

<<信息安全技术与实施>>

图书基本信息

书名：<<信息安全技术与实施>>

13位ISBN编号：9787121118807

10位ISBN编号：7121118807

出版时间：2010-10

出版时间：电子工业出版社

作者：武春岭 编

页数：274

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>

## <<信息安全技术与实施>>

### 前言

随着科学技术的迅猛发展和信息技术的广泛应用，特别是我国国民经济和社会信息化进程的全面加快，网络与信息系统的基础性、全局性作用日益增强，信息安全已经成为国家安全的重要组成部分。近年来，在党中央、国务院的领导下，我国信息安全保障工作取得了明显成效，建设了一批信息安全基础设施，加强了互联网信息内容安全管理，为维护国家安全与社会稳定、保障和促进信息化健康发展发挥了重要作用。

但是，我国信息安全保障工作仍存在一些亟待解决的问题：网络与信息系统的防护水平不高，应急处理能力不强；信息安全管理和技术人才缺乏，关键技术整体上还比较落后，产业缺乏核心竞争力；信息安全法律法规和标准不完善；全社会的信息安全意识不强，信息安全管理薄弱等。

与此同时，网上有害信息传播、病毒入侵和网络攻击日趋严重，网络泄密事件屡有发生，网络犯罪呈快速上升趋势，境内外敌对势力针对广播电视卫星、有线电视和地面网络的攻击破坏活动和利用信息网络进行的反动宣传活动日益猖獗，严重危害公共利益和国家安全，影响了我国信息化建设的健康发展。

随着我国信息化进程的逐步推进，特别是互联网的广泛应用，信息安全还将面临更多新的挑战。

## <<信息安全技术与实施>>

### 内容概要

本书作为信息安全知识普及与技术推广教材，涵盖信息安全概念、信息安全防御模型、信息安全法律法规、信息安全物理防御技术、网络攻防技术、密码技术、防火墙技术、入侵检测技术、操作系统安全技术和无线网安全技术等多方面的内容。

不仅能够为初学信息安全技术的学生提供全面、实用的技术和理论基础，而且能有效培养学生信息安全的防御能力。

本书的编写融入了作者丰富的教学和企业实践经验，内容安排合理，每个章节都从“引导案例”开始，首先让学生知道通过本章学习能解决什么实际问题，做到有的放矢，激发学生的学习热情，使学生更有目标地学习相关理念和技术操作，最后针对“引导案例”中提到的问题给出解决方案，使学生真正体会到学有所用。

整个章节围绕一个主题——案例，从问题提出(引导案例)到问题解决(案例实现)，步步为营、由浅入深，结构严谨、浑然天成。

此外，每章还配有习题和实训，不仅可以巩固理论知识，而且也为技能训练提供了基础。

本书可以作为高职高专计算机信息类专业的教材，也可以作为企事业单位网络信息系统管理人员的技术参考用书，同时也适合趋势科技TCSP认证证书培训使用。

## <<信息安全技术与实施>>

### 书籍目录

第1章 信息安全概述 引导案例 1.1 信息安全介绍 1.1.1 信息安全的概念 1.1.2 信息安全的内容 1.1.3 信息安全策略 1.1.4 信息安全的要素 1.2 黑客的概念及黑客文化 1.2.1 黑客的概念及起源 1.2.2 黑客文化 1.2.3 如何成为一名黑客 1.3 针对信息安全的攻击 1.3.1 被动攻击 1.3.2 主动攻击 1.4 网络安全体系 1.4.1 网络安全体系的概念 1.4.2 网络安全体系的用途 1.4.3 网络安全体系的组成 1.4.4 网络安全体系模型发展状况 1.5 信息安全的三个层次 1.5.1 安全立法 1.5.2 安全管理 1.5.3 安全技术措施 习题 .....第2章 物理实体安全与防护第3章 网络攻击与防范第4章 密码技术与应用第5章 数字身份认证第6章 防火墙技术与应用第7章 入侵检测技术与应用第8章 计算机病毒与防范第9章 操作系统安全防范第10章 无线网安全与防范参考文献

## &lt;&lt;信息安全技术与实施&gt;&gt;

## 章节摘录

插图：(2) 机密性。

机密性是指网络中的信息不被非授权实体（包括用户和进程等）获取与使用。

这些信息不仅指国家机密，也包括企业和社会团体的商业秘密和工作秘密，还包括个人的秘密（如银行账号）和个人隐私（如邮件、浏览习惯）等。

网络在人们生活中的广泛使用，使人们对网络机密性的要求提高。

用于保障网络机密性的主要技术是密码技术。

在网络的不同层次上有不同的机制来保障机密性。

在物理层上，主要是采取电磁屏蔽技术、干扰及跳频技术来防止电磁辐射造成的信息外泄；在网络层、传输层及应用层主要采用加密、路由控制、访问控制、审计等方法来保证信息的机密性。

(3) 完整性。

完整性是指网络信息的真实可信性，即网络中的信息不会被偶然或者蓄意地进行删除、修改、伪造、插入等破坏，保证授权用户得到的信息是真实的。

只有具有修改权限的实体才能修改信息，如果信息被未经授权的实体修改了或在传输过程中出现了错误，信息的使用者应能够通过一定的方式判断出信息是否真实可靠。

(4) 可控性。

是控制授权范围内的信息流向和行为方式的特性，如对信息的访问、传播及内容具有控制能力。

首先，系统要能够控制谁能够访问系统或网络上的数据，以及如何访问，即是否可以修改数据还是只能读取数据。

这要通过采用访问控制等授权方法来实现。

其次，即使拥有合法的授权，系统仍需要对网络上的用户进行验证。

通过握手协议和口令进行身份验证，以确保他确实是所声称的那个人。

最后，系统还要将用户的所有网络活动记录在案，包括网络中计算机的使用时间、敏感操作和违法操作等，为系统进行事故原因查询、定位，事故发生前的预测、报警，以及为事故发生后的实时处理提供详细、可靠的依据或支持。

审计对用户的正常操作也有记载，可以实现统计、计费等功能，而且有些诸如修改数据的“正常”操作恰恰是攻击系统的非法操作，同样需要加以警惕。

## <<信息安全技术与实施>>

### 编辑推荐

《信息安全技术与实施》：涵盖信息安全防御模型、物理防御技术、网络攻防技术、防火墙技术、入侵检测技术和无线网安全技术等内容寓工作任务于章名、集工作任务于案例、涵技能干理论讲解、表能力于案例实现，有效培养学生信息安全综合能力

<<信息安全技术与实施>>

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>