

<<信息安全>>

图书基本信息

书名：<<信息安全>>

13位ISBN编号：9787560963495

10位ISBN编号：7560963498

出版时间：2011-1

出版时间：华中科技大学出版社

作者：胡爱群，宋宇波，蒋睿 等编著

页数：244

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

胡爱群、宋宇波和蒋睿合编的《信息安全》全面介绍了信息安全的基本理论与技术，包括信息安全概论、对称密码、公钥密码与数字签名、模式识别在信息安全中的应用、计算机病毒、黑客与远程攻击、信息隐藏与数字水印、可信计算与系统安全保护等方面，涵盖面广，适合信息安全专业教学的需要。

《信息安全》可作为高等院校信息安全专业本科生的教材，也可作为硕士生的科研辅导书和其它相关专业的教学、科研和工程技术人员参考书。

<<信息安全>>

书籍目录

第1章信息安全概论

1.1 信息系统及其信息安全问题概述

1.2 信息系统安全保障模型

1.3 信息安全的法制环境

1.4 本书的教学范围

参考文献

习题

第2章对称密码算法

2.1 前言

2.2 古典密码

2.3 乘积密码

2.4 DES算法

2.5 AES算法

2.6 SMS4算法

2.7 分组密码算法的加密模式

2.8 流密码

2.9 小结

参考文献

习题

第3章公钥密码、数字签名与身份证明

3.1 公钥密码算法

3.2 RSA密码系统

3.3 RSA算法

3.4 数字签名

3.5 消息摘要

3.6 身份证明理论

参考文献

习题

第4章模式识别及其在信息安全中的应用

4.1 绪论

4.2 统计模式识别

4.3 模式识别在信息安全中的应用

参考文献

习题

第5章计算机病毒

5.1 计算机病毒概述

5.2 计算机病毒工作原理

5.3 病毒触发机制

5.4 典型计算机病毒

5.5 病毒的防范与清除

5.6 常见杀毒软件

参考文献

习题

第6章黑客与远程攻击

6.1 黑客

<<信息安全>>

6.2 远程攻击与防范

6.3 IP欺骗攻击与防范

6.4 木马攻击与防范

6.5 缓冲区溢出攻击与防范

6.6 拒绝服务攻击

参考文献

习题

第7章信息隐藏与数字水印

7.1 信息隐藏概述

7.2 空间域信息隐藏技术

7.3 变换域信息隐藏技术

7.4 数字水印

参考文献

习题

第8章可信计算与信息系统安全防护

8.1 可信的概念与模型

8.2 可信计算平台体系结构

8.3 可信体系中的安全算法

8.4 可信体系中的安全协议

8.5 可信运行机制

8.6 可信移动平台TMP

8.7 小结

参考文献

习题

章节摘录

版权页：插图：研究信息安全问题也就是研究信息在采集、处理、存储或传输过程中面临的安全保障问题。

信息系统是信息的依存环境，是采集、处理、存储或传输信息的系统。

因此，信息系统本身的安全也就成为安全保障的重点。

《信息保障技术框架（IATF）》定义了对一个信息系统进行信息保障的过程，以及该系统中软件和硬件部分的安全要求，涉及保护网络基础设施、飞地边界、计算环境及支撑性基础设施四个方面。

其中网络基础设施是指服务器、路由器、交换机等网络节点，主要用来传输和保存信息；飞地边界是指网络或信息系统与外界的连接边界，它是信息进出网络的关口；计算环境是指计算机和服务器等信息处理系统；而支撑性基础设施是指保障网络信息系统正常运行的支撑系统，如网络管理系统、密钥管理系统、远程备份系统等。

信息系统的安全威胁很多，攻击类型也各种各样。

但总的来说，可以归结为如下五类攻击。

（1）被动攻击是指通过拦截网络流量，对其进行分析，从而获取信息。

例如，通过截获网络上的数据包，识别和提取出电子邮件，进行分析和解密，获取用户的信息。

这种攻击通常在网络的飞地边界以外进行。

（2）主动攻击是指通过发现协议和系统的漏洞，渗透到用户信息系统中，盗取信息、更改数据，甚至使系统不能提供正常服务等。

这种攻击通常采用远程攻击的方法进行。

（3）物理临近攻击是指攻击者接近实际的信息系统设备，进入实际系统工作环境，寻找可以攻击的手段。

<<信息安全>>

编辑推荐

《信息安全》：全国普通高等院校电子信息与通信类精品教材

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>