<<计算机安全原理与实践>>

图书基本信息

书名：<<计算机安全原理与实践>>

13位ISBN编号：9787111241492

10位ISBN编号：7111241495

出版时间：2008-7

出版时间：机械工业出版社

作者：William Stallings,Lawrie Brown

页数：510

译者：贾春福,刘春波

<<计算机安全原理与实践>>

内容概要

本书系统介绍计算机安全领域中的各个方面，不但包括相关的技术和应用方面的内容，同时还包括管理方面的内容。
本书共分六个部分：第一部分计算机安全技术与原理，概述支持有效安全策略所必需的技术领域；第二部分软件安全，包括软件开发和运行中的安全问题；第三部分管理问题，主要讨论信息与计算机安全在管理方面的问题；第四部分密码编码算法，包括各种类型的加密算法和其他类型的密码算法；第五部分Internet安全，关注的是为在Internet上进行通信提供安全保障的协议和标准；第六部分操作系统安全，详细讨论两种广泛使用的操作系统Windows(包含最新的Vista)与Linux的安全方法。
此外，各章后面都有一定数量的习题和思考题供读者练习，以加深对书中内容的理解。
同时，各章后面还附上了一些极有价值的参考文献和Web站点。
本书覆盖面广，叙述清晰，可作为高等院校计算机安全课程的教材，同时也是一本有关密码学和计算机网络安全方面的非常有价值的参考书。

作者简介

William Satllings，拥有美国麻省理工学院计算机科学博士学位，现任教于澳大利亚新南威尔士大学国防学院（堪培拉）信息技术与电子工程系。
他是世界知名计算机学者和畅销教材作者，已经撰写了17部著作，出版了40多本书籍，内容涉及计算机安全、计算机网络和计算机体系结构

<<计算机安全原理与实践>>

书籍目录

出版者的话译者序前言作者简介符号第0章 阅读指南 0.1 本书概览 0.2 阅读方案 0.3 Internet和Web资源 0.4 标准第1章 概述 1.1 计算机安全概念 1.2 威胁、攻击和资产 1.3 安全功能需求 1.4 开放系统的安全体系结构 1.5 计算机安全范畴 1.6 计算机安全发展趋势 1.7 计算机安全策略 1.8 推荐的读物和Web站点 1.9 关键术语、思考题和习题 附录1A 重要的安全标准和文献第一部分 计算机安全技术与原理 第2章 密码编码工具 第3章 用户认证 第4章 访问控制 第5章 数据库安全 第6章 入侵检测 第7章 恶意软件 第8章 拒绝服务攻击 第9章 防火墙与入侵防护系统 第10章 可信计算与多级安全第二部分 软件安全 第11章 缓冲区溢出 第12章 软件安全第三部分 管理问题 第13章 物理和基础设施安全 第14章 人为因素 第15章 安全审计 第16章 IT安全管理与风险评估 第17章 IT安全控制、计划和实施程序 第18章 IT安全中的法律与道德问题第四部分 密码编码算法 第19章 对称加密和消息认证 第20章 公钥密码和消息认证第五部分 Internet安全 第21章 Internet安全协议和标准 第22章 Internet认证应用 第23章 Linux安全 第24章 Windows和Windows Vista安全附 录 附录A 数论的相关内容 附录B 随机数与伪随机数的生成 附录C 密码学和网络安全教学项目

章节摘录

第0章　阅读指南本书及与本书相关的Web站点涵盖了很多学习资料。
这里我们将给读者做一个概括性的介绍。
0.1　本书概览本书共分为六个部分：第一部分（计算机安全技术与原理）：这一部分涵盖了有效安全策略所涉及的技术领域。
第2章列举了一些重要的密码算法，讨论了它们的使用及强度问题。
该部分剩余的章节则涉及其他特定的计算机安全技术领域：认证、访问控制、数据库安全、入侵检测、恶意软件、拒绝服务、防火墙、可信计算与多级安全等。
第二部分（软件安全）：这一部分主要涉及操作系统、实用软件和应用软件的开发和实现。
第11章讨论长期存在的缓冲区溢出问题，第12章则分析了一些其他的软件安全问题。
第三部分（管理问题）：这一部分主要涉及信息与计算机安全在管理方面的问题。
第13章专注于物理安全的方法，是对第一部分技术方法实现安全的必要补充。
第14章分析了与计算机安全相关的各种人为因素问题。
一个重要的管理工具是安全审计，安全审计在第15章中进行了探讨。
第16章和第17章涉及与风险评估相关的管理实践，具体内容包括管理计算机安全的安全控制、计划和实施程序的建立。
第18章探讨了与计算机安全有关的法律和道德方面的内容。
第四部分（密码编码算法）：许多支持计算机安全的技术措施，主要依靠的是各种类型的加密和其他类型的密码编码算法。
第四部分就是对这些算法的一个技术性概述。
第五部分（Internet安全）：这一部分关注为Internet上进行通信提供安全保障的协议和标准。
第21章讨论Internet上使用的一些最为重要的安全协议。
第22章涉及与Internet认证相关的各种标准和协议。
第六部分（操作系统安全）：这一部分详细地讨论了两种广泛使用的操作系统Windows（包含最新的Vista）与Linux的安全策略。
在操作系统安全策略的实现项目中，以这两个操作系统作为研究实例。
第六部分后的附录部分涵盖了与本书相关的其他专题。
本书网站上的在线附录也涵盖了其他相关的专题。

<<计算机安全原理与实践>>

编辑推荐

《计算机安全原理与实践》系统地介绍了计算机安全领域中的各个方面，全面分析了计算机安全威胁、检测与防范安全攻击的技术方法以及软件安全问题和管理问题。
《计算机安全原理与实践》重点介绍核心原理，揭示了这些原理是如何将计算机安全领域统一成一体的，并说明了它们在实际系统和网络中的应用。
此外，《计算机安全原理与实践》还探讨了满足安全需求的各种设计方法，阐释了对于当前安全解决方案至关重要的标准。
《计算机安全原理与实践》思路清晰，结构严谨，并且提供了扩展的教学支持——数百个精心设计的实践问题，是高等院校计算机安全专业的理想教材，同时也可作为研究人员和专业技术人员的非常有价值的参考书。
《计算机安全原理与实践》主要内容：●安全技术和原理，包括密码编码技术、认证以及访问控制。
●威胁及其对策，从检测入侵者到应对DoS攻击。
●可信计算与多级安全。
●安全软件：避免缓冲区溢出、恶意输入和其他弱点。
●Linux和Windows安全模型。
●管理安全：物理安全、培训、审计和策略等。
●计算机犯罪、知识产权、隐私和道德。
●密码算法，包括公钥密码体制。
●Internet安全：SSL、TLS、IP安全、S/MIME、Kerberos、X.509以及联合身份管理。

<<计算机安全原理与实践>>

版权说明