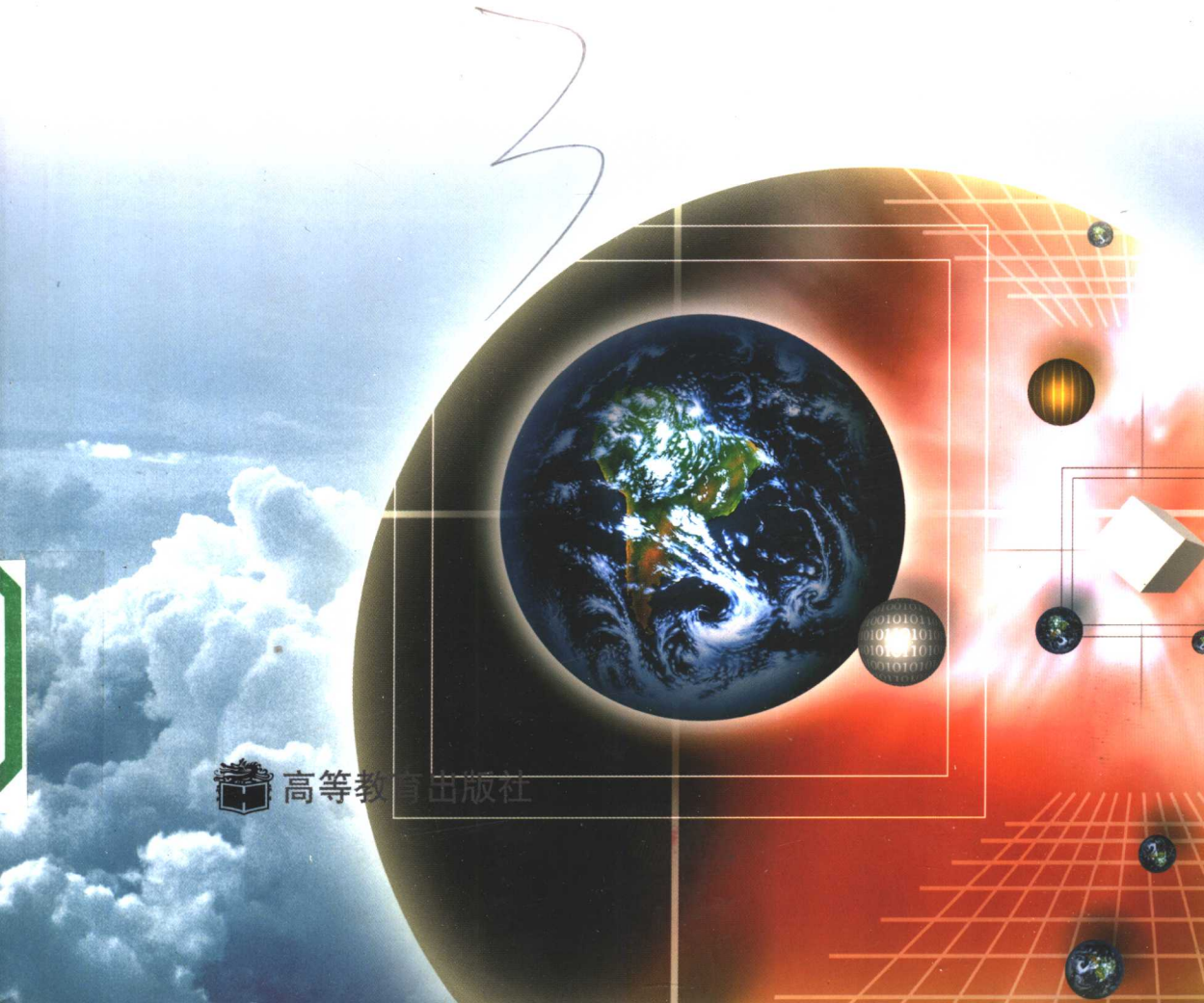
高 等 学 校 教 材

计算机信息安全技术

步山岳 张有东



高等教育出版社

高等学校教材

计算机信息安全技术

步山岳　张有东

高等教育出版社

内容简介

本书较好地体现了计算机信息安全体系，主要内容包括 DES、AES、RSA、NTRU 算法；信息隐藏、数字水印技术；数字签名；单向散列函数；Kerberos；PKI；用户 ID 与口令机制；生物特征识别技术；计算机病毒与黑客防范；网络攻击与防范；网络欺骗与防范；网络安全服务协议；无线网安全；防火墙技术；入侵检测技术；数字取证技术；操作系统安全机制与配置；系统数据、用户数据、网络数据备份以及数据恢复技术；软件静态、动态分析技术；常用软件保护技术；软件加壳与脱壳等。全书每章都配有大量习题和实验。

本书可作为计算机和通信专业本科或专科相关课程的教材，也可供信息安全专业和从事信息安全研究的工程技术人员参考。

图书在版编目（CIP）数据

计算机信息安全技术/ 步山岳，张有东. —北京：高等教育出版社，2005.9

ISBN 7-04-017818-4

Ⅰ.计… Ⅱ.步… Ⅲ.电子计算机-安全技术-高等学校-教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2005）第 113223 号

策划编辑 倪文慧　　**责任编辑** 倪文慧

封面设计 刘晓翔　　**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
经　　销	北京蓝色畅想图书发行有限公司	**网上订购**	http://www.landraco.com
印　　刷	高等教育出版社印刷厂		http://www.landraco.com.cn
开　　本	787×960　1/16	**版　　次**	2005 年 9 月第 1 版
印　　张	22.25	**印　　次**	2005 年 9 月第 1 次印刷
字　　数	400 000	**定　　价**	28.00 元

物料号　17818-00

前　言

在社会面临严重信息安全问题的环境下，国家和各行业对信息安全人才的需求日臻旺盛，而真正具备渊博知识、丰富实践的信息安全人才却不多，远远不能满足社会需求。因此，学校对培养信息安全人才具有义不容辞的责任。

1. 教材特色

正是在社会需求动力的推动下，作者经过3年多时间的精心准备，使得教材具有如下特色：

（1）知识实用、丰富、新颖

本教材的编写基于应用型人才培养的需要，以知识实用、丰富、新颖为原则，以通过学习计算机信息安全技术基础理论，使学生初步掌握计算机信息安全实用技能为主导目标，为学生今后进一步学习、研究信息安全技术打下坚实的基础。

教材在有限的篇幅中尽可能蕴涵了更多的信息量，语言尽可能做到文字通顺、语言简练、语义清晰而明确，并在不影响对基础知识理解的前提下，尽可能减少“概念性”和“理论性”知识介绍，增加能解决“实际问题”的内容。同时，吸取了目前已出版的信息安全技术教材、相关信息安全论文的精髓，充分反映了计算机信息安全领域的前沿技术和成果。

（2）完整的信息安全体系

目前计算机信息安全研究的主要方向包括密码学、计算机网络安全、计算机病毒、信息隐藏技术、软件保护技术、数据恢复技术和信息安全管理等方面。本教材力求融合信息安全研究的基础知识与核心内容，全面反映整个计算机信息安全体系。

虽然教材几乎囊括了信息安全的各个方面，但教材的内容只涉及到计算机信息安全体系最基础、最核心的部分。而这些“最基础、最核心”的知识又是建立在最实用的基础上，学生不但可以从该教材中全面了解到信息安全概貌，同时又可以迅速掌握信息安全技术的基本技能，为学生今后的工作和研究提供方向性指导。

（3）大量的习题与实验

教材提供了大量的习题与实验。习题与实验的编写是建立在对教材内容理解和巩固的基础上，习题中很少涉及到类似理论性推导或证明性问题。编写习题与实验的目的就是要巩固学生所学的知识，训练学生解决实际问题的能力，这非常适合定位于培养应用型人才的高等院校。

2. 教学和学习建议

计算机信息安全课程的教学和学习目标就是要使学生能够全面了解整个计算机信息安全体系，掌握基本的应用技能。受到教材篇幅等原因的限制，我们没有对教材的每个知识点都进行深入的探讨。教师可以根据学校的教学条件、自己的专业特长和教学需要，适当补充或删除教学内容。学生阅读本教材后，也可以根据个人爱好，选择研究方向，再进行深入的学习和研究。

教材中介绍的软件大多可以从网上免费下载，这样既方便教师教学，也方便学生自学。当然，如果学校条件允许的话，也可介绍一些商业软件，使学生能更好地了解信息安全产品。

有关本教材的电子课件等教学辅助材料，我们将放到高等教育出版社高等理工教学资源网上（http://www.hep-st.com.cn）供教师下载，也可直接和作者（bushanyue@Sina100.com）联系索取。在教学大纲中将对教材每章的教学重点、教学要求进行详细说明，供教师和学生参考。教师课堂教学时，如果有条件的话，最好使用多媒体课件与板书相结合，这样可能会达到应有的教学效果。

3. 致谢

教材第7、8章由张有东编写，张勇军编写了5.5.1节中一个程序示例的运行分析，步山岳编写了其余章节，并对整个教材进行了修改和统稿。在本书的编写过程中，梁民、唐洪、寇海洲、冯万利、张亚红、金圣华和徐成杰等老师给予了大力支持和帮助，夏新瑜等同学积极参与教材的文字校对工作，高等教育出版社计算机分社的有关同志也提出了很多建设性意见，在此谨向他们表示衷心的感谢。最后还要特别感谢北京电子科技学院的李凤华教授，他仔细审阅了全书，提出了很多宝贵的建议，使得本书更加充实和完善。

尽管作者满怀热情与自信，在编写教材的过程中投入了极大的精力，但因能力所限，书中难免存在疏漏之处，恳请读者批评指正。我们会及时吸纳您的意见，进一步完善教材。同时，我们向所有提出批评和建议的读者表示衷心的感谢！

作 者

2005年9月

目　录

第1章　计算机信息安全概述

1.1　威胁计算机信息安全的因素

在我们享受信息社会带来的巨大经济利益和娱乐时，计算机信息安全问题正面临着严峻的挑战。争夺信息资源，获取对方机密，篡改、破坏和销毁对方重要数据，破坏对方的信息处理设备等，早已成为一场看不见硝烟的全球性战争。信息安全已是世界性的现实问题，信息安全与国家的政治稳定、军事安全、经济发展和民族兴衰息息相关，提高国家信息安全体系的保障能力已成为各国政府优先考虑的战略问题。

对于每个普通公民来说，信息安全问题同样严峻。当我们将重要的数据存放在硬盘上时，会因操作不当或计算机病毒等原因在顷刻之间化为乌有。我们信用卡账户、证券账户和期货账户的资金会不明原因地减少。我们的计算机系统会在毫无察觉的情况下被破坏而无法运行，甚至我们的计算机会在毫无察觉的情况下成为攻击、破坏其他计算机的工具，成为罪犯的帮凶。

目前对计算机信息系统的威胁大致可分为3个方面：

（1）直接对计算机系统的硬件设备进行破坏。

（2）对存放在系统存储介质上的信息进行非法获取、篡改和破坏等。

（3）在信息传输过程中对信息非法获取、篡改和破坏等。

影响计算机信息安全的因素很多，大致可分为如下几类。

1. 自然环境

自然环境的破坏包括火灾、水灾、雷电、地震以及计算机设备硬件失常等造成信息的丢失。为减少自然环境的破坏和影响，在建设计算机机房等基础设施时就要考虑到计算机机房地点的选择、计算机机房结构等因素。应该说保障计算机设备物理安全是相对比较容易的，只要把握好从选购设备到机房建设的每个环节，认真做好设备管理等工作就可以避免或减少因物理设备损坏而造成的影响。

2. 人为失误

人为操作失误是指用户没有严格按照操作规程操作计算机。如错误删除重要文件；安全配置不当造成的系统安全漏洞；用户口令设置不慎，将自己的口令和账

号随意告诉其他人等都会对系统信息安全带来威胁。

3. 人为恶意破坏

人为恶意破坏是目前计算机系统所面临的最大威胁。这种破坏是以各种方式有选择地或无选择地破坏计算机系统信息的有效性和完整性，或者进行窃取、破译以获得重要机密信息。人的威胁来自内部威胁和外部威胁两个方面，据不完全统计，有80%的计算机犯罪和系统安全遭破坏都与内部人员密切相关。

4. 软件设计等不完善

从技术上来说，造成计算机信息系统容易受到攻击的根本原因是计算机信息系统本身存在固有的漏洞和脆弱性。如在优盘、硬盘、光盘上能存放大量的数据，而这些存储介质很容易携带或受到意外损坏，会造成信息失窃和丢失；由于软件自身的固有特性等因素，使得开发出的操作系统和各类软件漏洞百出，很容易成为攻击的对象。

要确保计算机系统和信息安全是相当困难的，其根本原因是计算机软件可修改性以及人们在设计程序时无法尽善尽美造成的。在人们大谈计算机软件的可修改性给编程带来巨大便利，能创造出各种各样软件的同时，计算机软件的可修改性也正暴露出软件的脆弱性。人们也可以利用计算机软件的可修改性方便地修改程序达到破坏其他程序和信息、或非法占有信息等目的。

1.2　计算机信息安全研究的内容

研究计算机信息安全技术关系到国家和民族的兴衰，也关系到每个人的切身利益，必须严肃对待和深入研究。从目前对计算机信息安全的威胁方面看，计算机信息安全技术研究的内容应该包括3个方面：一是计算机外部安全；二是计算机信息在存储介质上的安全，有时也称为计算机内部安全；三是计算机信息在传输过程中的安全，或称为计算机网络安全。

1.2.1　计算机外部安全

计算机外部安全包括计算机设备的物理安全、与信息安全有关的规章制度的建立和法律法规的制定等。它是保证计算机设备正常运行，确保系统信息安全的前提。

1. 安全规章制度

安全规章制度是计算机安全体系的基础。作为一个企业或部门，如果没有健全的规章制度，就很可能陷入利润损失、法律诉讼和恶劣的社会形象的被动地位。

规章制度的内容可以包括计算机操作管理制度、用户账号管理制度、远程访问管理制度、信息保护管理制度、防火墙管理制度、特殊访问权限管理制度等。规章制度的内容要具体,具有可操作性。规章制度制定完成后,要有一个规章制度的推行过程,必须保证对违反规章制度的行为进行惩罚。最后还要对规章制度的实施进行监督,以保证规章制度能顺利执行。同时在监督规章制度实施过程中,还要不断总结规章制度在执行中所碰到的问题,及时修改和完善规章制度。

政府制定完善的信息安全管理法规可以从宏观上打击和惩治计算机犯罪,目前我国已制定了一些与计算机信息安全相关的法规,相信政府今后还会针对新的形势进一步改进和完善信息安全法规。

2. 设备的物理安全

设备的物理安全问题包括对计算机设备和工作环境的防护措施。如防火、防盗、防水、防尘、防地震、防电磁辐射等措施。在建造计算机机房时就考虑避开地震多发地带,远离危险物品聚集地,远离易发生火灾的地方,远离强电场、强磁场等;要设计好计算机设备供电系统,确保设备用电稳定和可靠;还要注意设备的地线质量,地线质量的好坏和是否合理会直接关系到人身安全、设备稳定与可靠运行。一般要求交流电接地电阻在4欧姆左右,整机接地电阻,即安全保护地电阻要小于4欧姆。

计算机设备的物理安全问题相对来说一般容易避免、发现和解决。

3. 防电磁波辐射

在计算机外部安全中,计算机防电磁波辐射也是一个重要的问题。它包含两个方面的内容:一是计算机系统受到外界电磁场的干扰,使得计算机系统不能正常工作;二是计算机系统本身产生的电磁波包含有用信号,造成信息泄漏,为攻击者提供了信息窃取的可能性。

1985年,荷兰一位无线电技术人员就在计算机通信安全大会上用一台稍加改装的黑白电视机,演示了在1公里距离内接收到的计算机显示屏辐射信息,并在电视机荧屏上复原出来,可以看到与计算机显示屏上完全相同的内容。研究表明不仅仅计算机的显示屏能辐射电磁波,其他外部设备,如键盘、磁盘和打印机等设备在工作过程中同样也会辐射电磁波,造成信息泄漏。

电磁泄漏不仅影响周围人的身体健康,对其他电子设备形成干扰,有时还会导致重要信息的泄密。针对这个问题,美国国家安全局与美国国防部联合研究和开发了一种称为TEMPEST的技术。该技术的主要目的是防止计算机系统中因电磁辐射而产生的信息泄密,是信息安全保密的一个专门研究领域。它包括对信息设备电磁泄漏发射信号中所携带的敏感信息进行分析、测试、接收、还原以及防护等一系列技术。TEMPEST采取的防护措施包括抑源法、电磁屏蔽法和噪声干扰法。

(1) 抑源法是从降低信息设备电磁发射源发射强度的角度来采取措施,如采取抑制电磁辐射,传导发射滤波等措施。

(2) 屏蔽技术包括对设备的屏蔽和环境的屏蔽,主要通过金属板和金属网等,将信息设备或系统放置在全封闭的电磁屏蔽室内。

(3) 噪声法是在信道上增加噪声,从而降低窃收系统的信噪比,使其难以将泄漏的信息还原。

1.2.2　计算机内部安全

计算机内部安全是计算机信息在存储介质上的安全,包括计算机软件保护、软件安全、数据安全等。计算机内部安全要研究的内容也是非常广泛的,如软件的防盗版,操作系统的安全性问题,磁盘上的数据防破坏、防窃取以及磁盘上的数据恢复与拯救技术等问题。

由于磁盘容量大,存取数据方便,磁盘是目前存放计算机信息最常用的载体。但由于磁性介质都具有剩磁效应现象,保存在磁性存储介质中的数据可能会使存储介质永久性磁化。所以保存在磁性存储介质上的信息可能会擦除不尽,永久地保留在磁盘上。因此对于一些重要的信息,尽管已经使用擦除软件等手段擦除过信息,但如果擦除不彻底就会在磁盘上留下重要信息的痕迹,一旦被别人利用,通过使用高灵敏度磁头和放大器可以将磁盘上的信息还原出来,造成机密信息泄漏。

另外在计算机操作系统中,使用类似格式化命令 format,或删除命令 del 时,仅仅能破坏或删除文件的目录结构和文件指针等信息,磁盘上的原有文件内容仍然原封不动地保留在磁盘中,只要不在磁盘中重新存放数据,使用 unformat 等方法就可以非常完整地将磁盘上的数据恢复出来。在 Windows 操作系统中甚至可以从回收站找回被删除的数据,利用这些就可以窃取重要的机密信息。

计算机的信息安全还可以用信息的完整性、可用性、保密性等属性加以说明。

(1) 完整性技术是保护计算机系统内软件和数据不被偶然或人为蓄意地破坏、篡改、伪造等的一种技术手段。只有经过授权的人才能对信息进行修改,并且能够判断出信息是否已被修改,从而保持信息的整体完整性。完整性是对信息可靠性和精确性的度量。

(2) 可用性技术是在用户授权的条件下,无论什么时候,只要用户需要,信息必须是可用的,是可以访问的,信息系统不能拒绝服务。

(3) 保密性技术是防止信息失窃和泄露的技术,信息必须按照信息拥有者的要求保持一定的秘密性。只有得到拥有者的许可,其他人才能获得该信息。加密是对存储在各种介质上的信息实施保护的有效和必不可少的技术手段。

完整性、可用性、保密性是信息安全中最重要的 3 个属性,在信息安全属性中

还有可控性、不可抵赖性和有效性等。

1.2.3 计算机网络安全

计算机信息在传输过程中的安全是指在通过庞大的计算机网络系统交换数据时确保信息的完整性、可靠性和保密性。Internet 为世界各地的人们交换信息提供了巨大的便利,同时也为世界上的各类犯罪分子打开了方便之门。计算机网络已成为攻击、破坏和获取情报的重要工具,可以说计算机网络安全问题是计算机安全中最严重的问题,一直受到人们的高度关注。

建立网络信息安全保障体系可以采用边界防卫、入侵检测和安全反应等技术。

(1) 边界防卫技术通常将安全边界设在需要保护的信息周边,重点阻止诸如病毒入侵、黑客攻击、冒名顶替、线路窃听等试图"越界"的行为。相关的技术包括数据加密、数据完整性检查、防火墙、访问控制和公证仲裁等。

(2) 入侵检测技术是发现"敌方"渗透企图和入侵行为的技术,是对网络系统运行状态进行监视,发现各种企图攻击行为和攻击结果,并及时作出反应的技术。入侵检测技术是基于入侵者的攻击行为与合法用户正常行为有着明显的不同,实现对入侵行为的检测和报警,以及对入侵者的跟踪定位和行为取证。

(3) 安全反应技术是将破坏所造成的损失降低到最小限度的技术,安全的网络信息系统必须具备在被攻陷后能迅速恢复的能力。其中分布式动态备份技术与方法、动态漂移与伪装技术、各种灾难的快速恢复与修复算法、防守反击技术等都是目前正在研究的课题。

由此可见,计算机信息安全技术所要研究的内容十分广泛,它包括电子学、计算机硬件设计、计算机软件设计、密码学、数学、信息论、信息管理、社会学和法律等,是多学科的边缘性综合性研究技术。它不仅仅涉及到国家的政治、经济和军事等重要部门,还与我们的日常生活息息相关,对现代文明社会将产生重大影响。

1.3 OSI 信息安全体系

1989 年 12 月国际标准化组织 ISO 颁布了信息处理系统开放系统互连基本参考模型(OSI)第 2 部分安全体系结构 ISO7498 - 2 标准,是目前国际上普遍遵循的计算机信息系统互连标准,我国将其作为 GB/T9387 - 2 标准并予以执行。ISO7498 - 2 标准包括 5 类安全服务以及提供这些服务所需要的 8 类安全机制。

1.3.1 安全服务

安全服务是在 OSI 参考模型框架中能提供的可选的安全服务,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 5 大类安全服务，即：鉴别服务、访问控制服务、数据保密性、数据完整性和禁止否认服务。

1. 鉴别服务

鉴别服务可以鉴别参与通信的对等实体和数据源的合法性。

(1) 对等实体鉴别。这种安全服务由 N 层实体提供时，可向 $N+1$ 层实体证实对等实体是它所需要的 $N+1$ 层实体，提供对等实体之间的合法性判断。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 层实体提供时，可向 $N+1$ 层实体证实数据源是它所需要的对等 $N+1$ 层实体。这种服务用来鉴别发送实体的合法性，确保数据是由合法实体发出的，以防假冒。但不提供防止数据单元被复制或篡改的保护。

2. 访问控制服务

访问控制服务能够防止未经授权而利用 OSI 可访问的资源。这种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)，或用于对所有资源的某类访问。

3. 数据保密性

这种安全服务能够防止数据未经授权而被泄露，防止在系统之间交换数据时，数据被截获。它包括连接保密性、无连接保密性、选择字段保密性、业务流保密性 4 项服务。

4. 数据完整性

这种安全服务是用于对付主动威胁的，用来防止在系统之间交换数据时，数据被修改、插入，或造成数据丢失。它包括带恢复的连接完整性、不带恢复的连接完整性、选择字段连接完整性、无连接完整性、选择字段无连接完整性。

5. 禁止否认服务

这种安全服务是防止数据发送方发送数据后又否认发送数据的行为，或接收方接收到数据后又否认接收到数据的行为，即防止通信双方否认发送或接收数据的行为。它包括带数据源证明的禁止否认、带递交证明的禁止否认。

1.3.2　安全机制

ISO7498-2 确定了 8 类安全机制，即：加密机制、数字签名机制、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. 加密机制

加密是提供数据保护最常用的方法，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。加密机制包括加密的保密性、加密算法、密钥管理等。

2. 数字签名机制

数字签名主要用来解决通信双方发生否认、伪造、篡改和冒充等问题。这种安全机制决定两个过程：

(1) 对数据单元签名。

(2) 验证签过名的数据单元。

3. 访问控制机制

访问控制机制是按照事先制定的规则确定主体对客体的访问是否合法，防止未经授权的用户非法访问系统资源。如果某个实体试图使用非授权的资源，或者以不正当方式使用授权资源，那么访问控制功能将拒绝这一企图。同时还可能产生一个报警信号或记录它作为安全审计跟踪的一个部分来报告这一事件。访问控制机制主要利用访问控制表、口令、安全标记、能力表等表示合法访问权。

4. 数据完整性机制

数据完整性机制包括两个方面：

(1) 单个的数据单元或字段的完整性。

(2) 数据单元串或字段串的完整性，即要求数据编号的连续性和时间标记的正确性等。

确定单个数据单元的完整性可以利用分组校验码或密码校验值防止信息被修改；保护数据单元串或字段串的完整性，可以利用顺序号、时间标记或密码链等防止信息被扰乱、丢失、插入等。

5. 鉴别交换机制

这种机制是以交换信息的方式来确认对方身份的机制。可用于鉴别交换的技术有口令、密码技术、实体的特征或占有物、时钟标志和同步时钟、双向和三向握手(分别用于单方和双方鉴别)、数字签名或公证机构等。

6. 业务填充机制

这是一种造假的通信实例，产生欺骗性数据单元或在数据单元中产生假数据的安全机制。如在无信息传输时，发送伪随机序列信号，使非法监听者无法确认哪些是有用信息，哪些是无用信息。该机制只有在业务填充受到保密性服务保护时