP的一些安全配置 15.3 Linux/Unix系统安全技术 15.3.1 Linux身份验证 15.3.2 Linux的文件访问控制 15.3.3 Linux的审计和日志系统 15.3.4 Linux系统安全配置 第16章 网络信息安全产品 参考文献

章节摘录

插图：第1章 信息安全概述1.1 信息安全背景20世纪40年代，随着计算机的出现，计算机安全问题也随之产生。随着计算机在社会各个领域的广泛应用和迅速普及，使人类社会步入信息时代，以计算机为核心的安全、保密问题越来越突出。20世纪70年代以来，在应用和普及的基础上，以计算机信息为主体的信息处理系统迅速发展，计算机应用也逐渐向信息化发展。集通信、计算机和信息处理于一体的信息系统，是现代社会不可缺少的基础。计算机应用发展到信息化阶段后，信息安全技术得到迅速发展，原有的计算机安全问题增加了许多新的内容。同以前的计算机安全保密相比，计算机信息安全技术的问题要多得多，也复杂得多，涉及到物理环境、硬件、软件、数据、传输、体系结构等各个方面。除了传统的安全保密理论、技术及单机的安全问题以外，计算机信息安全技术包括了计算机安全、通信安全、访问控制的安全，以及安全管理和法律制裁等诸多内容，并逐渐形成独立的学科体系。换一个角度讲，当今社会是一个信息化社会，计算机通信在政治、军事、金融、商业、交通、电信、文教等方面的作用日益增大。社会对计算机信息的依赖也日益增强，尤其是计算机技术和通信技术相结合所形成的信息基础设施已经成为反映信息社会特征最重要的基础设施。人们建立了各种各样完备的信息系统，使得人类社会的一些机密和财富高度集于计算机中。但是这些信息系统都是依靠计算机接受和处理信息，实现其相互间的联系和对目标的管理、控制。以信息方式获得信息和交流信息已成为现代信息社会的一个重要特征。随着信息的开放性、共享性及互联程度的扩大，特别是Internet网的出现，信息的重要性和对社会的影响也越来越大。随着信息上各种新业务的兴起，比如电子商务（Electronic Commerce）、电子现金（Electronic Cash）、数字货币（Digital Cash）、信息银行（Network Bank）等的兴起，以及各种专用网（例如金融网等）的建设，使得安全问题显得越来越重要，因此对信息安全的研究成了现在计算机和通信界的一个热点。

《信息安全理论、技术与应用基础》

编辑推荐

《信息安全理论.技术与应用基础》由机械工业出版社出版。

《信息安全理论、技术与应用基础》

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:www.tushu111.com