

<<信息安全>>

图书基本信息

书名：<<信息安全>>

13位ISBN编号：9787302180999

10位ISBN编号：7302180997

出版时间：2008-10

出版时间：清华大学出版社

作者：（美）梅柯，（美）布莱特普特 著

页数：312

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>

<<信息安全>>

内容概要

《信息安全：原理与实践》以国际信息系统安全认证联盟制定的知识体系为背景，首先概述了信息安全的基本原则和概念，然后介绍了信息安全的公共知识体系，而且提供了该体系10个知识范畴的概况：安全管理，安全架构与模型，业务持续计划和灾难恢复计划，法律、调查与道德规范，操作安全，访问控制系统与方法论，密码学和电信、网络以及Internet安全。

《信息安全：原理与实践》适用于高等院校计算机及相关专业的本科生和教师、从事信息安全方面的专业人员。

作者简介

Mark Merkow获得了CISSP和CISM认证。
他和他公司的CIO办公室一同致力于建立用于金融管理和设施的IT安全策略。
其中所含的金融设施包括信用卡、银行业以及证券产品和服务。
Mark是ANSIX9F委员会代表，曾和国家标准与技术研究所（National Institute of Standards and Technology，NIST）紧密合作“通用安全准则的测试与评估方法论”研究。

<<信息安全>>

书籍目录

第1章 为什么研究信息安全1.1 导言1.2 增长的IT安全重要性与新的职业机会1.2.1 政府和私营工商业的持续需求1.3 成为信息安全专家1.3.1 应运而生的教育机构51.3.2 综合学科研究法1.4 信息安全的环境1.4.1 信息安全职业——业务安全的需要1.5 本章小结1.6 技能测试1.6.1 多项选择题1.6.2 练习题1.6.3 项目题1.6.4 案例研究第2章 信息安全的成功原则2.1 导言2.2 原则1：没有绝对的安全2.3 原则2：安全三目标——私密性、完整性和可用性2.3.1 完整性模型2.3.2 可用性模型2.4 原则3：部署安全分层机制2.5 原则4：人们容易自行做出最糟的安全决定2.6 原则5：决定计算机安全的两项需求——功能性需求与保险性需求2.7 原则6：模糊性不是安全的解决之道2.8 原则7：安全=风险管理2.9 原则8：安全控制的三种类型：预防型控制、探测型控制和响应型控制2.10 原则9：复杂性是安全性的大敌2.11 原则10：担忧、不确定性、疑惑对销售安全没用2.12 原则11：必要的人、流程、技术是系统或设施安全的保障2.13 原则12：公开已知的漏洞有助于安全2.14 本章小结2.15 技能测试2.15.1 多项选择题2.15.2 练习题2.15.3 项目题2.15.4 案例研究第3章 认证计划与公共知识体系3.1 导言3.2 信息安全及其认证3.2.1 国际信息系统安全认证联盟信息安全——原理与实践3.3 信息安全的公共知识体系（CBK）3.3.1 安全管理实务3.3.2 安全体系结构和模型3.3.3 业务持续性计划3.3.4 法律、调查和道德3.3.5 物理安全3.3.6 操作安全3.3.7 访问控制系统和方法3.3.8 密码学3.3.9 电信、网络和Internet安全3.3.10 应用开发安全3.4 其他安全认证项目3.4.1 注册信息系统审计师（CISA）3.4.2 注册信息安全员（CISM）3.4.3 全球信息保证证书（GIAC）3.4.4 CompTIA Security+认证3.4.5 针对供应商的认证3.5 本章小结3.6 技能测试3.6.1 多项选择题3.6.2 练习题3.6.3 项目题3.6.4 案例研究第4章 安全管理第5章 安全架构与模型第6章 业务持续计划和灾难恢复计划第7章 法律、调查与道德规范第8章 物理安全控制第9章 操作安全第10章 访问控制体系和方法论第11章 密码学第12章 通信、网络和Internet安全第13章 应用开发的安全性第14章 未来的安全性的未来附录A 公共知识体系附录B 安全策略和标准分类附录C 策略样本附录D 安全策略和标准管理系统内幕附录E HIPAA安全规则 and 标准

章节摘录

第1章 为什么研究信息安全 **本章目标** 通过阅读本章与完成章末的习题，应该掌握如下内容： 认识到在IT（Information Technology）业中，信息安全专家日益增长的重要性，以及信息安全业如何成为收入可观的行业。

制定投身信息安全职业的战略。

理解在一定商业背景下的信息安全需求和内涵。

1.1 导言 随着网络化的计算机技术数十年的快速进步和Internet的惊人扩张，公众愈加关注网络犯罪对个人隐私的威胁。

偷窃身份、盗版银行账户、伪造，这一连串的电子化犯罪，正如犯罪分子恶意运用计算机技术的想象力一般——不可限量。

由于Internet使用方便，计算机网络的开放，客户和业务越多，公众越容易遭受精明但居心不良的网络罪犯的攻击。

为了对计算机、网络以及其中存储的信息进行保密，各个组织机构纷纷寻求信息安全专家的帮助。

信息安全专家不仅仅是狙击黑客攻击网站的技术人员。

实际上，你将惊讶地了解到，信息安全学科既是商业管理的坚实基础，也是对密码学以及防火墙技术（用于保障信息系统的两项技术）的综合。

本书将审视理论及实践中的技巧，但首先，我们先回答大多数学员开始该领域学习的第一个问题：为什么要研究信息安全？

1.2 增长的IT安全重要性与新的职业机会 在首席信息官（Chief Information Officer，CIO）看来，信息安全是要保护数据私密性、完整性以及可用性，以免数据被意外抑或故意误用。

信息安全学科包含技术与非技术性的两个方面，用以降低信息系统越来越多地使用开放架构的风险。

也就是说，组织对客户、商业伙伴以及员工开放越来越多的系统内部细节时，它们也将自身置身于更大的黑客攻击风险中。

如银行对客户开通网上支票或信用卡交互业务，也就开启了伪造好像是来自于该银行的电子邮件的攻击的魔盒。

这些伪装来自于银行的电子邮件，巧妙地收集用户访问网上银行的ID号与密码。

一旦ID与密码被获取，银行客户就会吃惊地获悉，他们的账户莫名其妙地被洗劫一空。

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>