<<信息安全理论与技术>>

图书基本信息

书名：<<信息安全理论与技术>>

13位ISBN编号：9787560624396

10位ISBN编号：7560624391

出版时间：2010-8

出版时间：西安电子科技大学出版社

作者：李飞，陈艾东，王敏　编著

页数：282

字数：430000

前言

“ 信息安全理论与技术 ”课是计算机科学技术、网络工程、通信工程和信息安全专业本科生的专业基础必修课程。
一般情况下课程安排2.5 ～3个学分，学时从32个学时到48个学时不等。
但是“ 信息安全理论与技术 ”这门课程不仅要介绍信息安全学科相关的理论知识，还要介绍信息安全技术和信息安全管理体系，内容较多。
因此，在教学上必须采取一些措施，才能完成大纲要求的教学任务。
目前国内大多数高校推行先进的工程教育理念，如CDl0工程教育理念，但许多工科学生有一个通病，即重技术轻理论。
如何结合工程教育理念来教育学生，使他们明白，理论是基础，技术只是理论指导下的实现手段，没有理论作指导，技术无法达到一定的高度，这是摆在教师面前的一个巨大问题。
解决不了这个问题，将无法教育出优秀的学生，也无法成为一个优秀的教育者。
具体到“ 信息安全理论与技术 ”这门课程来说，首先要使学生明白系统的概念，这就要求学生能将前面先修的课程，如数学相关课程以及“ C语言程序设计 ”、“ 数据结构 ”、“ 操作系统原理 ”和“ 计算机网络 ”等课程的理论，与本课程有关理论知识贯穿起来，同时在讲解“ 信息安全体系结构 ”相关内容时，使学生明白仅仅一种信息安全技术是无法完成系统安全保障要求的，要有一个系统的概念，即在管理制度约束下，在信息安全相关理论指导下，将多种技术集成，才能构成一个系统安全的保障体系。
没有系统的思维，单靠一门技术会给系统留下巨大的隐患。
在讲解信息安全理论时，教师要注意理论的承前启后，强调理论指导技术的重要性，让学生明白利用技术做设计时，没i有理论作指导，是无法完成好的设计和实现的。
在学习方法上，可以预先给学生布置讲述的内容，让学生预习，分组讨论，然后请学生代表在课堂作总结，教师和学生共同点评，培养学生的表达能力、团队协作能力以及发现问题和解决问题的能力。
这样，通过一门课程的教学，可以完成工程教育理念所要求的培养学生的目标。

<<信息安全理论与技术>>

内容概要

本书介绍信息安全的基本概念、方法和技术，详细讲解了信息安全的基础知识、信息安全模型、当代主流的密码技术、访问控制技术、数字签名和信息认证技术、安全审计与监控技术、网络攻防技术、病毒及防范技术、信息安全体系结构以及各种安全服务及安全机制，为今后进一步学习与研究信息安全理论与技术或者从事计算机网络信息安全技术与管理工作奠定理论和技术基础。
教材内容涵盖了信息安全的理论、技术与管理三大体系，有助于学生信息安全整体解决理念的形成。

本书可以作为计算机网络安全类课程的相关教材，还可以作为电子商务专业本科生相关课程的教材。

<<信息安全理论与技术>>

书籍目录

章节摘录

插图：网络安全所涉及的领域相当广泛。
因为目前的公用通信网络中存在各种各样的安全漏洞和威胁。
从广义上讲，凡是涉及到网络上信息的保密性、完整性、可用性和可控性等的相关技术和理论，都是网络安全所要研究的领域。
网络安全，从本质上讲就是网络上信息的安全，即网络上信息保存、传输的安全，指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。
从用户（个人、企业等）的角度来说，他们希望所涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免他人或对手利用窃听、冒充、篡改和抵赖等手段对用户的利益和隐私造成损坏和侵犯，同时也希望当用户的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。
从网络运行和管理者的角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现病毒、非法存取、拒绝服务和网络资源的非法占用及非法控制等威胁，制止和防御网络“黑客”的攻击。
从安全保密部门的角度来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免其通过网络泄露，防止由于这类信息的泄露对社会产生危害，给国家造成巨大的经济损失，甚至威胁到国家安全。
从社会教育和意识形态的角度来说，网络上不健康的内容会对社会的稳定和人类的发展形成阻碍，必须对其进行控制。
由此，网络安全应包含四层含义：（1）运行系统安全，即保证信息处理和传输系统的安全，本质上是保护系统的合法操作和正常运行，包括计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的安全性考虑，硬件系统的可靠安全运行，计算机操作系统和应用软件的安全，电磁信息泄露的防护等。
它侧重于保证系统的正常运行，避免因系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免因电磁泄露产生信息泄露、干扰他人（或受他人干扰）。
（2）网络上系统信息的安全，包括用口令鉴别、用户存取权限控制、数据存取权限、方式控制、安全审计、安全问题跟踪、计算机病毒防治、数据加密等。
（3）网络上信息传播的安全，即信息传播后的安全，包括信息过滤技术。
它侧重于防止和控制非法、有害的信息进行传播后所带来的不良后果；避免公用通信网络上大量自由传输的信息失控，其本质上是维护道德、法规法则或国家利益。
（4）网络上信息内容的安全，侧重于网络信息的保密性、真实性和完整性；避免攻击者利用系统的安全漏洞进行窃听、冒充和诈骗等有损用户利益的行为，本质上是保护用户的利益和隐私。
。
由此可见，网络安全与其所保护的信息对象有关，本质上是信息的安全期内保证其在网络上流动时或静态存储时不被非法用户所访问，但授权用户可以访问。
因此，网络安全的结构层次包括：物理安全、安全控制和安全服务。

编辑推荐

《信息安全理论与技术》是高等学校计算机类专业规划教材。

版权说明