<<信息安全原理与应用>>

图书基本信息

书名：<<信息安全原理与应用>>

13位ISBN编号：9787121098871

10位ISBN编号：7121098873

出版时间：2010-1

出版时间：电子工业出版社

作者：王昭，袁春　编著

页数：317

前言

信息安全是一门跨学科跨专业的综合性学科，它涵盖了非常丰富的内容，涉及数论、密码编码、信息论、通信、网络、编程等多方面的知识，无论是从事管理，还是技术研发的人员，甚至普通的计算机用户，都需要从不同层次和角度了解这方面的基本知识。
并且随着信息技术的发展，信息安全新技术新思想不断涌现。
此外，它还是一门理论与实际紧密结合的学科。
本书主要是以作者多年来在北京大学讲授信息安全、应用密码学等课程讲义为基础编写而成的。
编写中，我们力求做到内容的系统、完整和深入浅出，理论与实际的结合，原理的经典性和技术的先进性。
信息安全问题的解决方案可以分为两类，一类是以密码编码为基础的解决方案，另一类是和密码无关的一些解决方案。
本书尽可能全面地涵盖这两类原理和技术，主要内容安排如下：第1章介绍了ISO 7498—2定义的OSI的五大类安全服务：数据机密性、数据完整性、不可否认性、鉴别和访问控制。
本书以经典的通信安全模型和信息访问安全模型为线索，介绍了这五大类安全服务。
第2～5章以密码分析和密码编码相结合的思路，比较完整地介绍了密码编码学的基本原理和算法实现，包括：古典密码、现代对称密码、公钥密码和散列函数。
密码算法都以国际上经典的标准或最新的标准为例。
在原理介绍的基础上，第6章和第7章讨论了密码算法实际应用中的一些问题，包括：密钥长度、密钥管理、硬件加密和软件加密，以及算法应用中曾经出现的教训等。
第8章、第10章和第11章介绍了密码编码的相关综合应用，包括鉴别协议、安全电子邮件和网络安全协议，其中的内容都以最新的RFC文档和相关文献资料为参考。
第9章和第12～15章主要讨论了与密码算法无关的安全解决方案，包括访问控制、防火墙技术、黑客攻击与防范技术、计算机病毒防治和入侵检测技术。
第16章介绍了信息安全的一些标准化情况，包括信息安全的标准化机构和有关标准。
最后，第17章介绍了一个综合应用信息安全有关原理的实例——数据库系统安全。
在相关章节后附有一些加深理论理解的难易程度不同的思考和练习题、实践／实验题，以帮助读者更深入和扎实地掌握相关知识。
根据编者经验，主要内容的课堂讲授需要50学时左右，也可根据教学对象和教学目标进行删减，建议根据课程内容再安排一定学时的课外实践／实验。
在本书的编写过程中，查阅和参考了大量文献资料，限于篇幅未能在书后的参考文献中一一列出，在此一并致谢。

<<信息安全原理与应用>>

内容概要

本书涉及密码编码与网络安全从技术到管理的方方面面，以数据机密性、数据完整性、不可否认性、鉴别和访问控制五大类安全服务和安全模型为线索，介绍了信息安全的基本原理。
以密码编码与密码分析相结合的思路，比较完整地介绍了密码编码学的基本原理和算法实现，包括：古典密码、现代对称密码、公钥密码和散列函数，并讨论了密码算法实际应用中的一些问题，如密钥长度、密钥管理、硬件加密和软件加密，以及算法应用中曾经出现的教训等。
在此基础上，介绍了相关综合应用，包括电子邮件的安全、网络安全协议和数据库安全。
在网络安全与系统安全方面讨论了网络入侵与攻击、入侵检测、防火墙和计算机病毒防范。
此外也介绍了信息安全的一些标准化情况，包括标准化机构和信息安全的评估标准。
本书不仅介绍网络安全的基本原理，更注重理论与实际的结合，在相关章节后附有一些加深理论理解的难易程度不同的思考练习题和实践／实验题。

本书可作为信息类专业高年级本科生和研究生教材，也可以为信息安全、计算机、通信和电子工程等领域研究和开发人员提供有益的帮助和参考。

<<信息安全原理与应用>>

书籍目录

章节摘录

插图：欧洲经济共同体（欧盟的前身）是一个在欧洲范围内具有较强影响力的政府间组织。
其成员国从20世纪70年代末到80年代初，先后制定并颁布了各自有关数据安全的法律。
德国政府于1996年夏出台了《信息和通信服务规范法》（即多媒体法），为电子信息和通信服务的各种利用可能性规定了统一的基本法律框架。
该国政府还通过了电信服务数据保护法，并根据需要对刑法法典、治安法、传播危害青少年文字法、著作权法和报价法做了必要的修改和补充。
新加坡在1996年宣布对互联网络实行管制，宣布实施分类许可证制度。
它是一种自动取得许可证的制度，目的是鼓励正当使用互联网络，促进其健康发展。
其他国家，如英国、法国、日本等也制定了相应的计算机安全政策法规。
关于密码使用的政策涉及使用密码进行加密和进行数字签名实施证书授权管理两个方面。
美国是最早允许在国内社会使用密码的国家，美国国内，政府、军界、企业和个人为了各自的利益，围绕信息加密政策的争论繁多，主要是密码的使用范围和允许出口的长度。
此外，多国出口控制协调委员会（COCOM）、欧盟和国际商务委员会等组织以及英国、法国、德国、意大利、俄罗斯、波兰、澳大利亚、中国香港地区等许多国家和地区也分别制定了自己的信息加密政策。
对于数字签名技术，有关国际组织、各国政府和企业为了各自的利益，很难达成一致观点。
1995年，美国犹他州通过了美国历史上（也是世界历史上）第一部数字签名法。
在犹他州的带动下，美国的其他一些州也确立了自己的数字签名法，但是美国联邦政府迟迟没有立法，德国有幸成为第一个以国家名义制定数字签名法的国家。
1.6.2 国内信息安全政策法规我国建立了如下国家信息安全组织管理体系：国务院信息化领导小组
对Internet安全中的重大问题进行管理协调，国务院信息化领导小组办公室作为Internet安全工作的办事机构，负责组织、协调和制定有关Internet安全的政策、法规和标准，并检查监督其执行情况。
政府有关信息安全的其他管理和执法部门（如工业和信息化部、国家安全部、公安部、国家保密局、国家密码管理局和国务院新闻办公室等）分别依据其职能和权限进行信息安全的管理和执法活动。
工业和信息化部协调有关部委关于信息安全的工作；公安部主管公共网络安全，即全国计算机系统安全保护工作；国家安全部主管计算机信息网络国际联网的国家安全保护管理工作；国家保密局主管全国计算机信息系统的保密工作；国家密码管理委员会主管密码算法与设备的审批和使用工作；国务院新闻办公室负责信息内容的监察。
我国信息安全管理的基本方针是“兴利除弊，集中监控，分级管理，保障国家安全”。
对于密码的管理政策实行“统一领导、集中管理、定点研制、专控经营、满足使用”的发展和管理方针。
相对国外网络立法已成普及之势的情况，我国目前的信息化立法，尤其是信息安全立法，尚处于起步阶段，我国政府和法律界都清醒地认识到这一。
问题的重要性，正在积极推进这一方面的工作。

<<信息安全原理与应用>>

编辑推荐

《信息安全原理与应用》在国家规划教材的基础上，进行全面更新，以适应高校课程与教学改革的需要，并特别注意教材的可读性和可用性。
为任课教师提供各种教学服务（包括教学电子课件、教学指导材料、习题解答和实验指导等）。
北京市高等教育精品教材立项项目网络工程与信息安全

<<信息安全原理与应用>>

版权说明