21世纪高等院校计算机教材系列

计算机网络与信息安全技术

●俞承杭　编著

购书可获得增值回报
提供教学用电子教案

机械工业出版社
CHINA MACHINE PRESS

21 世纪高等院校计算机教材系列

计算机网络与信息安全技术

俞承杭　编著

机 械 工 业 出 版 社

本书从分析信息安全问题的起因着手，分析了网络攻击和信息安全风险，并在此基础上介绍了信息安全的理论和技术体系，针对信息安全的不同环节给出了不同的技术实现方法。本书主要内容包括加密认证技术、内容安全技术、备份恢复技术、系统脆弱性评估技术、防火墙技术、入侵检测与防御技术、虚拟专用网络（VPN）技术、访问控制与审计技术、计算机病毒防范技术，结合管理问题提出了信息安全管理的实施步骤。本书最后有针对性地安排了18个实验项目，以巩固所学知识，加深理解。

本书面向应用型的本科专业，可作为计算机、通信、电子信息工程、电子商务等专业相关课程的教科书，也可作为网络工程技术人员、网络管理人员的技术参考书和培训教材。

图书在版编目（CIP）数据

计算机网络与信息安全技术/俞承杭编著. —北京：机械工业出版社，2008.3
（21世纪高等院校计算机教材系列）
ISBN 978-7-111-23388-6

Ⅰ.计… Ⅱ.俞… Ⅲ.计算机网络－安全技术－高等学校－教材
Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2008）第014131号

机械工业出版社（北京市百万庄大街22号 邮政编码 100037）
责任编辑：张宝珠
责任印制：李妍

唐山丰电印务有限公司印刷
2008年3月第1版·第1次印刷
184mm×260mm·18.25印张·451千字
0001—5000册
标准书号：ISBN 978-7-111-23388-6
定价：28.00元

凡购本书，如有缺页，倒页，脱页，由本社发行部调换
销售服务热线电话：（010）68326294
购书热线电话：（010）88379639 88379641 88379643
编辑热线电话：（010）88379739 88379753
封面无防伪标均为盗版

出 版 说 明

信息技术是当今世界发展最快、渗透性最强、应用最广的关键技术，是推动经济增长和知识传播的重要引擎。在我国，随着国家信息化发展战略的贯彻实施，信息化建设已进入了全方位、多层次推进应用的新阶段。现在，掌握计算机技术已成为21世纪人才应具备的基本素质之一。

为了进一步推动计算机技术的发展，满足计算机学科教育的需求，机械工业出版社聘请了全国多所高等院校的一线教师，进行了充分的调研和讨论，针对计算机相关课程的特点，总结教学中的实践经验，组织出版了这套“21世纪高等院校计算机教材系列”。

本套教材具有以下特点：

(1) 反映计算机技术领域的新发展和新应用。

(2) 注重立体化教材的建设，多数教材配有电子教案、习题与上机指导或多媒体光盘等。

(3) 针对多数学生的学习特点，采用通俗易懂的方法讲解知识，逻辑性强、层次分明、叙述准确而精炼、图文并茂，使学生可以快速掌握，学以致用。

(4) 符合高等院校各专业人才的培养目标及课程体系的设置，注重培养学生的应用能力，强调知识、能力与素质的综合训练。

(5) 适合各类高等院校、高等职业学校及相关院校的教学，也可作为各类培训班和自学用书。

机械工业出版社

前　言

网络技术、通信技术、多媒体技术的迅猛发展对 Internet 产生了极大的影响，其表现为联网方式多样化；网络带宽的大大拓宽；Internet 提供更多的服务，不再局限于传统应用，新的应用模式不断涌现。这几个方面的变化使得网络真正成为人类生活的一部分，人们可以利用快速而廉价的网络去了解缤纷的世界。互联网技术的发展引发了一场全方位的技术革命，它对人类的工作方式、生活方式，甚至思维理念都产生了巨大的影响，人们在自觉或不自觉地接受了网络化的思维方式和工作方式的同时，也在改变着自己的行为方式。

互联网的开放性方便了用户的使用，促进了互联网的高速扩展，而互联网“无序、无界和匿名”的特点也成为制约它应用的绊脚石。互联网带来的虚假、反动、黄色的信息，引出的假冒、伪造现象，以及网络攻击、病毒泛滥等恶意事件，不仅严重影响了个人、集体的利益，甚至危害了国家的信息安全。

伴随着信息产业发展而产生的网络信息安全问题，已成为各国政府有关部门、各大行业和企事业单位关注的热点问题。目前，全世界由于信息系统的脆弱性而导致的经济损失逐年上升，安全问题日益严重。面对这种现实，各国政府的有关部门和企业更加重视网络的安全问题。

国内许多高校陆续开设了网络信息安全课程，旨在让未来的应用人员和技术人员率先掌握信息安全防护技术。

本书就是在这样的背景下，经过作者多年的教学实践，以信息生命周期为主线，关注各环节的安全问题，反复调整、充实教学内容，从系统的角度，提出了技术安全、组织安全、管理安全的信息安全实现体系，每部分均通过专用的产品或技术实现其安全性。

本书结构可分五个部分，共 15 章。

第一部分：第 1～3 章，根据信息安全的风险与威胁，网络攻击技术，从理论上提出解决信息安全问题的体系结构。

第二部分：第 4～6 章，从信息内容的角度，介绍加密认证技术、内容安全技术和备份恢复技术，特别针对网站篡改和内容保密介绍的专用的技术和产品。

第三部分：第 7～13 章，针对网络安全问题，介绍各种网络安全技术，包括防火墙、入侵检测、漏洞扫描、VPN 技术、网络隔离、访问控制技术和网络防病毒技术。

第四部分：第 14 章，介绍了信息安全管理方面的要求和实施办法。

第五部分：第 15 章，网络信息安全课程实验。以应用为目标，精心组织了 18 个实验项目，通过设备或软件验证理论，掌握技术，加深理解，巩固知识。

本书在编写过程中，参考和引用了大量的产品技术资料、现有教材资料和工程文档，这些资料列在书末的参考文献中，在此谨对所有相关材料的作者表示感谢。

本书的编写得到浙江传媒学院领导的大力帮助，通过重点课程、教改项目等方式提供支持。此外还要感谢杭州师范大学、浙江警官学院等高校提供的教材体系应用检验。

本书提供电子课件和实验素材，需要的读者可在 www. cmpedu. com 上下载。

由于水平有限，本书还有许多不当之处，敬请各位专家和读者指正。

编　者

目　录

第 1 章　信息与信息安全风险

在信息化社会中，信息已成为制约社会发展、推动社会进步的关键因素之一，人们对信息和信息技术的依赖程度越来越高，人与人之间的交流也日趋机器化。本章将从信息的概念发展出发，介绍信息的作用，信息技术对人类生活的影响，描述信息面临的风险与威胁，最后介绍信息安全的目标。

1.1　信息与信息技术

1.1.1　信息的概念

“信息”一词早已出现在人类的生活中，人们由于研究目的和角度不同，对信息的理解和解释也不尽相同。到了 20 世纪，特别是 20 世纪中期以后，随着现代信息技术的飞速发展，信息才被赋予准确的含义。

1928 年，哈特雷(L.V.R.Hartley)在论文“信息传输”中将信息理解为“选择通信符号的方式”，并用选择的自由度来计量这种信息的大小。这种定义只是一种认识论意义上的信息，没有涉及信息的价值和统计性质。

1948 年，信息论创始人香农(C.E.Shannon)在“通信的数学理论”一文中认为“信息是用以消除不确定性的东西”，并推导出了信息测度的数学公式，提出香农定理，描述了有限带宽、有随机热噪声信道的最大传输速率与信道带宽、信号噪声功率比之间的关系，在此基础上发明了信息编码的三大定理，为现代通信技术的发展奠定了理论基础。但香农同样没有考虑信息的内容与价值。

1948 年，在香农创建信息论的同时，控制论的创始人维纳(N.Wiener)在专著“控制论——动物和机器中的通信与控制问题”中认为“信息是人们在适应外部世界，并使这种适应反作用于外部世界的过程中，同外部世界进行交换的内容的名称”，他还认为“接收信息和使用信息的过程，就是我们适应外部世界环境的偶然性变化的过程，也是我们在这个环境中有效地生活的过程。”，这一定义包含了信息的内容与价值，从动态的角度揭示了信息的功能与范围。

决策学的代表人物西蒙则提出，“信息是影响人们改变对决策方案的期待或评价的外界刺激”。

如此等等，信息的定义有 100 多种，从不同侧面、不同层次揭示了信息的特征与性质，但都存在着局限性。

1988 年，中国学者钟义信在《信息科学原理》一书中认为“信息是事物运动的状态与方式，是事物的一种属性”，通过引入约束条件，推导了信息的概念体系，对信息进行了完整而准确的论述。这一定义具有最大的普遍性，涵盖了所有其他的信息定义，并通过约束条件实现与其他定义的转换。

1.1.2 信息的性质

信息来源于物质，但又不是物质本身；信息也来源于精神世界，但又不限于精神领域。信息是物质的普遍属性，是物质运动的状态与方式。信息的物质性决定了它的一般属性，主要包括普遍性、客观性、无限性、相对性、抽象性、依附性、动态性、异步性、共享性、可传递性、可交换性、可处理性和可伪性等。其中与信息安全相关的性质有以下几个。

(1) 依附性

依附性有两个层次的涵义：一是信息必须借助于某种特定的“符号”来表示，如文字、图形和图像等；二是信息符号必须依附于一定的物理介质上，如纸张、磁盘等。信息的这一特征要求设计和选择恰当的信息载体，并对其进行科学的编码，才能使信息的传递、保存、加工与利用更加方便有效。

(2) 动态性

客观事物(或系统)都是在不断发展变化的，信息只有及时、新颖才有价值，才能发挥巨大的作用。换句话说，一条信息在某一时刻可能有很高的价值，但过了这一时刻它的价值可能就会大大降低，甚至变得没有价值。

(3) 可处理性

可处理性是指信息的内容是可以被识别的，信息的形式是可以转换或变换的。信息可以被各种方法多环节地加工和处理，而经过某些处理(如分析、综合和提炼)后的信息可以比原始信息更具有价值。

(4) 共享性

信息可无限扩散，信息本身不会因为知道的人数增加而减少，却可能会因信息被分享，而使信息的所有者蒙受损失。例如，企业的技术专利、军事动态等就有这种共享性。为了避免共享给信息的所有者造成损失，信息共享往往有范围(区域上、时间上)和条件的限制。

(5) 可传递性

信息在时间和空间上都具有传递性。从时间的延续性讲，信息可以借助于各种载体而被代代相传，信息在时间上的传递叫做信息的存储；从空间转移的角度讲，信息也可以从一个位置传递到另一个位置，信息在空间上的传递叫做通信。

(6) 异步性

异步性体现在通常以存储信息的方式来接收信息，然后人们可以在任何时间来消费、使用这些信息。

(7) 可交换性

可交换性是指信息可在两个主体间实现交换。

(8) 可伪性

信息是可以伪造的。

信息安全将处理与信息的依附性、动态性、可处理性、共享性、可传递性、异步性、可交换性和可伪性等相关的问题。

1.1.3 信息的功能

信息的功能是信息属性的体现，主要可分为两个层次：基本功能和社会功能。基本功能在

于维持和强化世界的有序性。可以说,缺少物质的世界是空虚的世界,缺少能量的世界是死寂的世界,而缺少信息的世界则是混乱的世界。社会功能则表现为维系社会的生存、促进人类文明的进步和自身的发展。信息的功能主要表现在以下几个方面。

1) 信息是一切生物进化的导向资源。生物生存于自然环境中,而外部自然环境经常发生变化,如果生物不能得到这些变化的信息,就不能及时采取必要的措施来适应环境的变化,就可能被变化了的环境淘汰。

2) 信息是知识的来源。知识是人类长期实践的结晶,它一方面是人们认识世界的结果,另一方面又是人们改造世界的方法,信息具有知识的秉性,可以通过一定的归纳算法被加工成知识。

3) 信息是决策的依据。决策就是选择,而选择意味着消除不确定性,意味着需要大量、准确、全面及时的信息。

4) 信息是控制的灵魂。控制是依据策略信息来干预和调节被控对象的运动状态和状态变化的方式,没有策略信息,控制系统便会不知所措。

5) 信息是思维的材料。思维的材料只能是"事物的运动状态和状态变化的方式",而不可能是事物的本身。人的思维和智慧是信息过程的产物。

信息是管理的基础,是一切系统实现自组织的保证。

信息是一种重要的社会资源,虽然人类社会在漫长的进化过程中一直没有离开信息,但是只有到了信息时代的今天,人类对信息资源的认识、开发和利用才可以达到高度发展的水平。现代社会将信息、物质和能源看成支持社会发展的三大支柱,充分说明了信息在现代社会中的重要性。

信息安全的任务就是确保信息功能的正确实现。

1.1.4 信息技术与信息安全

信息技术,最简单的理解就是人们处理信息的相关技术。它是随着人类的出现而出现,随着人类文明的进步而不断发展起来的。尤其是在最近二,三十年,科学技术得到了迅猛的发展,各种高新技术如雨后春笋般纷纷出现。借助于这些高新技术,信息技术也得到了前所未有的发展,而且已经成为当代新技术革命最活跃的领域。

我们现在所讲的信息技术一般是指近几十年刚刚发展起来的现代信息技术,它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、音频以及语音信息,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。

具体来讲,信息技术主要包括以下几个方面。

(1) 感测与识别技术

感测技术包括传感技术和测量技术,它的作用是扩展人类获取信息的感觉器官功能,尤其是由传感技术、测量技术和通信技术相结合而产生的遥感技术,更使人感知信息的能力得到进一步的加强。信息识别包括文字识别、语音识别和图形识别等,识别技术的实现通常要借助于一种叫做"模式识别"的方法。

(2) 信息传递技术

信息传递技术的主要功能是实现信息快速、可靠、安全地转移。各种通信技术都属于这个范畴。广播技术也是一种传递信息的技术。由于存储、记录可以看成是从"现在"向"未来"或

从“过去”向“现在”传递信息的一种活动，因而也可以将它看作是信息传递技术的一种。

(3) 信息处理与再生技术

信息处理包括对信息的编码、压缩、加密等。在对信息进行处理的基础上，还可以形成一些新的更深层次的决策信息，这称为信息的“再生”。信息的处理与再生都有赖于现代电子计算机的超凡功能。

(4) 信息施用技术

信息施用技术是信息过程的最后环节。包括控制技术、显示技术等。

从以上分析可以看出，在信息技术中信息的传递是通过现代的通信技术来完成的，处理信息是通过各种类型的计算机(智能工具)来完成的，而信息要被人类所利用，必须可以控制，因此也有人认为信息技术(Information Technology)简单地说就是 3C——Computer(计算机)、Communication(通信)和 Control(控制)，即 IT = Computer + Communication + Control。

信息安全关注的是信息在各种信息技术的施用过程中是否能维持它的基本性质，信息的功能是否能正确实现这些问题。

1.1.5 信息系统与信息安全

信息系统是指基于计算机技术和网络通信技术的系统，是人、规程、数据库、硬件和软件等各种设备、工具的有机集合。

信息系统的发展经历了电子数据处理系统(EDPS)、管理信息系统(MIS)、决策支持系统(DSS)、办公自动化系统(OAS)和多媒体信息系统(MMIS)等几个阶段。在管理科学和方法的指导下，同统计理论和方法、计算机技术、通信技术等相互渗透、相互促进，迅速形成一个专门的应用领域。

在信息安全领域，重点关注的是与信息处理生命周期相关的各个环节，包括信息本身在整个生命周期中的存在形式、存储处理相关的设备、传递交换所用的通信网络、相应的计算机软件和协议等。

1.2 信息安全的重要性与严峻性

1.2.1 信息安全的重要性

1946 年，世界第一台电子计算机 ENIAC 在美国诞生后，经过 60 多年的发展，作为社会发展三要素的物质、能源和信息的关系发生了深刻的变化。在计算机技术和通信技术的推动下，信息要素已成为支配人类社会发展进程的决定性力量之一，信息关系到一个人的成长、一个单位的业务发展，甚至一个国家的生死存亡。可以这么说，我们的社会已经开始从工业化社会逐渐进入到信息化社会。

微型计算机和大容量存储技术的发展和应用，推动了信息处理的电子化；通信技术和通信协议的发展推动了信息的高速传输和信息资源的广泛共享。20 世纪 80 年代以后，特别是 90 年代中后期开始的互联网狂潮，彻底改变了人们获取知识、了解信息的习惯，互联网已经成为继电视、电台、报刊之后的第四媒体，是我们获取信息、传播信息的重要载体。互联网的使用已经深入到政治、军事、文化、商务、学习和日常生活等各个领域和方面，深刻影响着社会各阶层、