HZ BOOKS

重点大学
计算机教材

国内首部权威实用的信息安全学专业教材

# 信息安全学

周学广　刘艺　编著

沈昌祥院士　审

机械工业出版社
China Machine Press

重点大学
计算机教材

# 信息安全学

周学广　刘艺　编著



机械工业出版社
China Machine Press

本书全面细致地介绍了信息安全的概念、原理和知识体系，并阐述了如何使用核心加密技术、密钥分配与管理技术、访问控制与防火墙技术、入侵检测技术等技术手段构建信息安全体系；同时结合信息安全领域的最新研究成果和解决方案，对信息安全软件应用、企业及个人信息安全、军队和国家信息安全等专题进行了研究和讨论。

本书题材新颖，内容翔实，既有权威的理论知识，又有大量的实用技术。可用作高校计算机类、信息技术类本科生或低年级研究生教材，也可供从事信息处理、通信保密、军事指挥等专业工程技术人员参考使用。



**图书在版编目（CIP）数据**

信息安全学/周学广，刘艺编著．－北京：机械工业出版社，2003.3
（重点大学计算机教材）
ISBN 7－111－11584－8

Ⅰ.信… Ⅱ.①周…②刘… Ⅲ.信息系统－安全技术－高等学校－教材 Ⅳ.TP309.08

中国版本图书馆 CIP 数据核字（2003）第 006339 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：白红莉 李 炎
北京第二外国语学院印刷厂印刷·新华书店北京发行所发行
2003 年 3 月第 1 版第 1 次印刷
787mm×1092mm 1/16·15.75 印张
印数：0 001-5 000 册
定价：25.00 元

# 序

信息社会的到来，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，极大地推动了人类社会的发展和人类文明的进步，把人类带入了崭新的时代；信息系统的建立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、决策资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程度和综合国力的重要标志。抢占信息资源已经成为国际竞争的重要内容。

党中央及时提出了大力推进国民经济和社会信息化，并做出“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，人们在享受网络信息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，我们既要看到它带来的发展机遇，同时也要正视它引发的严峻挑战。国家“十五”国民经济发展计划决定了要“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，就需要尽快并长期致力于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、维护和提高管理人员的素质和能力。

当前，美国等发达国家，已把信息争夺与对抗作为未来国与国之间斗争的主要方式，因此在信息安全保障方面十分重视。美国最早关注通信保密，1990年提出了信息战及信息安全的概念，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），美国国家安全局也于同年10月提出信息保障技术框架（IATF1.1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到全球战略高度来考虑，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已不能适应当今的需要。信息保障依赖于人、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、完整性的可用性；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。这两者的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、防病毒和防黑客入侵等安全机制（措施）来加以解决。其中，密码技术和管理是信息安全的核心，而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、推动社会文明的发展，发挥着日益重要的作用。由于信息技术本身的特殊性，因此在整个信息化进程中，也同时带来了巨大的信息安全风险。信息安全问题涉及到国家安全、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，以化解日益严峻的信息安全风险，因此，面对日益迫切的需要，惟一的出路就是尽快培养信息安全方面的专门人才，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防线。本书作为重点大学的计算机教材，为培养信息安全专业人才、普及信息安全教育提供了有力支持。

本书具有以下几个特点：

第一、本书内容翔实、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不同院校相关专业的教学需要。

第二、本书选材精、技术新。既介绍了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信息安全技术的综合应用。

第三、图文并茂，深入浅出。本书包括了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。

本书的两位作者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积累了丰富的经验。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。刘艺副教授是知名的计算机技术作家，编著和翻译了大量计算机专著，目前正式出版的已有 10 部，他还曾荣获全军软件比赛一等奖。

两位作者力邀我为本书作序，虽工作繁忙，但通读全书，得益不浅，欣然命笔，是为序。

沈昌祥

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

# 致　谢

本书由周学广承担全书统稿工作。史燕华、戚寒冰、张琪、杨金宝、洪蕾等参加了本书部分录入工作及插图制作。尤其要感谢的还有史燕华女士，她不但完成了大部分的书稿录入工作，还参与完成了本书的初校。本书编著过程中，作者得到了许多领导和专家的支持。他们是：张玉新、尹聚杭、陈志敏、苗小伟、马曲立、王良钢、傅子奇、孙允标、李殿伟、刘可等。在此一并表示谢意！

本书的出版得到了淡菊资讯工作室的协助。

读者联系 Email：my _ reader@sina.com

作　者

2002 年岁末于海军工程大学

# 目　录

# 第1章　信息安全概述

信息是社会发展的重要战略资源，也是衡量国家综合国力的一个重要参数。在信息时代的今天，任何一个国家的政治、军事和外交斗争都离不开信息，经济建设、科学发展和技术进步也同样离不开信息。对信息的开发、控制和利用已成为国家间利益争夺的重要内容，信息安全与国家的安危息息相关。信息的地位与作用因信息技术的快速发展而急剧上升，信息安全问题同样因此而日显突出。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。因此，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。本书主要阐述了信息安全的概念、介绍了信息安全核心技术、密钥分配与托管、访问控制与防火墙技术、入侵检测技术等；通过了解信息安全的两种主要应用软件，去分析个人和企业如何才能搞好信息安全建设，最后简要地介绍了军队和国家信息安全建设现状。

## 1.1　信息的定义与特征

### 1.1.1　信息定义

究竟什么是信息，目前理论界中尚无定论。据粗略统计，在我国书刊中公开出现过的信息定义就有30多种。比较有代表性的有：

信息论的奠基人香农在著名的论文《通信的数学理论》中提出，信息是“两次不确定性之差异”，是用以消除随机不确定性的东西。

控制论的创始人维纳认为：信息是人与外部世界互相交换的内容的名称。

我国信息论专家钟义信教授把信息定义为：事物运动的状态和方式。

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。也有人从信息的实用意义来进行表述，把一切包含新的知识内容的消息、情报、数据和图像等都概括为信息。

我们认为：所谓信息，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。

信息是主观世界联系客观世界的桥梁。在客观世界中，不同的事物都具有不同的特征，这些特征给人们带来不同的信息，而正是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

**一是普遍性和可识别性。**信息来源于物质和物质的运动。只要存在着物质，只要有变化着的事物或运动着的客体，就会存在信息。信息不仅普遍存在，而且也可以进行识别。人们通过

感官或多种探测手段都可以直接或间接地识别出客观事物的形状、特征以及变化所产生的信息，特别是找出其中的差异，这就是认识信息的关键。

**二是存储性和可处理性。**信息依赖于物质和意识，但又可以脱离物质和意识而独立存在，并可以存储起来。信息存储是通过信息载体来将信息进行保存，以备后用，或先存入然后再进行分析整理。这就是信息不同于物质和能源的重要特征。信息不仅可以进行存储，还可以进行处理，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。处理是为了更好地开发和利用，同时也有利于传递和存储。

**三是时效性和可共享性。**信息有较强的时效性。一个信息生成、获取的越早，传递的越快，其价值就越大。随着时间的推延，其价值就会逐渐衰减以至消失。信息的共享性就是指信息可以为多个主体所利用。

**四是增值性和可开发性。**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，以使有限的资源发挥最大的作用；二是可以利用急剧增长的信息，去发掘新的材料和能源。而信息本身在不断地使用中也得到了增值。同时，信息还具有可开发性，需要人们不断地去探索和挖掘，才能充分开发利用信息资源。

**五是可控性和多效用性。**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，同时也增加了信息技术利用的复杂性；而信息的多效用性则是由信息所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、控制的灵魂和管理的保证。

此外，信息还具有转换性、可传递性、独立性和可继承性等特征。信息也具有很强的社会功能，主要表现在资源功能、启迪功能、教育功能、方法论功能、娱乐功能和舆论功能等。信息的社会功能则是由信息的基本特征所决定和派生的。

## 1.2 信息安全基本概念

### 1.2.1 信息安全定义

“安全”并没有统一的定义，但其基本含义可以解释为：客观上不存在威胁，主观上不存在恐惧。

“信息安全”同样也没有公认和统一的定义，但国内外对信息安全的论述大致可以分成两大类：一类是指具体的信息技术系统的安全；而另一类则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。但有人认为这两种定义均失之于过窄，而应把信息安全定义为：一个国家的社会信息化状态不受外来的威胁与侵害，一个国家的信息技术体系不受外来的威胁与侵害。原因是：信息安全，首先应该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的问题。

### 1.2.2 信息安全属性

不管信息入侵者怀有什么样的阴谋诡计、采用什么手段，但他们都要通过攻击信息的以下几种安全属性来达到目的。所谓“信息安全”，在技术层次上的含义就是保证在客观上杜绝对

信息安全属性的安全威胁使得信息的主人在主观上对其信息的本源性放心。信息安全的基本属性有：

1. 完整性（integrity）

完整性是指信息在存储或传输的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，完整性被破坏可能就意味着延误战机、自相残杀或闲置战斗力。破坏信息的完整性是对信息安全发动攻击的最终目的。

2. 可用性（avaliability）

可用性是指信息可被合法用户访问并能按要求顺序使用的特性，即在需要时就可以取用所需的信息。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这种类型的攻击。

3. 保密性（confidentiality）

保密性是指信息不泄漏给非授权的个人和实体，或供其使用的特性。军用信息的安全尤为注重信息的保密性（相比较而言，商用信息则更注重于信息的完整性）。

4. 可控性（controlability）

可控性是指授权机构可以随时控制信息的机密性。美国政府所提倡的“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（reliability）

可靠性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），但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”的内在含义就是指采用一切可能的方法和手段，来千方百计保住信息的上述“五性”安全。

### 1.2.3 信息安全分类

信息安全有多种不同的分类。表 1-1 是其中的一种分类。

**表 1-1 信息安全的一种分类**

| 技术 | 分类 | | 说明 |
|---|---|---|---|
| 信息安全 | 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 | 多级安全用户鉴别术的管理 |
| | | | 多级安全加密术的管理 |
| | | | 密钥管理术的管理 |

（续）

| 技术 | 分类 | | 说明 |
|---|---|---|---|
| 信息安全 | 管理安全 | 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”（OECD）于1992年11月26日一致通过了“信息系统安全指南”。该指南共制定了九项安全原则，欧美各国已明确表示在建设国家信息基础设施NII时都要遵从这一指南的九项原则，它们是：

**第一，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；

**第二，知晓原则**：网络的所有者、提供者和用户以及其他有关方面应当能够了解网络安全方面的措施、具体办法和工作程序；

**第三，道德原则**：在提供和使用以及保障网络安全性时应当尊重他人的权利和合法的权益；

**第四，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；

**第五，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当与网络的价值和可靠程度以及可能造成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；

**第六，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相互协调一致，而且与其他措施、具体办法和工作程序互相协调一致。信息安全也像社会治安一样是一个综合治理的问题；

**第七，及时原则**：无论是国营、私营还是国内外机构都应当及时协调一致来保障网络的安全；

**第八，重新评价原则**：定时对网络的安全措施重新进行评价。由于当前高技术的发展速度十分迅速，有些安全措施没过多久就会变得过时，甚至完全失效，因此在过一段时间之后，还必须对已有的安全措施作一次全面的评审，以期跟上技术的发展；

**第九，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 ISO7498-2 标准

ISO7498 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 ISO7498-2 标准，并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。我国将其作为 GB/T9387-2 标准，并予以执行。下面就来详细介绍一下 ISO7498-2 标准，其中包括了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所提供的服务，它确保了该系统或数据传输具有足够的安全性。ISO7498-2 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

这种安全服务可以鉴别参与通信的对等实体和数据源。

（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所需要的（N+1）实体。该服务在建立连接或在数据传输期间的某些时刻使用，以证实一个或多个其他实体连接的一个或多个实体的身份。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，而且没有试图非法重演以前的某个连接。它们可以实施单向或双向对等实体的鉴别，既可以带有效期校验，也可以不带，以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。这种服务对数据单元的来源能够提供确证，但不提供防止数据单元复制或篡改的保护。

2. 访问控制

这种安全服务提供的保护，能够防止未经授权而利用通过 OSI 可访问的资源。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，信息资源的阅读、书写或删除，处理资源的执行等）或用于对某个资源的所有访问。

3. 数据保密性

这种安全服务能够提供保护，以防止数据未经授权而泄露。

(1) 连接保密性

这种安全服务向某个（N）连接的所有（N）用户数据提供保密性。

**注意**：在某些使用和层次上，这种安全服务可能并不适合保护所有的数据，譬如加速的数据或连接请求中的数据。

(2) 无连接保密性

这种安全服务向单个无连接（N）安全数据单元（SDU）中的所有（N）用户数据提供保密性。

(3) 选择字段保密性

这种安全服务向（N）连接上的（N）用户数据内或单个无连接（N）SDU 中的被选字段提供保密性。

(4) 业务流保密性

这种安全服务防止通过观察业务流以得到有用的保密信息。

4. 数据完整性

这种安全服务用于对付主动威胁。

**注意**：在一次连接中，连接开始时使用对等实体鉴别服务，连接期间使用数据完整性服务，这样就能证实在该连接中传输的所有数据单元的来源及其完整性，若利用序号，还能检测数据单元的复制情况。

(1) 带恢复的连接完整性

这种安全服务向某个（N）连接上的所有（N）用户数据提供完整性保护，并检测对某个完整的 SDU 序列内任何一个数据所做出的任何篡改、插入、删除或重演（非法者在对数据进行了这些非法处理之后，试图恢复数据原貌）。

(2) 不带恢复的连接完整性

与（1）相同，但没有试图恢复数据原貌的功能。

(3) 选择字段连接完整性

这种安全服务向在某个连接中传输的某个(N)SDU 的(N)用户数据内的被选字段提供完整性保护，并能确定这些字段是否经过篡改、插入、删除或重演。

(4) 无连接完整性

这种安全服务由（N）层提供，向提出请求的（N+1）实体提供完整性保证。这种服务可以对单个无连接 SDU 的完整性提供保证，并能确定收到的 SDU 是否经过篡改；另外，还可以

对重演情况进行有限的检测。

(5) 选择字段无连接完整性

这种安全服务对单个无连接 SDU 中的被选字段的完整性提供保证，并能确定被选字段是否经过篡改。

5. 不可否认

(1) 带数据源证明的不可否认

向数据接收者提供数据来源的证明，以制止发信者不真实地否认发送该数据或其内容的任何企图。

(2) 带递交证明的不可否认

向数据发送者提供数据递交的证明，以制止收信者不真实地否认接收该数据或其内容的任何事后的企图。

### 1.3.3 安全机制

ISO7498-2 确定了八大类安全机制，即：加密、数据签名机制、访问控制机制、数据完整性机制、鉴别交换机制、业务填充机制、路由控制机制和公证机制。

1. 加密

(1) 保密性

加密可向数据或业务流信息提供保密性，并能对其他安全机制起作用或对它们进行补充。

(2) 加密算法

加密算法可以是可逆或不可逆的，可逆加密算法有以下两大类：

对称（即秘密钥）加密。对于这种加密，知道了加密密钥也就意味着知道了解密密钥，反之亦然。

非对称（即公开钥）加密。对于这种加密，知道了加密密钥并不意味着知道解密密钥，反之亦然。这种加密系统的两个密钥有时被称为“公开钥”和“秘密钥”。

不可逆加密算法可以使用密钥，也可以不使用。在使用密钥时，这个密钥可以是公开的或秘密的。

(3) 密钥管理

除了某些不可逆加密算法的情况之外，加密机制的存在意味着使用密钥管理机制。

2. 数字签名机制

这种安全机制决定于两个过程：

- 对数据单元签名
- 验证签过名的数据单元

第一个过程可以利用签名者私有的（即独有和保密的）信息，而第二个过程则要利用公之于众的规程和信息，但通过它们并不能推出签名者的私有信息。

(1) 签名

签名过程是利用签名者的私有信息作为秘密钥，或对数据单元进行加密，或产生该数据单元的密码校验值。

(2) 验证

验证过程是利用公开的规程和信息来确定签名是否是利用该签名者的私有信息产生的。

(3) 特征

签名机制的主要特征是签名只有利用签名者的私有信息才能产生出来，这样在签名得到验证之后，就可以在任何时候向第三方（如法官或仲裁人）证明：只有秘密信息的惟一拥有者才能够产生那个签名。

3. 访问控制机制

(1) 确定访问权

这种安全机制可以利用某个实体经鉴别的身份或关于该实体的信息（如在某个已知实体集里的资格）或该实体的权标，进行确定并实施实体的访问权。如果该实体试图利用未被授权的资源或用不正当的访问方式利用授权的资源，那么访问控制功能将会拒绝这个企图，另外还可能产生一个告警信号或把它作为安全审计线索的一部分记录下来，并以此报告这一事件。对于无连接数据的传输，则只有在数据源强制实施访问控制之后，才有可能向发信者提出任何拒绝访问的通知。

(2) 访问控制机制可以建立在下列一个或多个手段之上

a) 访问控制信息库，它保存着对等实体的访问权限。这种信息可由授权中心来保存，或由被访问的实体来保存。可采用访问控制表的形式，或分层式结构矩阵的形式，或分布式结构矩阵的形式。这里，假定对等实体鉴别已经得到保证；

b) 像通行字之类的鉴别信息，对这种信息的占有和出示便证明正在访问的实体已被授权；

c) 权标，对这个权标的拥有和出示便证明有权访问该权标规定的实体或资源；

注：权标应该是不可伪造的，而且应该以可信方式进行传送。

d) 安全标签，当与某个实体相关联时，可用于同意或拒绝访问，通常可以根据安全策略而定；

e) 试图访问的时间；

f) 试图访问的路由；

g) 访问持续的时间。

(3) 访问控制机制可用于通信连接的任何一端或用在中间的任何位置

访问控制在数据源或任何中间点用于确定发信者是否被授权与收信者进行通信，或被授权可以利用所需要的通信资源。无连接数据传输目的地对同等级访问控制的要求必须先让数据源知道，而且必须记录在安全管理信息库中。

4. 数据完整性机制

(1) 数据完整性机制的两个方面

单个的数据单元或字段的完整性以及数据单元串或字段串的完整性。总之，不同的机制用于提供这两类不同的完整性服务，尽管没有第一类完整性服务就无法提供第二类完整性服务。

(2) 确定单个数据单元的完整性

确定单个数据单元的完整性涉及到两个处理：一个在发送实体中进行，而另一个在接收实体中进行。发送实体给数据单元附加一个由数据自己决定的量，而这个量可以是分组校验码或