普通高等教育“十一五”国家级规划教材

信息安全学

第2版

周学广　等编著
海军工程大学

为教师配有电子课件

机械工业出版社
China Machine Press

普通高等教育“十一五”国家级规划教材

信息安全学

第2版

周学广　张焕国　张少武
周学军　潘　恒　薛丽敏　编著

机械工业出版社
China Machine Press

本书从信息安全的基本概念、信息安全的支撑技术以及信息安全应用技术三个方面向读者全面介绍信息安全领域的相关知识。本书题材新颖，讲解力求深入浅出。每章均提供了丰富的习题，便于学生巩固基本知识，并为教师开展教学提供方便。

本书是长期从事信息安全研究和教学的作者群的智慧结晶，可作为信息安全、计算机、通信工程专业及相关专业本科生和研究生教材，也可作为信息安全工程师、网络安全管理员和信息技术类用户的培训教材和参考书。

图书在版编目（CIP）数据

信息安全学　第2版/周学广等编著. —北京：机械工业出版社，2008.1
（普通高等教育"十一五"国家级规划教材）
ISBN 978-7-111-22276-7

Ⅰ.信…　Ⅱ.周…　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137404号

机械工业出版社(北京市西城区百万庄大街22号　邮政编码　100037)
责任编辑：朱　劼
三河市明辉印装有限公司印刷·新华书店北京发行所发行
2008年1月第2版第1次印刷
184mm×260mm·18.75印张
定价：32.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换
本社购书热线：(010)68326294

作者介绍

周学广，海军工程大学电子工程学院信息安全系副主任，教授，硕士研究生导师。毕业于解放军信息工程大学电子技术学院，分别于1989年7月和1992年1月获得工学学士和军事学硕士学位，现在武汉大学计算机学院在职攻读博士学位。长期从事信息安全教学与科研工作，先后主持和参与军队科研课题8项，获军队科技进步奖5项，公开发表学术论文20余篇，主编的教材《信息安全学》(第1版)被教育部推荐为“研究生教学用书”。

张焕国，武汉大学计算机学院教授，博士研究生导师，主要从事信息安全方面的教学科研工作。先后担任中国密码学会理事，中国计算机学会容错专业委员会副主任，国家信息安全成果产业化基地(中部)专家委员会副主任等职。曾主编《密码学引论》等专著多部，在《计算机学报》、《中国科学》、《通信学报》上发表论文多篇，获得部级科技进步奖多项。

张少武，解放军信息工程大学电子技术学院教授，硕士研究生导师。1985年7月毕业于武汉大学，1991年1月毕业于解放军信息工程大学并获得军事学硕士学位。长期从事密码编码的理论和密码系统设计的教学与科研工作，先后主持、参加和完成国家和军队科研课题10项，获军队科技进步一、二、三等奖各一项，公开发表论文30余篇。

周学军，海军工程大学电子工程学院通信工程系主任，博士，教授，硕士研究生导师。1983年7月毕业于西安电子科技大学电子对抗专业，在解放军理工大学和国防科技大学分别获硕士和博士学位。长期从事军事通信与信息工程教学和科研工作，是军队重点建设学科“军事通信工程”的负责人。获军队教学成果奖2项，科技进步奖8项，发表学术论文30余篇，编写50余万字的教材和公开出版的专业著作。

潘恒，中原工学院副教授，博士。1999 年毕业于解放军理工大学，获工学学士学位，2002 年和 2006 年于解放军信息工程大学，先后获得军事学硕士学位和工学博士学位。主要研究方向为密码学、信息安全技术。参加过 2 项国家自然科学基金、2 项军队科技攻关，主持河南省自然科学基金 1 项，公开发表论文 15 篇，三大检索 9 篇次，获军队科技进步奖 1 项，获河南省自然科学优秀论文一等奖 1 项。

薛丽敏，海军指挥学院信息安全研究室副教授，1989 年 7 月毕业于北方交通大学软件工程专业，获工学学士学位，在海军工程大学获得工学硕士学位。主要从事通信与信息系统、信息安全、信息对抗等方面的研究和教学工作，获军队科技进步奖 1 项，公开发表学术论文多篇。

序（第1版）

信息社会的兴起，给全球带来了信息技术飞速发展的契机；信息技术的应用，引起了人们生产方式、生活方式和思想观念的巨大变化，极大地推动着人类社会的发展和人类文明的进步，把人类带入新时代；信息系统已逐渐成为社会各个领域不可或缺的基础设施；信息已成为社会发展的重要战略资源、决策之源和控制战场的灵魂；信息化水平已成为衡量一个国家现代化和综合国力的重要标志。争夺“制信息权”已成为国际竞争的重要内容。

党中央及时提出大力推进国民经济和社会信息化，做出“以信息化带动工业化，发挥后发优势，实现社会生产力的跨越式发展”的重要决策，信息网络系统的建设和应用必将成为新世纪国家发展的重点。江泽民同志曾指出：各地各部门的领导干部，必须加紧学习网络化知识，高度重视网上斗争的问题。我们的党建工作、思想政治工作、组织工作、宣传工作、群众工作，都应适应信息网络化的特点，否则是很难做好的。总之，对信息网络化问题，我们的基本方针是积极发展，加强管理，趋利避害，为我所用，努力在全球信息网络化的发展中占据主动地位。

然而，人们在享受信息网络所带来的巨大利益的同时，也面临着信息安全的严峻考验。信息安全已成为世界性的现实问题，信息安全与国家安全、民族兴衰和战争胜负息息相关。没有信息安全，就没有完全意义上的国家安全，也没有真正的政治安全、军事安全和经济安全。面对日益明显的经济、信息全球化趋势，我们既要看到它带给我们的发展机遇，也要正视它给我们带来的严峻挑战。国家“十五”国民经济发展计划决定要“强化信息网络的安全保障体系”。因此，加速信息安全的研究和发展，加强信息安全保障能力已成为我国信息化发展的当务之急，成为国民经济各领域电子化成败的关键，成为提高中华民族生存能力的头等大事。为了构筑21世纪的国家信息安全保障体系，有效地保障国家安全、社会稳定和经济发展，需要尽快并长期增强广大公众的信息安全意识，提升信息系统研究、开发、生产、使用、维护、教育管理人员的素质和能力。

当前，美国等发达国家十分重视信息安全保障，把信息争夺与对抗作为未来国与国之间斗争的主要方式。美国最早关注通信保密，1990年以后提出信息战及信息安全概念，1998年5月克林顿总统发布了《对关键基础设施保护政策第63号总统令》(PDD63)，美国国家安全局于同年10月提出信息保障技术框架(IATF 1.1版)。这一系列举措表明了美国作为全球化浪潮的领导者，正在利用信息霸权谋求主宰世界，正在准备信息威慑及战略信息战。因此，要把我国的信息安全问题放在全球战略角度考虑，也就是放在政治角度来考虑。

当前，信息安全的概念正在与时俱进。它从早期的通信保密发展到关注信息的保密、完整、可用、可控和不可否认的信息安全，并进一步发展到如今的信息保障和信息保障体系。单纯的保密和静态的保护都已不能适应今天的需要。信息保障依赖人、操作和技术实现组织的任务/业务运作。针对技术/信息基础设施的管理活动同样依赖于这三个因素。稳健的信息保障状态意味着信息保障和政策、步骤、技术与机制在整个组织的信息基础设施的所有层面上均能得以实施。

可以这样说，面向数据的安全概念是信息的保密性、完整性和可用性，而面向使用者的安全概念则是鉴别、授权、访问控制、抗否认性和可服务性以及基于内容的个人隐私、知识产权等的保护。这两者结合就是信息安全体系结构中的安全服务，而这些安全问题又要依靠密码、数字签名、身份验证技术、防火墙、安全审计、灾难恢复、防病毒、防黑客入侵等安全机制(措施)加

以解决。其中密码技术和管理是信息安全的核心，安全标准和系统评估是信息安全的基础。总之，从历史的人网大系统的概念出发，现代的信息安全涉及个人权益、企业生存、金融风险防范、社会稳定和国家的安全。它是物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全与公共信息安全的总和。

信息技术的发展与广泛应用，已经并还将深刻地改变人们的生活方式、生产方式与管理方式，对推进国家现代化、推进社会文明的发展产生日益重大的影响。由于信息技术本身的特殊性，在整个信息化进程中，必将带来巨大的信息安全风险。信息安全问题涉及国家安全、社会公共安全和公民个人安全的方方面面。要使我们的信息化、现代化的发展不受影响，就必须克服众多的信息安全问题，化解日益严峻的信息安全风险，因此，面对日益迫切的需要，唯一的出路就是尽快培养信息安全方面的专业人才，加大信息安全教育的普及力度，树立国民的信息安全意识，建设好国家的信息安全边防线。本书作为高等院校计算机教材，为培养信息安全专业人才，普及信息安全教育提供了有力的支持。

本书有以下几个特点：

1)内容翔实、覆盖面广，较完整地给出了信息安全的体系结构，有较强的系统性和实用性，能够满足军队和地方院校相关专业的教学需要。

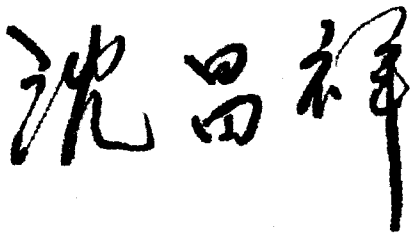
2)选材精，技术新。本书既介绍密码学与密码分析学、信息安全测评认证和美国高级加密标准等先进技术和原理，也讨论了企业和个人信息安全、国家和军队信息安全等最新的信息安全技术综合应用。

3)图文并茂，深入浅出。本书包括大量的图片和阅读重点提示，并提供了指导读者进一步学习的参考文献。

本书的主编都是信息科学领域的年轻人，长期从事该领域的教学和科研工作，成绩斐然，特别是在编写计算机和信息专业教材和技术专著方面都积累了丰富的经验。本书主编之一周学广副教授是从事军事信息安全教学和科研的专家，已出版专业教材和教学用书5部，并多次获奖。本书另一位主编刘艺副教授是知名的计算机技术作家，编著和翻译了大量的计算机专著，目前已经正式出版的有10部。他还曾荣获过全军软件比赛一等奖。

两位主编力邀我为本书作序，虽工作繁忙，但通读全书，得益不浅，欣然提笔，是为序。

中国工程院院士、国家信息化专家咨询委员会委员



2002年11月4日于武汉

前　言

本书第1版自2003年3月出版以来，已在全国多所高校使用。从教学反馈意见来看，本书对我国的信息安全普及教育和提高全民信息安全意识起到了积极的作用。承蒙中国工程院院士、国家信息化专家咨询委员会委员沈昌祥先生为本书第1版作序，对他提出的建议以及宝贵的修改意见，我们表示诚挚的谢意。

2003年7月，中办[2003]27号文转发的《国家信息化领导小组关于加强信息安全保障工作的意见》成为在经济全球化深入发展、社会信息化全面加快的新形势下加强中国信息安全保障工作的纲领性文件。

在这个大背景下，我们深感原教材的分量和内容均不足以适应信息安全如火如荼的发展需要。在机械工业出版社华章分社领导和编辑朋友们的大力支持下，我们提出了《信息安全学　第2版》的选题申请，于2005年底通过机械工业出版社申报了普通高等教育"十一五"国家级规划教材并获得成功，在此，向机械工业出版社华章分社的领导和朋友们表示衷心的感谢。

本书第2版的编写工作得到了海军工程大学的大力支持，海军工程大学研究生院给予了热心资助，电子工程学院通信工程系以及信息安全系的同事们给予了真切的关心、指导和热情帮助，在此向各级机关以及所有关心、支持本书出版工作的朋友表示衷心的感谢。

在第2版的编写过程中，我们组织了专家型写作班子。武汉大学计算机学院信息安全专业博士生导师张焕国教授编写第4章和第8章；解放军信息工程大学电子技术学院张少武教授编写第9章；海军工程大学电子工程学院通信工程系主任周学军教授编写第5章；中原工学院长期从事信息工程开发的潘恒副教授编写第10章；海军指挥学院信息安全研究室薛丽敏副教授编写第6章；周学广教授编写本书第1章、第2章、第3章、第7章和第11章，并负责全书的统稿、定稿工作。参与本书编写的还有刘艺副教授(参与11.1节和11.2节的编写)、傅子奇处长(参与5.3节和5.4节的编写)、刘可工程师(参与6.4节和6.5节的编写)、田巧云硕士(参与4.1节的编写)。与本书第1版相比，第2版新增内容5章，新增和修改篇幅达到50%以上。

在本书编写过程中，许多领导和专家给予了关注和指导，他们是：郭立峰、周长海、高敬东、李敬辉、温莉芳、苗小伟、陈林根、陈少昌、王丽娜、潘正运、贺国、孙允标、李殿伟，在此一并表示感谢。另外，除书后的参考文献外，本书还参考了许多作者的论文、著作等，由于篇幅所限无法一一列出，在此也对他们表示衷心感谢。

本书是普通高等教育"十一五"国家级规划教材，获得国家自然科学基金项目(60673071)、国家863计划项目(2006AA01z442)、海军工程大学研究生教材建设基金和军队"2110工程"(军事通信工程)的资助，特此致谢。

周学广　张焕国

2007年5月1日于武汉大学

目　录

第1章　信息安全概述

信息是与物质、能源同样重要的社会发展急需的重要战略资源，是衡量一个国家综合国力的重要参数。在信息时代的今天，每个国家的政治、军事、外交斗争都离不开信息，经济建设、科学发展和技术进步也离不开信息。信息的开发、利用和控制已经成为国家间利益争夺的重要目标，信息安全与国家安全息息相关。信息的地位与作用因信息技术的快速发展而急剧上升，信息安全问题也因此变得日益突出。未来的军事斗争将首先在信息领域展开，并全程贯穿着信息战。信息安全将成为赢得战争胜利的基础和重要保障。加强信息安全研究，营造信息安全氛围，既是时代发展的客观要求，也是做好未来军事斗争准备的迫切需要。

本章将阐述信息和信息安全的基本概念，介绍信息安全体系结构、信息安全管理体系、信息安全测评认证体系以及信息安全与法律等内容。

1.1　信息的定义与特征

信息是人类社会日常生活中必不可少的一项交流内容。以前，人们对信息和消息的含义没有进行明确区分，但进入20世纪后，尤其是近50年来，现代信息技术的迅猛发展对人类社会产生了深远影响，迫使人们开始研究信息的准确含义。

1.1.1　信息的定义

据不完全统计，在我国书刊上公开出现过的信息定义至少有30种。比较有代表性的有以下几种：

- 1928年，哈特莱(Hartley，L. V. R.)在《贝尔系统技术杂志》上发表了一篇名为“信息传输”的论文。在这篇论文中，他把信息定义为“选择通信符号的方式，且用选择的自由度来计量各种信息的大小”。[Hartley 1928]
- 1948年，信息论的奠基人香农(Shannon，C. E.)在《贝尔系统技术杂志》上发表的著名论文“通信的数学理论”中提出，信息是“两次不确定性之差异”，用以消除随机不确定性。[Shannon 1948]
- 1948年，控制论的创始人维纳(Wiener，N.)在他的专著《控制论：动物和机器中的通信与控制问题》一书中提出：“信息是人与外部世界互相交换的内容的名称。”[Wiener 1948]
- 1975年，意大利学者朗高(Longo，G.)在《信息论：新的趋势与未决问题》一书中指出：“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，而不存在于事物本身。”[Longo 1975]
- 1988年，中国信息论专家钟义信在《信息科学原理》一书中，把信息定义为“事物运动的状态和方式”。[钟义信 1988]

还有人从哲学的角度对信息的本质进行探讨，认为“信息是一切物质的属性”，信息是由物质到精神的转化物，既非物质又非精神，是独立的第三态；信息是与物质、能量密切相关的事物属性。有人从信息的实用意义来表述，把一切包含新的知识内容的消息、情报、数据、图像等统称为信息。

我们认为，所谓信息(information)，就是“客观世界中各种事物的变化和特征的最新反映，是客观事物之间联系的表征，也是客观事物状态经过传递后的再现。”[周学广 2003]

信息是主观世界与客观世界联系的桥梁，客观世界中不同事物都具有不同的特征，这些特征给人们带来不同的信息，而这些信息使人们能够认识客观事物。

1.1.2 信息的性质和特征

信息有两个根本作用，一是“表征”，二是“控制”。也就是说，信息是对现实事物的表征，且信息用于控制现实社会。例如，在现实生活中，人们的财富大多体现为银行存款数字和(或)股市里的股票数字。通过大量买卖某一只股票可以操控该股票价格，实现财富积累。这一过程可通过股市里股票信息的变化和银行存款信息的变化反映出来。

因此，信息有以下几个性质：

1)普遍性和可识别性。信息来源于物质和物质的运动，只要存在物质，只要事物有变化，或客体在运动着，就存在信息。信息不仅普遍存在，而且可以识别。人们可以通过感官或多种探测手段，直接或间接地识别客观事物的形状、特征以及变化所产生的信息，特别是找出其差异，这是认识信息的关键。

2)存储性和可处理性。信息依赖于物质和意识，又可以脱离物质和意识而独立存在，可以存储起来。信息存储就是利用信息载体将信息保存下来，以备今后再用，或先保存起来再进行分析整理。这是信息不同于物质、能源的重要特征。信息不仅可以存储，还可以处理，即对获得的大量纷繁的信息，根据目的进行筛选、分析、分类、整理、控制和使用。处理是为了开发和利用信息，也有利于传递和存储信息。

3)时效性和可共享性。信息有较强的时效性。一个信息生成、获得的越早，传递越快，其价值就越大。随着时间的推移，其价值会逐渐衰减以致失去其价值。信息的可共享性是指信息可以为多个主体所利用。

4)增值性和可开发性。信息资源的增值性主要表现在两个方面：一是对具体形式的物质资源和能量资源进行最佳配置，使有限的资源发挥最大作用；二是可以利用急剧增长的信息，发掘新的材料和能源。而信息本身也在不断使用中得到增值。信息还具有可开发性，人们要不断地探索和挖掘，才能充分地开发、利用信息资源。

5)可控性和多效用性。信息的可控性反映在三个方面：一是可扩充，二是可压缩，三是可处理。信息的可控性使信息技术具有可操作性，也增加了利用信息技术的复杂性。信息的多效用性是由信息具有的知识性决定的。无论是认识世界还是改造世界，信息都是基础，它是知识的源泉，决策的依据，控制的灵魂，管理的保证。

此外，信息还有转换性和可传递性、独立性和可继承性等特征。信息有很强的社会功能，主要表现在资源功能、启迪功能、教育功能、方法论功能、娱乐功能、舆论功能等方面。信息的社会功能是由信息的基本特征决定与派生的。

1.2 信息安全的基本概念

安全(safety)没有统一的定义，因此什么是真正的安全也没有标准答案。安全的基本含义可以归纳为：客观上不存在威胁，主观上不存在恐惧。也就是说，一个客体/系统客观上没有受到威胁，可以正常运行，做客体/系统应该做的事情；主观上不担心客体/系统自身受到威胁和破坏，提供客体/系统应该提供的服务。

社会进入信息化时代意味着社会对信息的深度依赖，正是这种深度依赖导致了信息安全问题的出现。

1.2.1 信息安全的定义

信息安全(information security)同样没有公认、统一的定义。国际、国内对信息安全的定义大致可以分成两类：一类是指具体的信息技术系统的安全；另一类是指某一特定信息体系(如一个国家的银行信息系统、军事指挥系统等)的安全。

我们把信息安全定义为“一个国家的社会信息化状态不受外来威胁与侵害；一个国家的信息技术体系不受外来的威胁与侵害”。因为信息安全首先是一个国家宏观的社会信息化状态是否处于自主控制之下、是否稳定的问题；其次才是信息技术安全问题。

1.2.2 信息安全的属性

不管入侵者怀有什么目的，采用什么手段，他们都要通过攻击信息的安全属性来达到目的。信息安全有以下5个基本属性。

1. 完整性

完整性(integrity)是指信息在存储或传输过程中保持不被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性。对于军用信息来说，完整性被破坏可能意味着延误战机、自相残杀或闲置战斗力。对信息安全发动攻击主要是为了破坏信息的完整性。

2. 可用性

可用性(availability)是指信息可被合法用户访问并按要求顺序使用的特性，即指当需要时可以使用所需信息。对可用性的攻击就是阻断信息的可用性，例如破坏网络和有关系统的正常运行就属于对可用性进行攻击。

3. 保密性

保密性(confidentiality)是指信息不泄露给未经授权的个人和实体，或被未经授权的个人和实体利用的特性。军用信息安全尤为注重信息的保密性(相比较而言，商用信息则更注重信息的完整性)。

4. 可控性

可控性(controllability)是指授权机构可以随时控制信息的机密性，美国政府提倡的“密钥托管”、“密钥恢复”等措施就是实现信息安全可控性的例子。

5. 可靠性

可靠性(reliability)指信息以用户认可的质量连续服务于用户的特性(包括信息的迅速、准确和连续地转移等)，也有人认为可靠性是人们对信息系统而不是对信息本身的要求。

“信息安全”的内在含义是指采用一切可能的办法和手段，千方百计保证信息的上述“五性”安全。信息对抗/信息攻击是指采用一切努力，破坏信息的上述“五性”安全。

1.2.3 信息安全的分类

信息安全可有多种不同的分类方式。表1-1给出了其中的一种分类。

表 1-1 信息安全的一种分类

分类		说明
监察安全	监控查验	发现违规
		确定入侵
		定位损害
		监控威胁
	犯罪起诉	起诉
		量刑
	纠偏建议	
管理安全	技术管理安全	多级安全用户鉴别技术的管理
		多级安全加密技术的管理
		密钥管理技术的管理
	行政管理安全	人员管理
		系统
	应急管理安全	应急的措施组织
		入侵的自卫与反击
技术安全	实体安全	环境安全(温度、湿度、气压等)
		建筑安全(防雷、防水、防鼠等)
		网络与设备安全
	软件安全	软件的安全开发与安装
		软件的安全复制与升级
		软件加密
		软件安全性能测试
	数据安全	数据加密
		数据存储安全
		数据备份
	运行安全	访问控制
		审计跟踪
		入侵告警与系统恢复等
立法安全	有关信息安全的政策、法令、法规	
认知安全	办学、办班	
	奖惩与扬抑	
	信息安全宣传与普及教育	

1.2.4 信息系统安全基本原则

国际经济合作与发展组织(Organization for Economic Cooperation and Development, OECD)于1992年11月26日一致通过了"信息系统安全指南"[OECD 1992],该指南制定了九项安全原则,欧美各国已明确表示在建设他们的国家信息基础设施(National Information Infrastructure, NII)时要遵从这一指南和九项原则。这九项原则是:

- **负责原则**:网络的所有者、提供者和用户以及其他有关方面应当明确各自对信息安全的责任。
- **知晓原则**:网络的所有者、提供者和用户及其他有关方面应当了解网络安全方面的措施、具体办法和工作程序。
- **道德原则**:在提供和使用网络以及保障网络安全性时应当尊重他人的权利和合法权益。
- **多方原则**:网络安全方面的措施、具体办法和工作程序应当考虑到所有相关的问题,其中包括技术、行政管理、组织机构、运行、商业、教育和法律等方面的问题。
- **配比原则**:安全水平、费用以及安全措施、具体办法和工作程序应与网络的价值和可靠程

度以及可能造成的损害的严重程度和发生概率成合适的比例，即适度安全原则。

- **综合原则**：网络安全方面的措施、具体办法和工作程序之间应当协调一致，并且与其他措施、具体办法和工作程序协调一致。信息安全也和社会治安一样是一个需要综合治理的问题。
- **及时原则**：无论是国营单位还是私营单位、无论是国内机构还是国际机构，都应当及时协调一致来保障网络的安全。
- **重新评价原则**：定时对网络的安全措施重新评价，由于当前技术的发展速度十分迅速，有些安全措施没过多久就会过时，甚至完全失效。因此在过一段时间后，必须对已有的安全措施做一次全面的评审，以跟上技术的发展。
- **民主原则**：网络的安全应当兼顾信息和数据的流动和合法使用，并相互兼容。

1.3 OSI 信息安全体系结构

1.3.1 ISO 7498-2 标准

ISO 7498 标准是目前国际上普遍遵循的计算机信息系统互连标准。1989 年 12 月，ISO 颁布了该标准的第二部分，即 ISO 7498-2 标准[ISO 7498-2，1989]，首次确定了开放系统互连(OSI)参考模型的信息安全体系结构。我国于 1995 年将其作为 GB/T9387-2 标准，即国家标准《信息处理系统 开放系统互连 基本参考模型——第二部分：安全体系结构 GB/T9387-2》予以执行。ISO 7498-2 与因特网安全体系结构(RFC 2401)是两个普遍适用的安全体系结构，目的是保证开放系统进程之间远距离安全交换信息。这两个标准确立了与安全体系结构有关的一般要素，适用于开放系统之间需要通信保护的各种场合。我们以 ISO 7498-2 标准为主，介绍安全体系结构需要的五大类安全服务以及提供这些服务所需要的八大类安全机制。

1.3.2 安全服务

安全服务是由参与通信的开放系统的某一层提供的服务，它确保该系统或数据传输具有足够的安全性。ISO 7498-2 确定了五大类安全服务，即鉴别、访问控制、数据保密性、数据完整性和不可否认。

1. 鉴别

这种安全服务可对参与通信的对等实体和数据源进行鉴别。

(1)对等实体鉴别

这种安全服务由(N)层提供时，可向($N+1$)实体证实对等实体是它需要的($N+1$)实体。该服务在建立连接或数据传输期间的某些时刻使用，证实一个或多个其他实体连接的一个或多个实体身份。该服务在使用期内让使用者确信：某个实体没有试图冒充别的实体，或者没有试图非法重演以前的某个连接。可以实施单向和双向对等实体鉴别，既可以带有效期校验，也可以不带，它们能够提供不同程度的保护。

(2)数据源鉴别

这种安全服务由(N)层提供时，可向($N+1$)实体证实数据源正是它所需要的对等($N+1$)实体。这种服务能够确认数据单元的来源，但不提供防止数据单元被复制或篡改的措施。

2. 访问控制

这种安全服务能够防止未经授权就利用资源，这些资源可能是通过 OSI 协议可访问的 OSI 资源或非 OSI 资源。这种安全服务可用于对某个资源的各类访问(如通信资源的利用，信息资源的