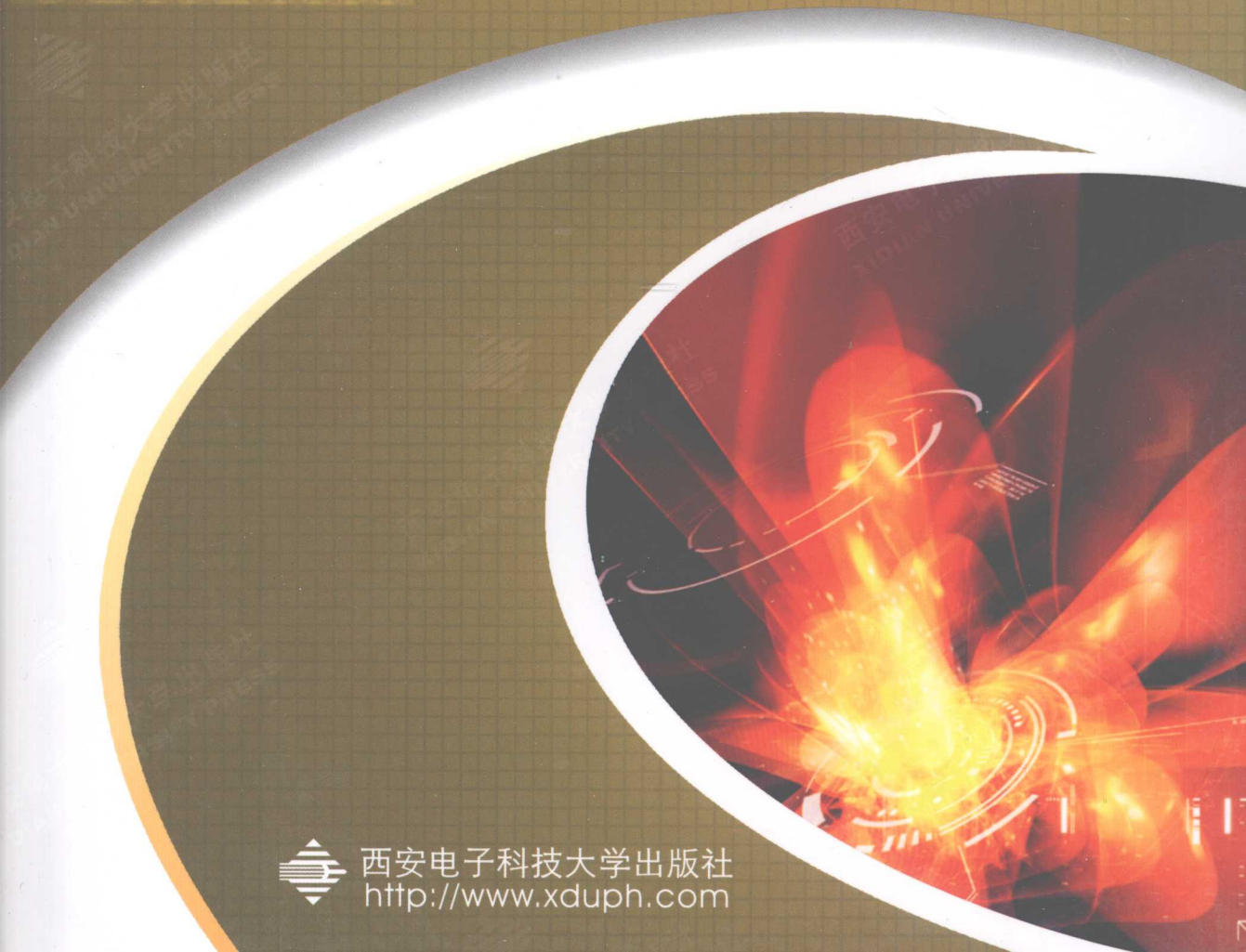
十一五

高等学校电子与通信类专业“十一五”规划教材

通信网安全与保密

王景中　徐小青　曾凡锋　编著
杨义先　主审



西安电子科技大学出版社
http://www.xduph.com

高等学校电子与通信类专业“十一五”规划教材

通信网安全与保密

王景中　徐小青　曾凡锋　编著
杨义先　主审

西安电子科技大学出版社
2008

内 容 简 介

本教材是作者在多次讲授“通信网络安全技术”课程的基础上，参考国内外相关文献，经过重新整理，编写而成的。在编写过程中，力求做到内容全面，重点突出，注重知识点的结合，强调基本概念和基本方法。本教材以加强实践能力的培养为特色，通过将信息安全认证内容引入本课程，调动学生对本课程的学习兴趣，使学生灵活掌握通信网络安全的基本知识和基本技能。学完本课程后，学生可以参加信息安全认证考试，对就业很有帮助。

本教材分别介绍了计算机病毒、密码技术、安全服务、防火墙技术、安全管理、安全协议、安全工具等内容，并且用具体例子对知识点进行讲解，每一章后都有小结和习题。

本书适合作为计算机科学与技术、电子信息工程、通信工程以及电子信息类本科专业通信网络安全相关课程的教学用书，也可作为相关工程技术人员的参考书。

图书在版编目（CIP）数据

通信网安全与保密 / 王景中，徐小青，曾凡锋编著. —西安：西安电子科技大学出版社，2008.9

高等学校电子与通信类专业“十一五”规划教材

ISBN 978-7-5606-2117-3

Ⅰ. 通… Ⅱ. ① 王… ② 徐… ③ 曾… Ⅲ. ① 通信网—安全技术—高等学校—教材 ② 保密通信—高等学校—教材 Ⅳ. TN915.08 TN918

中国版本图书馆 CIP 数据核字（2008）第 127851 号

策　　划　曹　昳

责任编辑　段　蕾　曹　昳

出版发行　西安电子科技大学出版社（西安市太白南路 2 号）

电　　话　(029)88242885　88201467　邮　编　710071

http://www.xduph.com　E-mail: xdupfxb001@163.com

经　　销　新华书店

印刷单位　西安文化彩印厂

版　　次　2008 年 9 月第 1 版　2008 年 9 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　印张 19.5

字　　数　459 千字

印　　数　1～4000 册

定　　价　28.00 元

ISBN 978 – 7 – 5606 – 2117 – 3 / TN • 0458

XDUP 2409001-1

西安电子科技大学出版社
高等学校电子与通信类专业“十一五”规划教材
编审专家委员会名单

主　任：杨　震（南京邮电大学校长、教授）

副主任：张德民（重庆邮电大学通信与信息工程学院副院长、教授）
秦会斌（杭州电子科技大学电子信息学院院长、教授）

通信工程组

组　长：张德民（兼）

成　员：（成员按姓氏笔画排列）
王　晖（深圳大学信息工程学院副院长、教授）
巨永锋（长安大学信息工程学院副院长、教授）
成际镇（南京邮电大学通信与信息工程学院副院长、副教授）
刘顺兰（杭州电子科技大学通信工程学院副院长、教授）
李白萍（西安科技大学通信与信息工程学院副院长、教授）
张邦宁（解放军理工大学通信工程学院卫星系系主任、教授）
张瑞林（浙江理工大学信息电子学院院长、教授）
张常年（北方工业大学信息工程学院院长、教授）
范九伦（西安邮电学院信息与控制系系主任、教授）
姜　兴（桂林电子科技大学信息与通信学院副院长、教授）
姚远程（西南科技大学信息工程学院副院长、教授）
康　健（吉林大学通信工程学院副院长、教授）
葛利嘉（中国人民解放军重庆通信学院军事信息工程系系主任、教授）

电子信息工程组

组　长：秦会斌（兼）

成　员：（成员按姓氏笔画排列）
王　荣（解放军理工大学通信工程学院电信工程系系主任、教授）
朱宁一（解放军理工大学理学院基础电子学系系主任、工程师）
李国民（西安科技大学通信与信息工程学院院长、教授）
李邓化（北京信息工程学院信息与通信工程系系主任、教授）
吴　谨（武汉科技大学信息科学与工程学院电子系系主任、教授）
杨马英（浙江工业大学信息工程学院副院长、教授）
杨瑞霞（河北工业大学信息工程学院院长、教授）
张雪英（太原理工大学信息工程学院副院长、教授）
张　彤（吉林大学电子科学与工程学院副院长、教授）
张焕君（沈阳理工大学信息科学与工程学院副院长、副教授）
陈鹤鸣（南京邮电大学光电学院院长、教授）
周　杰（南京信息工程大学电子与信息工程学院副院长、教授）
欧阳征标（深圳大学电子科学与技术学院副院长、教授）
雷　加（桂林电子科技大学电子工程学院副院长、教授）

项目策划：毛红兵

策　　划：曹　昳　寇向宏　杨　英　郭　景

前　言

通信网络安全与保密技术是以信息安全为基础的确保网络安全畅通的综合技术。现代通信已进入计算机数字通信时代，可以说，现代通信网络的核心就是计算机通信网络，本书的核心内容也正是计算机通信网络的安全与保密技术。随着计算机网络、数据通信、电子商务、办公自动化等领域的快速发展，信息安全问题日趋重要。为了满足社会对通信网络安全技术的迫切需求，各高等院校计算机科学与技术、通信工程以及电子信息工程等信息技术类本科专业相继开设了有关信息安全方面的课程。为了满足这些课程的需要，我们本着内容全面、强调实践的原则编写了本教材。

本教材是作者在多次讲授通信网络安全技术类本科课程的基础上，参考国内外相关文献，经过重新整理，编写而成的。在编写过程中，力求做到突出重点、注重知识点的结合、强调基本概念和基本方法、深入介绍安全协议。

本教材共分 8 章。第 1 章对通信网络安全所涉及的基本概念、研究内容、安全服务、安全标准等进行了概括性的介绍。通过本章的学习，使读者对本课程有一个比较全面的了解，激发学习兴趣。第 2 章详细讲解了计算机病毒的组成结构、基本概念和基本原理，介绍了一些基本的研究方法，使读者建立基本的概念，增强对计算机病毒的认识，掌握计算机病毒的诊断方法。本章还具体分析了几种病毒实例。第 3 章讲解了通信网络所涉及的密码技术，重点介绍了对称密码体制和非对称密码体制，并且具体分析了典型的对称密码算法 DES 和典型的非对称密码算法 RSA。第 4 章详细介绍了认证、访问控制、机密性、完整性以及不可否认性等基本的安全服务。第 5 章介绍了防火墙的基本知识，重点介绍了包过滤技术和代理服务技术，并且简单介绍了 Firewall-1 等防火墙产品。第 6 章介绍了安全管理的概念和协议，介绍了安全审计的方法，详细介绍了入侵检测技术。第 7 章介绍了安全体系结构的概念，详细介绍了 IPSec 安全协议、SSL 安全协议和 TLS 安全协议，使读者对安全协议有一个比较深入的了解。第 8 章介绍一些实用的安全工具，包括病毒清除工具、扫描工具以及入侵检测工具等。本教材每一章后都有小结和习题。

本教材适合作为计算机科学与技术、电子信息工程、通信工程以及电子信息工程等信息技术类本科专业信息安全相关课程的教学用书，也可作为相关工程技术人员的参考书。

本教材由王景中、徐小青和曾凡锋编写。参加本书编写工作的还有苏东峰、张璐、冯祎、张鹏、史峰、范金龙、吕游、李丹、李小科、杜飞等。在本书的编写过程中，北京邮电大学信息安全中心杨义先教授提出了许多宝贵意见，并且审阅了全部书稿，西安电子科技大学出版社的曹昳编辑对本书的出版给予了大力支持，在此一并表示感谢。

由于作者水平有限，书中难免有不妥之处，敬请读者批评指正。

编　者

2008 年 6 月

目　录

第1章 绪 论

现代通信已进入计算机数字通信时代，可以说，现代通信网络的核心就是计算机通信网络。本书所讲授的通信网络的安全与保密，其核心内容就是计算机通信网络的安全与保密技术。

计算机通信网络是计算机技术与通信技术的有机结合，是两台以上具有自治功能的计算机通过传输媒体连接在一起，在通信协议的作用下，实现信息传输、信息共享和信息处理的系统集合。通信网络的安全与保密技术是以信息安全为基础的确保网络安全畅通的综合技术。

在当今的网络信息时代，计算机网络无所不在，它为人们的工作、学习和生活等诸多社会活动提供了十分方便、快捷的手段。特别是因特网的出现，在某种程度上使我们的社会活动发生了根本的转变。通过计算机网络，我们可以不出家门就能了解世界各地所发生的新闻，浏览世界著名图书馆的图书资料，随时随地通过网络欣赏电影、音乐、电视连续剧，收集我们所需要的各个方面的信息，足不出户就能购买商品，管理自己的银行存款，进行股票交易，在家里就能完成自己的工作任务，并且随时与工作单位保持联系。计算机网络的飞速发展和应用也加快了各种新技术、新知识、新文化的传播，涉及到社会、政治、军事、经济、文化、医疗、社会保障、交通、通信、商务、生产、学习、交流等各个领域，极大地影响着社会、团体、个人自身内部以及相互之间关系的思维方式和行为方式。

计算机网络是以网络服务的形式为我们提供各种功能和帮助的。这些服务的提供，一方面需要完善的计算机网络基础设施，另一方面，需要完善的保障体系。计算机网络基础设施由网络硬件和通信软件构成，构成网络服务的信息存储、处理以及传输平台；而完善的保障体系则保证了信息传输、信息共享和信息处理的安全实现。如果没有通信信息的安全保证，那么我们从计算机网络获得的服务将是非常有限的，而且其服务质量也无从保证。

从通信网络的组成方面来讲，计算机网络由用户资源子网络和通信子网络构成。用户资源子网由用户终端以及网络接口设备构成，主要完成信息的收与发、信息处理等功能，直接向用户提供服务；通信子网主要由信息传输媒体、传输设备、路由设备等构成，主要完成信息传输的功能。因此，计算机网络不但涉及在用户终端上直接为用户提供的信息处理功能，也涉及到在传输媒体、传输设备中的信息传输功能。所以通信网络安全问题贯穿于整个通信网络的各个方面，涵盖了网络信息的存储、处理和传输各个过程。

1.1 信息安全基础

通信网络的功能就是网络信息的存储、传输、共享和处理，因此，通信网络安全问题

就是网络信息在存储、传输、共享和处理等阶段的安全问题，广义地讲，就是信息安全问题。本节首先介绍信息概念的发展，然后介绍有关信息的定义和特性，最后给出信息安全的概念。

1.1.1　信息的定义

由于信息概念本身的复杂性以及应用的广泛性，在不同的领域，对信息有着不同的定义，它们从不同的角度、不同的层次揭示了信息的特征与性质，但也都有这样或那样的局限性。

1948 年，维纳(N.Wiener)从控制论的角度给出了信息的定义：“信息是人们在适应外部世界并且使这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容的名称”。这个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。

意大利学者朗高(G.Longo)在 1975 年提出“差异就是信息”的观点，他指出，“信息是反映事物的形成、关系和差别的东西，它包含在事物的差异之中，而不在事物本身”。目前，这个观点被普遍接受。

在通信领域，人们对信息的研究有着悠久的历史，信息科学是通信理论研究的最重要的内容之一，目前普遍接受的对信息的定义是：信息是事物运动的状态与方式，是事物的一种属性。

在通信领域，有几个常见的概念需要加以区别。信息不同于消息，消息只是信息的外壳，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。信息不同于情报，情报通常是揭示秘密的、专门的、新颖的一类信息；可以说所有的情报都是信息，但不能说所有的信息都是情报。信息也不同于知识，知识是认识主体所表达的信息，是逻辑化的信息，并非所有的信息都是知识。

1.1.2　信息技术

在计算机通信领域，信息技术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、音频以及语音信息的方法与设备的总称。这个定义从功能方面揭示信息技术的本质。从语法角度来看，“信息技术”作为专门术语，其概念的本质是“技术”而非“信息”。

我们学习通信网络安全与保密，主要强调信息技术是信息的获取、处理、存储、变换这一过程中的有关技术，而重点主要集中在这些过程中的信息安全技术上。

1.1.3　信息系统

信息系统有两种定义：一种是广义的定义，它定义的信息系统包括的范围很广，各种处理信息的系统都可以认为是信息系统，包括人体本身和各种人造系统；第二种是狭义的定义，它定义的信息系统是指基于计算机的系统，是人、规程、数据、网络、硬件和软件等各种设施、工具和运行环境的有机结合，它突出的是计算机和网络通信等技术的应用。

1.1.4 信息安全

信息安全是一个广泛和抽象的概念，在信息处理过程中涉及的安全问题统称为信息安全问题。本书涉及的信息安全概念是狭义的，主要用于计算机通信网络的信息系统安全，是指在信息获取、加工、存储、变换、显示和传输等过程中，确保信息不被未授权者所获得并非法使用或篡改。

具体来讲，信息安全的定义是，确保以电磁信号为主要形式的、在计算机网络化系统中进行获取、处理、存储、传输和利用的信息内容，在各个物理位置、逻辑区域、存储和传输介质中的机密性、完整性、可用性、可审查性和不可否认性，使这些信息内容与人、通信网络、环境有关的技术和管理规程形成有机集合。这里的人指信息系统的主体，包括各类用户、支持人员以及技术管理和行政管理人员；通信网络则指计算机和网络互联设备、传输介质、操作系统、通信协议和应用程序所构成的物理的和逻辑的完整体系；环境则指系统稳定和可靠运行所需要的保障系统，包括机房、动力保障与备份以及应急与恢复系统。

1.1.5 通信网络安全与保密

通信网络是计算机网络中信息传输的子系统，它的安全直接影响到信息传输的状态和为用户提供的服务的质量。通信网络安全工作主要是对计算机和计算机之间相连接的传输线路、设备和协议进行管理，特别是对通信网络的组成方式、拓扑结构和网络应用进行管理，保障信息传输的安全性。这里所说的通信网络包括各种类型的计算机局域网、通信与计算机相结合的广域网，以及更为广泛的因特网。通信网络的安全与保密主要是保护网络系统中的硬件、软件及其数据和数据的传输不因偶然或者恶意原因而遭到破坏、更改和泄露，是系统能够连续可靠地正常运行，使网络服务不中断。

本书所研究的通信网络包含用户资源子网络和通信子网络，因此，所研究的通信网络安全与保密技术涵盖了网络信息的获取、传输、存储、处理和检索等方面。

1.2 通信网安全研究的内容

数字通信网络有三个主要的组成部分，即若干个为用户提供服务的主机结点，结点交换机与通信链路构成的通信子网，以及协调主机与主机之间、主机与通信子网络之间信息交换的通信协议。从网络安全的角度来看，通信子网和通信协议是实现网络通信的基本要素，因此，我们可以把通信网络看成是由主机和通信网络构成的系统。网络安全研究的内容也围绕着这两个组成部分展开。对主机安全的研究主要进行通信设备(以计算机为基础)安全技术的研究；对通信网络安全的研究主要进行通信信息安全技术的研究。两方面研究的基础都是信息安全技术。当然，随着计算机技术、通信技术和信息安全技术的发展，计算机安全技术与通信信息安全技术朝着不断融合的方向发展，不可能把二者截然分开。它们都从不同的角度涉及计算机病毒、密码技术、安全服务、安全体系结构、安全协议、安全管理协议、入侵检测与安全审计等方面的内容。

1.2.1　防病毒技术

现代数据通信网络的主要设备(通信终端、路由器、交换机等)都是以计算机为基础的通信设备，而目前计算机设备安全的最大危害之一就是计算机病毒，且大部分计算机病毒通过网络进行传播，其传播速度快，传播面广，危害程度大，已经成为通信网络安全的重要威胁。因此，在通信网络安全建设过程中，必须考虑对计算机病毒的防护。

1.2.2　保密技术

保密技术在通信网络中的具体体现是密码技术。基于密码学的密码技术是计算机通信网络安全的核心技术，密码技术几乎渗透到信息系统安全的各个领域以及大部分安全机制之中。密码学是研究信息安全保密的学科，是保护信息在信道的传输过程中不被窃取、解读和利用的方法。它是信息安全学科建设和信息系统安全工程实践的基础理论之一。

随着社会信息化的不断发展，信息的商品属性也慢慢显露出来，信息商品的存储和传输的安全也日益受到广泛的关注。如果非法用户获取系统的访问控制权，从存储介质或设备上得到机密数据或专利软件，或根据某种目的修改了原始数据，那么网络信息的机密性、完整性、可用性、真实性和可控性将遭到破坏。如果信息在通信传输过程中受到不同程度的非法窃取，或虚假的信息和计算机病毒充斥最终的信息系统，使得系统无法正常运行，将造成真实信息的丢失和泄露，会给使用者带来经济或者政治上的巨大损失。

密码技术研究的领域相当广泛。从信息的层次来看，包括信息的来源、去向、真实性、完整性、保密性以及信息的发送者和接收者无法否认自己所做过的操作行为的不可否认性。从网络层次来看，网络和信息系统随时可用，运行过程中不出现故障，如果遇到意外攻击，能够尽量减少损失并尽早恢复，保证信息的可靠性。由此可见，密码技术是信息安全技术的核心技术，几乎所有的安全服务都可以用密码技术来实现。

1.2.3　通信网络安全技术

通信网络安全(网络安全)技术是一个相对复杂的领域，它是一门涉及计算机科学、网络通信、密码学、应用数学、数论、信息论等多种学科的综合性学科。具体地说，网络安全是指网络系统的硬件、软件及系统中的数据受到保护，不被意外的或者恶意的操作破坏、更改和泄露，保证系统连续可靠正常地运行，保证网络服务不中断。就其本质而言，通信网络安全是一种动态的信息安全问题。从广义上来说，凡是涉及到网络上信息的机密性、完整性、可用性、真实性和可控性的相关技术和理论，都是通信网络安全的研究领域。

可以从三个层次来说明网络安全涉及的主要内容。第一个层次涉及到密码学的研究，密码技术是网络安全技术的基础和核心，密码技术不等同于网络安全技术，但有直接的关系；第二个层次是基本的安全技术，包括安全机制、安全方法等；第三个层次是应用系统的安全，应用系统根据不同的需求，需要结合密码技术和基本的安全技术，网络安全最终的目的是保障应用的安全。

从对安全的处理角度来看，网络安全包含四个主要内容：第一是网络攻击，网络攻击也是网络安全的一个组成部分，对网络攻击的研究可以加深对网络脆弱性的认识和了解；

第二是安全防御，即网络安全措施，重点在于怎样保护网络信息的安全，使之可以对抗网络攻击；第三是攻击检测，即除了做好安全防御外，还应该对网络攻击进行检测，识别出网络攻击行为，检测出潜在的威胁；第四是应急处理和灾难恢复，即在紧急情况下的应急处理手段和措施，及在安全事件发生后对损失的恢复。

1.3 安全威胁

安全威胁是指某个人、物或者事件对某一资源的机密性、完整性、可用性或者合法性所造成的危害。攻击是威胁的具体体现。

通信网络的发展，使信息共享日益广泛与深入。但是信息在公共通信网络上存储、共享和传输，会被非授权的入侵者非法窃听、截取、篡改或毁坏，从而导致不可估量的损失，尤其是在银行系统、商业系统、管理部门、政府或军事领域中，人们对公共通信网络中的存储与传输数据的安全问题更为关注。如果因为安全因素，使得我们不敢把信息放进因特网这样的公共网络，那么办公效率及资源的利用率都会受到影响，甚至使人们丧失了对因特网及信息高速公路的信赖。因此，在研究网络安全时，首先要了解通信网络系统面临的各种威胁，这样，我们才能有的放矢地对抗这些威胁。

1.3.1 基本的安全威胁

安全威胁是一个内容广泛的概念。本课程主要研究与通信网络安全相关的基本安全威胁，主要包括以下几种类型：

(1) 非授权访问，指一个非授权用户的入侵。

(2) 信息泄露，指造成将有价值的和高度机密的信息暴露给无权访问该信息的人的所有安全问题。

(3) 拒绝服务，指使系统难以或不能继续执行任务的所有安全问题。

对非授权访问威胁所造成的破坏的评估，要考虑这个威胁所造成的影响有多大，包括受影响的用户数量、受到的破坏程度以及可能由于非授权访问而泄露的信息的机密性。对于某些组织来说，入侵将动摇该组织中其他人的信心。而入侵者往往将目标对准政府部门或学术组织，它们是对入侵最难以处理的单位。但对于大多数单位来说，除非入侵涉及到信息泄露和拒绝服务，否则非授权访问不是一个主要问题，通过加强访问控制，可以有效地对付这种威胁。

信息泄露威胁造成的危害取决于可能泄密的信息类型。具有高机密级的信息系统不应该直接连接到因特网上，要有隔离措施。私人信息、健康信息、公司计划和信用记录等都具有一定程度的机密性，必须给予保护。在大多数情况下，可以利用标准的 UNIX 文件给这类信息提供适当的保护。然而在某些情况下，这类信息泄露出去的责任风险，足以阻止存储该信息的主机连接到因特网。通过加密技术可以对付信息泄露的威胁。

拒绝服务威胁的典型结果是系统瘫痪，停止运行，线路断开。这种威胁的产生来自于多方面。有意攻击可以产生这种威胁，无意的系统运算错误也可以产生这种威胁，计算机病毒也可以产生这种威胁。

在一个通信网络中，这几种安全威胁不是孤立存在的，它们往往互相结合，共同对网络产生作用，因此，在对付威胁的时候，我们要进行综合考虑。

1.3.2　攻击类型

通信网络中，我们把安全威胁的具体实现叫做安全攻击。本课程研究几种常见的攻击类型。

1．冒充

冒充就是一个实体假装成另一个不同的实体实施非法攻击。在信息安全概念中，实体是指实施安全防护或者实施非法攻击的客体，包括人或者物。冒充常被与其它类型的主动攻击形式一起使用，特别是消息的重放与篡改。例如，认证序列能够被截获，并在一个有效的认证序列发生之后被重放。特权很小的实体为了得到额外的特权，可能通过冒充装扮成具有某些更大特权的实体。用别人的账号和口令进入计算机系统也是冒充的例子。

2．重放

非授权用户通过录制并重放授权用户的消息而对系统进行的攻击，称为重放。例如，一个含有认证信息的有效消息可能为另一个实体所截获，然后进行重放，其目的是让验证方来认证这个实体，使得他所进行的其它非法操作合法化。重放攻击对金融业务会构成很大的威胁。

3．消息篡改

所传送的内容被改变而未被发觉，并导致一种非授权的后果，叫做消息篡改。例如，消息“允许用户 A 读机密文卷账目”被篡改为“允许用户 B 读机密文卷账目”，而这里用户 B 是未经过授权的用户，没有权限读取这些机密文卷账目，B 一旦读取了这些信息，就可能泄露这里的机密，并且对后续事物产生不良影响。

4．服务拒绝

当一个实体不能执行它的正常功能，或它的动作妨碍了别的实体执行它们的正常功能时，便发生服务拒绝。这种攻击可能是一般性的，例如一个实体抑制所有的消息，也可能是有具体目标的，例如一个实体可以抑制所有流向某一特定目的端的消息，如安全审计服务。

这种攻击可能是对通信业务流的抑制，或产生额外的通信业务流，也可能是制造出试图破坏网络操作的消息，特别是如果网络具有中继实体，这些中继实体根据从别的中继实体那里接收到的状态报告做出路由选择的决定，进而可能造成网络的阻塞，终止网络服务。

5．内部攻击

当系统的合法用户以非故意或非授权方式进行操作时，会出现内部攻击。多数已知的计算机犯罪都和内部攻击有密切的关系，它对系统安全的损害非常大，这就像日常生活中的内部作案一样，防不胜防。在计算机通信安全系统中用来防止内部攻击的保护方法包括：对工作人员进行仔细审查；仔细检查硬件、软件、安全策略和系统配制，以便在一定程度

上保证它们运行的正确性(称为可信功能度)；审计跟踪可以提高检测出这种攻击的可能性。

6. 外部攻击

外部攻击是指从系统的外围环境出发，对系统进行攻击。外部攻击常用的方法有搭线(主动的与被动的)、截取辐射、冒充为系统的授权用户或冒充为系统的组成部分、为认证或访问控制机制设置旁路。

7. 陷门

当系统的实体受到改变，致使一个攻击者能对命令及预定的事件或事件序列产生非授权的影响时，其结果就称为陷门。例如，口令的有效性可能被修改，使得除了其正常效力之外，攻击者的口令也生效。

8. 特洛伊木马

信息系统中所说的特洛伊木马，是指此类程序不但具有自己的授权功能，而且还有非授权功能。一个向非授权信道拷贝消息的中继就是一个特洛伊木马。

1.4 安 全 服 务

在通信网络中，系统提供的主要的安全防护措施被称做安全服务。通用的安全服务有5种，即：认证服务，提供某个实体的身份的保证；访问控制服务，保护资源免遭非法使用和操纵；机密性服务，保护信息不被泄露或暴露给未授权的实体；数据完整性服务，保护数据以防止未授权的修改、删除或替代；不可否认服务，防止参与某次通信交换的一方事后否认本次交换曾经发生过。

为某一安全区域所制定的安全策略决定着在该区域内或者在与其它区域进行通信交换时，应采用哪些安全服务。它也决定着在什么条件下可以使用某个安全服务，以及对此服务的任意一个变量参数施加什么限制。

在通信网络环境中，主要提供上面 5 种通用的服务。这些安全服务以及它们的各种组合，在一定程度上可实现不同环境的安全目的。

1.4.1 认证服务

认证是一种最重要的安全服务，因为在某种程度上其它所有的安全服务都依赖于它。认证是对付假冒攻击的有效方法。认证服务提供了关于某个实体身份的保证。这意味着当某个实体声称具有一个特定的身份时，认证服务将通过某种方法来证实其是否具有这一身份。口令认证就是一种最简单的认证方法。

认证用于一个特定的通信过程，在此过程中需要提交实体的身份。认证又分为实体认证和数据起源认证两种形式。

如果身份是由参与某次通信连接或会话的远端的一方提交的，则这种情况下的认证服务被称做实体认证。这种认证只是简单地认证实体本身的身份，不会和实体想要进行的某种活动联系起来。显然，它的作用是有限的，因为实体通常是希望在识别身份的基础上执行其它操作的。因此，在实际工作中，实体认证通常会产生一个明确的结果，允许实体进

行其它活动或通信。例如在实体认证过程中将产生一个对称密钥，可以用来解密一个文件进行读写，或者与其它实体建立一个安全通信通道。实体身份一旦获得认证，也可以和访问控制列表中的权限关联起来，决定能否进行访问。

如果身份是由声称它是某个数据项的发送者的那个实体所提交的，此身份连同数据项一起发送给接收者，则这种情况下的认证服务被称做数据起源认证。这种认证就是认证某个指定的数据项是否来源于某个特定的实体。这既不是孤立地认证一个实体，也不是为了允许实体执行下一步的操作而认证它的身份，而是为了确定被认证的实体与一些特定数据项有着静态的不可分割的联系。

在达到基本的安全目标方面，上述两种类型的认证服务都具有重要的作用。数据起源认证是保证部分完整性目标的直接方法，即保证知道某个数据项的真正起源。而实体认证则采用以下各种方式，以便达到安全目标。

第一，它作为访问控制服务的一种必要的支持，访问控制服务的执行依赖于确知的身份；

第二，它作为提供数据起源认证的一种可能的方法；

第三，它作为对责任原则的一种直接的支持，例如，在审计追踪过程中做记录时，提供与某一活动相联系的确知身份。

1.4.2　访问控制服务

访问控制的目标是防止对任何计算机资源、通信资源或信息资源进行未授权的访问。所谓未授权访问，包括未经授权的使用、泄露、修改、销毁以及颁发指令等。访问控制直接支持机密性、完整性、可用性以及合法使用的安全目标。它对机密性、完整性和合法使用所起的作用是十分明显的。它对可用性所起的作用，取决于对访问者的有效控制。

访问控制是实施授权的一种方法，它既是通信安全的问题，又是系统安全的问题。然而，由于必须在系统之间传输访问控制信息，因此它对通信协议具有很高的要求。

访问控制的一般模型假定了一些主动的实体，称为发起者或主体。它们试图访问一些被动的资源，称做目标或客体。授权决策控制着可以由哪些发起者，在何种条件下，为了什么目的，来访问哪些目标。这些决策以某一访问控制策略的形式反映出来，通常使用一个访问控制列表来表示。访问请求通过某个访问控制机制而得到过滤。

访问控制的另一作用是保护敏感信息不经过有风险的环境传送。这涉及到对网络的业务流或消息所实施的路由控制。所谓路由控制，是指选路规则，以选择或绕过指定的网络、连接或中继。访问控制服务的深入讨论主要涉及两个内容，一个是访问控制策略的类型，另一个是各组成部分的物理构成。

1.4.3　机密性服务

机密性服务就是保护信息不被泄露。通常，存储和传输中的某一数据项构成了某种形式的信息通道，数据的泄露自然就会导致信息的泄露，因此，保护数据不泄露是机密性的最基本的要求。然而，在计算机通信环境中，数据本身并不是唯一的信息通道，我们还可以通过其它通道获取信息。比如，我们通过观察某一数据项存在与否(不管它的内容)，就可