普通高等学校信息与计算科学专业系列丛书

教育科学“十五”国家规划课题研究成果

信息安全基础

徐茂智　编著

高等教育出版社
HIGHER EDUCATION PRESS

信息安全基础

普通高等学校信息与计算科学专业系列丛书

教育科学“十五”国家规划课题研究成果

信息安全基础

徐茂智　编著

高等教育出版社

内容简介

本书介绍信息安全事先防护理论和技术的基础知识，不追求大而全，而把目标确定为使学生学到结构化的知识和对信息安全有一个系统的了解。全书由基本概念、基本算法、基础密码协议、安全模型、应用技术和基础设施共六章组成。前四章为本书的重点，内容包括基本概念、基本算法与模型的详细讨论。第五章对繁杂的实用技术进行了介绍，主要包括 Web 安全、数据库安全、电子交易安全三个重要的应用技术的介绍，而对操作系统安全、数据库安全、病毒防护、防火墙、VPN 及入侵检测等系统安全方面的知识仅做了概念性的介绍。第六章围绕密钥安全和授权体系对 PKI、SKI、PMI 的基本知识进行讲述。

本书适用于数学、计算机、通信、电子和信息专业的本科高年级学生和研究生一学期课程使用。

图书在版编目(CIP)数据

信息安全基础/徐茂智编著. —北京:高等教育出版社,2006.12
ISBN 7-04-020196-8

Ⅰ.信… Ⅱ.徐… 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(2006)第 138044 号

策划编辑 张长虹 **责任编辑** 崔梅萍 **封面设计** 赵 阳 **责任绘图** 尹 莉
版式设计 马静如 **责任校对** 殷 然 **责任印制** 韩 刚

出版发行	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街 4 号	**免费咨询**	800-810-0598
邮政编码	100011	**网 址**	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	廊坊市科通印业有限公司	**畅想教育**	http://www.widedu.com
开 本	787×960 1/16	**版 次**	2006 年 12 月第 1 版
印 张	8.75	**印 次**	2006 年 12 月第 1 次印刷
字 数	160 000	**定 价**	11.60 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号 20196-00

信息与计算科学专业系列教材编委会

总　序

根据教育部1998年颁布的普通高等院校专业目录，“信息与计算科学”专业被列为数学类下的一个新专业（它覆盖原有的计算数学及其应用软件、信息科学与运筹控制等专业）。这一新专业的设置很好地适应了新世纪以信息技术为核心的全球经济发展格局下的数学人才培养与专业发展的需要。然而，作为一个新专业，对其专业内涵、专业规范、教学内容与课程体系等有一个自然的认识与探索过程。教育部数学与统计学教学指导委员会数学类专业教学指导分委员会（下称教指委）经过过去两年艰苦细致的工作，对这些问题现在已有了比较明确的指导意见，发表了《关于信息与计算科学专业办学现状与专业建设相关问题的调查报告》及《信息与计算科学专业教学规范》（讨论稿）（见《大学数学》第19卷1期（2003））。为此，全国高等学校教学研究中心在承担全国教育科学“十五”国家级规划课题——“21世纪中国高等教育人才培养体系的创新与实践”研究工作的基础上，根据教指委所颁布的新的教学规范，组织国内各高校的专家教授，进行其子项目课题“21世纪中国高等学校信息与计算科学专业教学内容与课程体系的创新与实践”的研究与探索。为推动本专业的教材建设，该项目课题小组与高等教育出版社联合成立了“信息与计算科学专业系列教材编委会”，邀请有多年教学和科研经验的教师编写系列教材，由高等教育出版社独家出版，并冠以教育科学“十五”国家规划课题研究成果。

按照新的《信息与计算科学专业教学规范》（讨论稿），信息与计算科学专业是以信息技术和计算技术的数学基础为研究对象的理科类专业。其目标是培养学生具有良好的数学基础和数学思维能力，掌握信息与计算科学基础理论、方法与技能，受到科学研究的训练，能解决信息技术和科学与工程计算中的实际问题的高级专门人才。毕业生能在科技、教育、信息产业、经济与金融等部门从事研究、教学、应用开发和管理工作，能继续攻读研究生学位。根据这一专业目标定位和落实“强基础、宽口径、重实际、有侧重、创特色”的办学指导思想，我们认为，本专业在数学基础、计算机基础、专业基础方面应该得到加强，而各学校在这三个基础方面可大体一致，但专业课（含选修课）允许各校自主选择、体现各自特点。考虑到已有大量比较成熟的数学基础与计算机基础课程教材，本次教材编写主要侧重于专业基础课与专业课（含选修课）方面。

信息与计算科学，就其范畴与研究内容而言，是数学、计算机科学和信息工

程等学科的交叉，已远远超出数学学科的范畴。但作为数学学科下的一个理科专业，信息与计算科学专业则主要研究信息技术的核心基础与运用现代计算工具高效求解科学与工程问题的数学理论与方法（或更简明地说，研究定向于信息技术与计算技术的数学基础），这一专业定位明显地与计算机科学与信息工程专业构成区别。基于这一定位，信息与计算科学专业可包括信息科学与科学计算（计算数学）两个大的方向。科学计算方向在我国已有长期的办学经验，通常被划分为偏微分方程数值解、最优化理论与方法、数值逼近与数值代数、计算基础等学科子方向。然而，对于信息科学，它到底应该怎样划分学科子方向？应该怎样设置专业与专业基础课？所有这些都仍是正在探索的问题。

任何技术都可以认为是延伸与扩展人的某种功能的方式与方法，所以信息技术可以认为是扩展人的信息器官功能的技术。人的信息器官主要包括感觉器官、传导器官（传导神经网络）、思维器官和效应器官四大类型，其功能则主要是信息获取、信息传输、信息处理和信息应用（控制），因而感测技术、通信技术、智能技术与控制技术通常被认为是最基本的信息技术（常称之为信息技术的四基元），其他信息技术可认为是这四种基本技术的高阶逻辑综合或分解衍生。所以可以把信息科学理解为是“有关信息获取、信息传输、信息处理与信息控制基础的科学”。从这个意义上，我们认为：信息处理（包括图像处理、信号分析等）、信息编码与信息安全、计算智能（人工智能、模式识别等）、自动控制等可构成信息科学的主要学科子方向。这一认识也是教指委设置信息与计算科学专业信息科学方向课程的基本依据。

本系列教材正是基于以上认识，为落实新的《信息与计算科学专业教学规范》（讨论稿）而组织编写的。我们相信，该系列教材的出版对缓解本专业教材的紧缺局面，对推动信息与计算科学专业的快速与健康发展会大有裨益。

从长远的角度看，为适应不同类型院校和不同层次要求的课程需求，本系列教材编委会还将不断组织教材的修订和编写新的教材，从而使本专业的教学用书做到逐步充实、完善和多样化。我们诚恳希望采用本系列教材的教师、同学们及广大读者对书中存在的问题及时指正并提出修改意见和建议。

信息与计算科学专业系列教材编委会

2003 年 8 月 31 日

前　言

信息安全的内容十分丰富，随着计算机网络的广泛应用，在近15年来得到了快速发展。国际上已经把信息安全的概念扩展为信息保障(IA)，即信息的保护(protect)、检测(detect)、响应(react)和恢复(restore)。信息的事先保护是信息安全研究中最为成熟的部分，它主要研究保护信息的机密性、完整性、访问控制、身份识别、防抵赖等内容，密码技术在其中占据着核心地位。

国内外已经出版了许多信息安全方面的专著，有的对一些专题做了非常深入的研究，有的试图对信息安全做一个全面的讨论。然而过分专门的专题作为教材会使学生“只见树木，不见森林”。另一方面，全面的讨论需要很大篇幅，但往往未等定稿，一些内容就已显得过时，而又需要加入新的内容。现存的教材或多或少有一些专著的味道。本书是作者在北京大学为数学和信息专业的研究生和本科高年级学生讲授信息安全课程讲义基础上，同时考虑到计算机科学、通信、电子工程等专业开设信息安全课程的需要而编写的，目的是提供一本有广泛的适用性的普通教学用书。

在选材原则上，首先为大学生提供系统的知识，而不去追求全面的知识。其次，在内容选择上还注重基本概念、基本算法和其他有较强的穿透力的知识点，而不在工程细节上过多地纠缠。再次，对待那些不太成熟的或缺乏理论支撑的或需要太多预备知识的内容只好“割爱”，最多交代一下概念。当然这些原则并不能排斥自己在选材上的偏好。本书作者认为信息安全保护应当以密码和访问控制中的算法、协议和模型为基础，依此搭建鲜活的应用。

在内容组织上，从信息安全的基本概念和模型出发，通过对基本算法和基本协议的讨论，学生可以比较容易地掌握信息安全中的研究方法，最后通过对应用技术的学习，学生可检验、巩固和深化前面学到的知识。

本书由六章组成。第一章介绍信息安全的基本概念，包括数据的机密性、完整性、访问控制、可用性、身份识别、防抵赖、系统安全、权利保护等内容。第二章、第三章则介绍密码技术中的一些具体算法和协议，着重讨论其原理和在信息安全保护中的应用，包括传统密码算法、公钥密码算法、Hash函数和数字签名算法、密钥分发技术、秘密共享和身份识别协议等。第四章则介绍了非密码保护的另一个重要基础——安全模型，包括访问控制矩阵模型、Bell-LaPadula模型和基于角色的访问控制模型。通过前面的关于算法、协议和模型准备，第五章对繁杂

的实用技术进行了介绍，主要包括 Web 安全、数据库安全、电子交易安全三个重要的应用技术的介绍，而对操作系统安全、数据库安全、病毒防护、防火墙、VPN 及入侵检测等系统安全方面的知识仅做了概念性的介绍。第六章围绕密钥安全和授权体系对 PKI、SKI、PMI 的基本知识进行讲述，同时对信息安全相关标准化组织也做了列举，以备参考。最后给出本书所参考的文献。前四章为本书的重点，后两章既拓宽了学生的知识面，也是对前面所学知识掌握程度的检验。

本书的写作得到高等教育出版社、科技部科学数据共享关键技术研究（项目编号：2004DKA20300）、国家自然科学基金网络与信息安全重大项目（批准号 90104004）、国家 973 项目（批准号 1998030420）的支持。同时得益于与北京大学安全与密码工程研究中心王杰教授、赵春来教授，博士生赵彦慧、沈浔浔的有益讨论，张瑞玲同志仔细校对了全稿。在此一并表示感谢。

公历 2006 年仲夏　于燕园

目　　录

第 I 章
基本概念

信息安全是一个新词，但并非是一个新概念. 在计算机出现之前，各组织机构把有价值的文件保存在坚固的文档柜中，而把机密文件锁在保险柜中. 部门之间文档的交换则通过专门的交通员来传递或通过密码电报进行传递. 同时对文档的保管、使用、传递、销毁等过程用一套完善的制度来管理. 这种文档安全管理实际上就是我们要说的信息安全，文档是这种情况下的信息载体而已. 文档管理目前仍然存在，所以我们并不陌生.

20 世纪 70 年代，计算机的引入，不仅方便了文档的处理和存储，而且保存在计算机上的文档信息还可使我们能更方便地使用和交换. 与纸质文档时代相比，这种变革使组织机构的办公效率有了本质上的提高. 人们一直在寻找电子文档的保护，原来的安全管理制度演变成对计算机系统的访问控制，而电子文档的传输则采用加密技术和数字签名技术进行保护. 与此同时，受保护对象也不仅仅是纸质文档的电子形式，而成为最广泛意义上的电子信息. 电子信息已经把原始的文档概念大大拓广了，它不仅包括普通文档文件，而且包括语音、图像等多媒体文件，甚至包括一些抽象数据结构、程序或对象. 可见计算机的引入，对信息安全的研究提出了新的课题. 其间，信息安全技术却并没有跟上计算机发展的步伐.

20 世纪 90 年代，计算机网络呈现了爆炸式的发展. 这种发展一下子把人们带到了一个全新的时空. 空间已经不再是地理的概念，它体现了信息资源在网络中的分布结构. 由于镜像、超文本链接等技术的应用可以把“点”随意地粘连或克隆，形成了一个甚至连维数都无法确定的、难以驾驭的拓扑构架. 在紧跟着网络技术推动应用发展的后面，是一个应用推动技术发展的时代，这个技术将围绕信息安全展开. 在人们几乎全方位地依赖计算机网络的同时，网络环境下的信息安全问题再次成为人们关注的焦点.

从上述三个信息安全发展的不同阶段，我们看到信息安全的保护对象越来越多，而环境越来越复杂. 本书的重点是描述网络环境下的信息安全概念和基本方法.

§1 因特网与网络环境下的信息安全

因特网(Internet),即国际互联网,是一个覆盖全球的信息网络,它把各种不同类型的计算机通过统一的 TCP/IP 协议连接在一起,使得任何与网络连接的计算机可以方便地与网上其他计算机进行交互,共享信息资源和计算资源. 现在人们最常使用的浏览器、电子邮件等都是建立在 TCP/IP 协议之上的应用.

Internet 是一个自由交易区,开放性和信息共享为其特点. 人们可以在网上公开任何信息或搜索自己想要的信息.

显然,人们的信息交互是有目的的,从而使网上的信息产生了价值. 这种价值有时体现为个人利益,有时体现为公司、政府或社会团体的集体利益. 另一方面,Internet 的自由特点使得非法分子或利益的敌对方轻易地破坏或危害网络的正常使用和信息的正常交流. 同时这些破坏或危害比其他环境下更加难以追查,也更难取证. 可见网络环境下信息安全的关键是防护.

理解信息安全内容首先需要了解信息所面临的安全攻击手段. 让我们看一下网络环境下的几种典型攻击.

1.1.1 安全攻击的基本类别

先介绍几个概念.

安全攻击(Security Attack):是指各种有损于信息安全性的操作.

计算机网络(Computer Network):计算机网络同所有的信息系统一样,由计算设备(如客户机、服务器)、交换设备(如集线器、路由器)以及连接设备(通信线路)组成. 网络中的计算设备构成了它的计算部分,而交换设备和连接设备共同组成了网络的通信部分.

计算机网络中的通信部分本身构成一个信息系统,也是由其自身的计算部分和通信部分组成,但它位于更低一个层次. 计算机网络中构成计算部分的计算机同孤立计算机系统相比,是一个开放的系统,实现了从"独立自治"到"开放互联"的跨越.

网络计算机(Network Computer):是指网络中的一个自治信息系统,它可以代表网络中的单台计算机,也可以表示网络中的一个局域网、子网或一个虚拟专用网.

网络计算机的概念实际上是现有各种内部网络(Intranet)连接到外部网络(Internet)的一种模型. 网络计算机把内部网看成了一个计算机系统,而把内网与外网的联接看成了这台"网络计算机"与外界的通信环境. 这种概念的意义在

于把普通计算机系统与“内网—外网”结构的网络计算机用一致的观点建立模型,这在第四章介绍安全模型时会详细论述.

计算机网络的信息安全是研究网络计算机的计算信息安全和它们之间的通信信息安全的科学.因为网络计算机的开放性实际上是一个从物理层到应用层的全面开放.这使得它的安全性问题变得非常复杂.

网络环境下,信息系统受到的威胁或攻击有很多种,下面介绍4种主要的分类.

1. 攻击的目的

按攻击者动机或目的,攻击可分为三个基本类别:非授权访问、假冒和拒绝服务.

(1) 非授权访问

非授权访问是指未经授权的实体获得了访问网络资源的机会,并有可能篡改信息资源.这种访问通常是通过在不安全信道上截取正在传输的信息或者利用技术及产品中固有的弱点来实现的.

网络上的包是否容易被探听(也称为窃听)主要依赖于所采用的技术.介质共享的网络最容易被窃听,因为这种类型的网络在将包从源地址传输到目的地址时,包有可能经过网络的任何一个地方.当在共享介质环境(如FDDI、10Base-T或100 Mb/s以太网)中使用集中器或集线器时,很容易插入具有包捕获功能的新节点,然后窃取网络中的通信量.如图1.1所示,入侵者可以接入以太网集线器,并用包解码程序读取以太网上传输的数据.

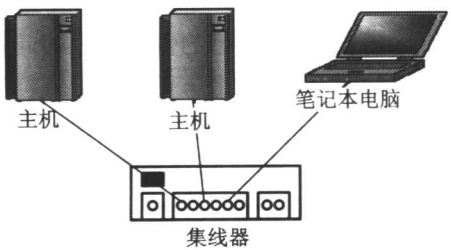

图1.1 以太网中的窃听

在本例中,入侵者利用以太网包解码器程序(如EtherPeek或TCPDump)可以截获用户名/用户口令信息和敏感的路由协议数据.发送出的数据被运行着EtherPeek程序的笔记本电脑捕获;然后解码器程序把十六进制数据转换成用户可读的形式.在获得所需的数据之后,入侵者就可以利用这些信息扩大访问范围,从而在非授权情况下阅读机密信息和程序.随后,入侵者甚至还可能篡改资源,也就是说,入侵者可能修改服务器上的记录或改变路由信息的内容.

如 EtherPeek 和 TCPDump 这样的包解码程序，它们的安装只占用很少的系统资源，而且界面友好. 当然，开发解码程序的最初目的是为了排除网络故障，但它同时也很容易被用作恶意攻击的工具.

某些情况下可以探测到包的窃听，但更多的时候不会有人知道它的发生. 要想窃听到包，必须在信息的发送端和接收端之间插入一台设备. 在点对点的连接方式（如串联方式）下，这项任务较难完成. 但在共享介质环境下则很容易实现.

防止非授权访问的最佳方法是采用加密和认证技术来对不安全通道的通信量进行加密和认证编码，使之在传输过程中不能被窃听和修改.

（2）假冒

假冒是指通过出示伪造的凭证来冒充别人或别的主体的能力. 非授权访问通常是假冒的基础，同时又是假冒的目的，二者有很密切的联系. 它们的差别是，假冒通过欺骗对方获得授权，而非授权访问则绕过授权机制进行访问.

假冒攻击有很多种表现形式：盗窃私钥、访问明码形式的用户名/口令，然后欺骗认证机构，或者记录一条授权序列并在以后重放. 在大型（内部）网络中，假冒具有很大的破坏性，因为它回避了结构化授权访问规则.

假冒攻击可分为重放、伪造和代替三种. 重放攻击是先把消息记录下来，然后再发送出去，利用身份验证机制或协议中的漏洞进行欺骗；伪造攻击指提供冒充主体身份的信息，以获得对系统及其服务的访问权力；代替攻击则通过分析截获的消息，构造一种难以辨别真伪的身份信息取代原来的消息，破坏正常的访问行为.

假冒通常是在窃听之后实施的. 典型的情形是先访问授权信息序列，然后利用这些信息来进行非授权访问. 一旦获得非授权访问，造成的损坏程度就要由入侵者的动机来决定了. 如果幸运的话，入侵者可能只是电脑空间中一名好奇的漫游者. 但大多数人不会那么幸运，他们的机密信息通常都会被危及并可能被破坏.

许多包窃听程序，同时具备包生成的功能，它们可以先截获数据包，然后再按原样发送出去，实现包欺骗和重放攻击.

利用加密、鉴别机制（也叫认证机制），可以有效预防假冒攻击. 使用这些密码技术的附加好处是在某些情况下，可以获得“不可否认”的特征. 即参与电子信息交换的用户事后不能否认他曾经发送了某条消息. 在涉及电子金融业务或电子合同时，这种“不可否认”的特征非常重要，因为人们通常都试图在这些方面抵赖曾经参与非法行为.

上面谈到的假冒主要是指身份的假冒和信息的假冒. 广义的假冒攻击还包括设备的假冒，包括由于未知的协议和软件行为意外地发生的设备假冒和人为