高等学校计算机科学与技术教材

信息安全概论

石志国　贺也平　赵　悦　编著

清 华 大 学 出 版 社
北京交通大学出版社
·北京·

内 容 简 介

本书系统介绍了信息安全学科的内容。本书与同类书籍相比，大大提高了实践部分的比例，全书理论与实践的比例约为6:4，并引用大量的经典例子，注重提高学习信息安全的趣味性与知识性及授课的生动性。

全书从信息安全研究层次角度分成4部分，共11章。第一部分：信息安全基础，介绍信息安全学的基本概念及安全的评价标准。第二部分：密码学基础，介绍信息加密与密码分析、认证及密钥管理技术。第三部分：网络安全技术，介绍PKI公钥基础设施原理、防火墙与入侵检测技术、IP安全与Web安全，以及简单介绍了典型攻击技术。第四部分：系统与应用安全技术，介绍安全操作系统理论、恶意代码与病毒机制、可信计算的基本概念及信息安全法律与法规。

本书可作为高等学校和各类培训机构相关课程的教材或参考书。本书提供全书源代码，以及涉及的所有软件和授课幻灯片等教学支持信息，读者可以从图书支持网站http://www.gettop.net下载，也可以从北京交通大学出版社网站http://press.bjtu.edu.cn的下载栏目中下载。

图书在版编目(CIP)数据

信息安全概论/石志国，贺也平，赵悦编著. —北京：清华大学出版社；北京交通大学出版社，2007.6
(高等学校计算机科学与技术教材)
ISBN 978－7－81082－998－4

Ⅰ.信…　Ⅱ.①石…　②贺…　③赵…　Ⅲ.信息系统－安全技术－高等学校－教材　Ⅳ.TP309

中国版本图书馆CIP数据核字(2007)第056547号

责任编辑：谭文芳
出版发行：清华大学出版社　邮编：100084　电话：010－62776969　http://www.tup.com.cn
　　北京交通大学出版社　邮编：100044　电话：010－51686414　http://press.bjtu.edu.cn
印 刷 者：北京东光印刷厂
经　　销：全国新华书店
开　　本：185×260　印张：18　字数：458千字
版　　次：2007年6月第1版　2007年6月第1次印刷
书　　号：ISBN 978－7－81082－998－4/TP·348
印　　数：5000册　定价：29.00元

前　言

信息安全学是一门新兴的学科，2004 年成为一门正式的本科专业，目前已经成为很多科研机构和大专院校的一个重要研究领域。信息安全概论需要全面阐述该学科目前的发展层次，研究内容和最新的发展方向。本书对信息安全学科内容进行整体介绍，根据信息安全学目前最新发展重新规划学科的内容及各部分比重。

信息安全学是一门实践性很强的学科，本书除了对相关理论进行全面讲解外，还通过具体的实验、例子等更加具体形象地化解理论的枯燥和繁杂。本书的整体定位是教材，书后提供大量习题，因此也可以同时作为相关考试的参考书。为了方便使用，提高质量，本书提供完整的教学大纲及教案等辅助资料。

目前很多信息安全教程理论性很强，这样接受起来相对比较困难。本书把理论知识和实验实践结合讲解，注重提高学习信息安全的趣味性与知识性，以及授课的生动性。

全书从信息安全研究层次角度分成 4 部分，共 11 章。

第一部分：信息安全基础

第 1 章 信息安全概述：介绍信息安全的学科内容、研究层次及安全威胁。研究信息安全的社会意义，相关道德标准及黑客行为学研究内容。

第二部分：密码学基础

第 2 章 信息加密与密码分析：介绍密码学的基本概念、加密类型，混合加密方法以及消息一致性。并介绍加密领域中两种主流加密技术：DES 加密和 RSA 加密。

第 3 章 认证与密钥管理技术：介绍哈希函数的分类与 MD5 的基本算法、常用的身份识别技术、电子 ID 身份识别和个人特征身份识别，以及密钥管理技术与管理系统。

第三部分：网络安全技术

第 4 章 PKI 公钥基础设施原理：介绍 PKI/CA 模型的构成、RSA 算法在 PKI/CA 中的应用、PKI 策略、PKI 的规划和建设，以及 CA 的应用。

第 5 章 防火墙与入侵检测技术：介绍防火墙的基本概念、分类、实现模型，以及如何利用软件实现防火墙的规则集；介绍入侵检测系统的概念、原理，以及如何利用程序实现简单的入侵系统。

第 6 章 IP 安全与 Web 安全：介绍 IPSec 的必要性，IPSec 中的 AH 协议和 ESP 协议、密钥交换协议 IKE 以及 VPN 的解决方案等。

第 7 章 典型攻击技术简介：介绍常用的网络入侵技术，包括社会工程学攻击、物理攻击、暴力攻击、漏洞攻击及缓冲区溢出攻击等。

第四部分：系统与应用安全技术

第 8 章 安全操作系统：介绍安全操作系统的基本概念、实现机制，安全模型及安全体系结构。

第 9 章 恶意代码与病毒：介绍恶意代码的发展史，恶意代码长期存在的原因，介绍恶意代

码实现机理、定义及攻击方法等。

第 10 章 可信计算简介：介绍可信计算的发展历史、可信计算的设计目标、可以计算的基本规范、可信计算中使用的密钥和信任状、平台配置寄存器 PCR 的原理及可信计算中信任状验证方式

第 11 章 信息安全法律法规与管理：介绍世界范围内的信息安全法规内容、国际相关法律法规现状与特点、相关政策法规的现状及特点；部分相关法律法规简介、立法方面存在的问题及信息安全犯罪案例分析。

总的来说，本书具有如下的特点。

⑴ 注重培养理论水平和实践能力。针对所讲述的理论知识提供直观的试验或者实例，涉及的实例或者试验，都具有很高的实用价值。

⑵ 总体上讲解信息安全的层次。适应目前计算机教学的需要。并对重要知识点进行详细的讲解，使之成为一本适合教学和自学的图书，本书浅显易懂、循序渐进、适合教学的需要。

⑶ 每章提供本章要点，小结。并全面地提供课后习题。习题包括：选择、填空、简答题和程序设计题目等，并在书后给出部分习题答案。

在本书的编写过程中，得到众多老师的指导和帮助。在此感谢中科院软件所卿斯汉研究员、淮晓永副教授、程光瑶老师、蒋建春老师、周辉老师、于文卫老师、张东帆老师、王秀利老师、张宏博士和金洁华工程师；感谢清华大学计算机系林闯主任、尹浩副教授；感谢北京科技大学王志良教授、徐正光教授、解仑副教授和王莉副教授；感谢中央广播电视大学崔林教授，徐孝凯教授、田萧老师和王春凤老师；感谢中国软件行业协会邱钦伦高级工程师。尤其要感谢的是北京交通大学出版社的编辑谭文芳老师，她的支持是本书能顺利出版的关键。感谢众多老师和同学们的支持，他们的每一个问题，都是本书要强调并解决的知识点，他们的认可是我最大的动力，本书献给你们，献给最广大的读者。

本书可以作为高等学校和各类培训机构相关课程的教材或者教学参考书，也可作为信息安全自学人员和信息安全开发人员的参考书。本书提供完整的教学幻灯片，书中的所有软件和源代码及相关学习资源，将在 http://www.gettop.net 或者 http://press.bjtu.edu.cn 下载栏目中发布，欢迎访问和下载。

由于作者水平和时间有限，难免出现错误，对于本书的任何问题请使用 E-mail 发送到作者邮箱：shizhiguo@tom.com。

石志国
2007 年 5 月

目　　录

第一部分　信息安全基础

第二部分　密码学基础

第三部分 网络安全技术

第四部分　系统与应用安全技术

第一部分

信息安全基础

第 1 章　信息安全概述

本章要点

- 信息的定义和信息技术的研究内容
- 信息安全的学科内容、研究层次和安全威胁
- 研究信息安全的社会意义、相关道德标准和黑客行为学研究内容
- 信息安全评价标准

1.1　信息技术的概念

信息是人类社会必需的重要资源，信息安全是社会稳定安全的必要条件。信息是一切生物进化的导向资源，信息是知识的来源、是决策的依据、是控制的灵魂、是思维的材料、是管理的基础。

1.1.1　信息的定义

信息是一种以特殊的物质形态存在的实体，1928 年哈特莱（L. V. R. Hartley）认为信息是选择通信符号的方式，且用选择自由度来计量这种信息的大小。1948 年，美国数学家香农（C.E.Shannon）认为信息是用来减少随机不定性的东西。1948 年，维纳（N.Wiener）认为信息是人们在适应外部世界和这种适应反作用于外部世界的过程中，与外部世界进行互相交换的内容的名称。1975 年，意大利学者朗高（G. Longo）认为信息反映了事物的形式、关系和差别，它包含在事物的差异之中，而不在事物本身。1988 年，我国信息论专家钟义信教授在《信息科学原理》一书中，把信息定义为事物的运动状态和状态变化的方式，并通过引入约束条件推导了信息的概念体系，对信息进行了完整和准确的描述。

信息不同于消息，消息是信息的外壳，信息则是消息的内核。信息不同于信号，信号是信息的载体，信息则是信号所载荷的内容。信息不同于数据，数据是记录信息的一种形式，同样的信息也可以用文字或图像来表述。当然，在计算机里，所有的多媒体文件都是用数据表示的，计算机和网络上信息的传递都是以数据的形式进行，此时信息等同于数据。

信息最基本的特征是信息来源于物质，又不是物质本身；它从物质的运动中产生出来，又可以脱离源物质而寄生于媒体物质，相对独立地存在。信息是具体的，并且可以被人（生物、机器等）所感知、提取、识别，可以被传递、储存、变换、处理、显示检索和利用。信息的基本功能在于维持和强化世界的有序性，维系着社会的生存，促进人类文明的进步和人类自身的发展。

1.1.2　信息技术的概念

人类的一切活动都可以归结为认识世界和改造世界。从信息的观点来看，人类认识世界

和改造世界的过程，就是一个不断从外部世界的客体中获取信息，并对这些信息进行变换、传递、存储、处理、比较、分析、识别、判断、提取和输出，最终把大脑中产生的决策信息反作用于外部世界的过程。现代（大体从 20 世纪中期算起）人类所利用的表征性资源是信息资源，表征性的科学技术是信息科学技术，表征性的工具是智能工具。

信息技术（Information Technology）是指在计算机和通信技术支持下用以获取、加工、存储、变换、显示和传输文字、数值、图像、视频、音频及语音信息，并且包括提供设备和信息服务两大方面的方法与设备的总称。也有人认为信息技术简单地说就是 3C，Computer（计算机）、Communication（通信）和 Control（控制），即 IT = Computer + Communication + Control。

1.2　信息安全的概念

信息安全学关注信息本身的安全，而不管是否应用了计算机作为信息处理的手段。信息安全的任务是保护信息财产，以防止偶然的或未授权者对信息的恶意泄露、修改和破坏，从而导致信息的不可靠或无法处理等。这样可以使得我们在最大限度地利用信息为我们服务的同时而不招致损失或使损失最小。

信息安全可以分为数据安全和系统安全。信息安全可以分成两个层次。

从消息层次来看，包括信息的完整性（Integrity），即保证消息的来源、去向、内容真实无误；保密性（Confidentiality），即保证消息不会被非法泄露扩散；不可否认性（Non-repudiation），也称为不可抵赖性，即保证消息的发送和接受者无法否认自己所做过的操作行为。

从网络层次来看，包括可用性（Availability），即保证网络和信息系统随时可用，运行过程中不出现故障，若遇意外打击能够尽量减少并尽早恢复正常；可控性（Controllability）是对网络信息的传播及内容具有控制能力的特性。

1.2.1　信息安全学科内容

信息安全是一门交叉学科。广义上，信息安全涉及多方面的理论和应用知识，除了数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学。狭义上，也就是通常说的信息安全，只是从自然科学的角度介绍信息安全的研究内容。信息安全各部分研究内容及相互关系如图 1-1 所示。

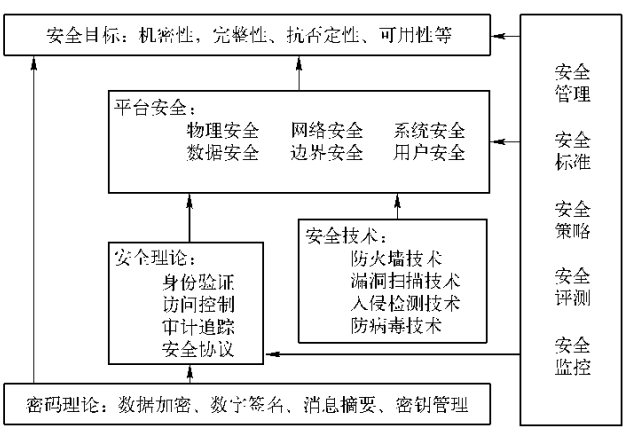

图 1-1　信息安全研究内容及关系