前　言

2018 年 12 月，《网络安全攻防技术》出版以来，不少读者提出最好有一本入门级的参考书。我们秉承“理论和实践相结合”的思想，结合多年网络与信息安全教学经验，基于苗刚中老师的《信息安全概论》讲稿，同时邀请了部分长期从事网络空间安全教学的高校教师、网络安全监管部门的技术专家和部分 Gartner 排名前列的国内网络安全厂商(包括梆梆安全、青藤云、安博通、科来、恒安嘉新、联软、君立华域、赛迪腾龙等)的总工程师或技术总监撰写这本《网络与信息安全技术导论》，旨在帮助读者了解和掌握网络与信息安全基础理论、实用技术以及主流的网络与信息安全产品。

这种校政企人员联合编写模式是我们做的一次尝试，得到了多方专家学者和从业者的认可。为了更好地完成内容的筛选，我们挑选了四名研究生，历时三个多月，对市面上几乎所有同类书籍进行了调研分析，为本书的撰写提供了宝贵借鉴素材。编者在编写基础理论知识部分时，力求简单明了，一改部分同类书籍的简而不明、明而不简，初学者不易入门的情况，希冀初学者能尽快进入网络与信息安全领域。书中所举案例和产品功能介绍，均重点着墨目前热门的、覆盖面大的、从业人员亟须了解的内容。书稿完成后，朱军老师率先进行了试用，对内容进行了优化。

本书由唐昊、苗刚中、朱军、王理冬主编，负责全书的体系架构、内容组织以及统稿、编著等工作，同时参加部分章节的撰写。其中，第 1 章由唐昊和苗刚中编写，第 2 章由苗刚中和李奇越编写，第 3 章由方贤进、陈付龙和朱晓玲编写，第 4 章由苗刚中、朱军和张仁斌编写，第 5、6 章由朱军、钱君生和杨春节编写，第 7 章由苗刚中、朱军和陈林硕编写，第 8 章由张羽、唐昊和苗露编写，第 9 章由苗刚中、郑明、方星星、薛洪亮、芮乐胤、张晶、张建耀编写，第 10 章由王理冬、冯玲莉和王永红编写，第 11 章由苗刚中、朱军和王刚编写。

本书在编写过程中，得到了多位网络与信息安全领域的领导、专家、学者和从业人员的大力支持和帮助，包括张福、尹华、金光成、李永生、吴多志、焦成俊、蔡藤波、孙志伟、李瑞、蔡月、程雨航、葛鹏飞、章正东、丁力、缪拥军、何小颖、刘冬晴、胡琳、陶志清、田洒洒、付一群、徐启坤、侯静云、马娟、王雷、江蒙、董卫国、张中坤等，他们或提出宝贵的意见，或参与部分文字、插图和表格的制作和整理，在此一并向他们表示衷心的感谢！

限于编者水平，书中难免存在一些不妥之处，恳请读者批评指正。

编　者

2025 年 12 月

目　录

第 1 章　概　　论

网络与信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种领域的综合性学科。其研究内容涉及如何保护信息系统的硬件、软件和数据不因偶然的或者恶意的原因遭到破坏、更改、泄露，如何保护系统连续可靠地运行、系统服务不中断。

1.1　网络与信息安全的基本概念

1.1.1　安全的本质

1. 安全的一般定义

安全是免除了不可接受的损害风险的状态。安全是指不受威胁，没有危险、危害、损失。从安全工程或者安全学的角度可以从两个侧面予以理解：①安全是一种状态，即人和物不会受到伤害和损失的理想状态；②安全是一个动态过程或状态，过程的趋势或状态是人和事物受到的伤害(包括身体的、精神的)或遭受的损失处在可以接受的范围内。

2. 安全保障和保护措施

安全保障：防止由于自己的无意行为或者系统(或其他存在物)天生缺陷、失误、故障等造成的事故、伤害和损失。通过对人员的培训、教育，对系统(或其他存在物)的设计、制造和操作规程全过程的严格把关、科学优化等措施保障安全。

保护措施：防范系统内部或外部故意的不良行为可能造成的损失、伤害。除了保障的措施，还需要设置警卫、岗哨等，部署防空袭力量，以及采取防间谍措施等。

3. 安全的属性

安全是一种状态，没有危险是其基本属性。在不同领域，描述这种状态的特征量并不相同。即使在大部分具体领域中，科学界对表征安全的特征量也有分歧，没有统一认识。但基本都承认安全是动力学过程中的演化状态，与环境、时间以及子系统之间的相互作用有密切关系。从系统动力学的角度观察，任何系统都不存在“绝对安全”的状态。判断某一系统是否安全，或判断其安全程度时，除了需要考察其内在因素，还与运行环境和时间维度具有重要关联。对于同一个系统，在不同的环境和不同时间，可能有着完全不同的安全状态。因此，环境和时间被认为是安全的两个重要影响因素。

1.1.2 信息安全

信息系统和信息资产的重要性，要求任何一个组织或机构都有必要采取措施保护其安全，使之不因偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够连续、可靠、正常地运行，使安全事件对业务造成的影响降到最低，确保业务运行的连续性。2017 年 6 月 1 日，《中华人民共和国网络安全法》实施，确立了我国网络与信息安全的战略基石，开启了信息安全研究、治理的新时代。

1. 信息安全的定义

国际标准化组织(International Organization for Standardization, ISO)的定义：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然或恶意的原因遭到破坏、更改和泄露。

欧洲联盟(欧盟)的定义：在既定的密级条件下，网络与信息系统抵御意外事件或恶意行为的能力。这些事件和行为将危及所存储或传输的数据以及经由这些网络和系统所提供的服务的可用性、真实性、完整性与机密性。

美国国防部在信息保障(information assurance, IA)中的定义：保护和防御信息及信息系统，确保其可用性、完整性、保密性、可认证性、不可否认性等特性。这包括在信息系统中融入保护、检测、反应功能，并提供信息系统的恢复功能。

我国信息安全专家沈昌祥院士的定义：保护信息和信息系统不被未经授权地访问、使用、泄露、修改和破坏，为信息和信息系统提供保密性、完整性、可用性、可控性和不可否认性。

和一般意义上的安全一样，信息系统安全也是一个动力学演化的动态变化概念，并且随着信息技术的发展以及信息化普及的程度不断被赋予新的内涵。

2. 信息安全目的

信息系统安全的终极目的：在系统实现过程中，对组织、合作伙伴及其客户的信息技术相关风险给予应有的关心和考虑，帮助组织实现其使命/业务的全部目标。

3. 信息安全目标

信息安全以保护信息资产、防止信息被恶意泄露、修改和破坏为目的，通过相关技术，保证信息在各环节中存储、传输和交换的机密(保密)性、完整性、可用性、可控性和不可否认性。

4. 信息安全的基本属性

机密性、完整性、可用性、可控性和不可否认性被称为信息系统安全的五大属性。

(1)机密性：私密的或机密的信息不能透露给非授权的主体。信息的机密性依据信息被允许访问对象的多少而不同，所有人员都可以访问的信息为公开信息，需要限制访问的信息为敏感信息或秘密信息，根据信息的重要程度和保密要求将信息分为不同密级。

一般分为公开、秘密、机密和绝密四个等级。已授权用户根据所授予的操作权限可以对保密信息进行操作。

(2) 完整性：完整性包括数据完整性和系统完整性，数据完整性指信息和程序只能按指定的且授权的方式修改；而系统完整性指系统不能受到故意的或无意的非授权操作，必须不折不扣地执行预定的功能。完整性一方面是保障在使用、传输、存储信息的过程中不发生篡改信息、丢失信息、信息错误等现象；另一方面是指信息处理的方法的正确性，执行不正当的操作，有可能造成重要文件的丢失，甚至整个系统的瘫痪。

(3) 可用性：系统必须及时工作，不能拒绝向授权用户提供服务。信息及相关的信息资产在授权人需要的时候，可以立即获得。例如，通信线路中断故障、网络的拥堵会造成信息在一段时间内不可用，影响正常的业务运营，就会造成对信息可用性的破坏。信息系统必须能适当地承受攻击并能在被攻击后得到恢复。

(4) 可控性：任何对信息的访问和对信息系统的使用都能得到有效的安全监控，防止对信息和信息系统的非法(非授权)利用。如果存在主体(人/程序)能不受限制地访问、更改以及传播信息系统中的敏感信息，则一定是安全保障系统失去了效用，信息系统处于失控状态。信息安全的可控性不仅涉及信息的可控性，还与安全产品、安全市场、安全厂商、安全研发人员的可控性紧密相关。

(5) 不可否认性：保护用户免遭来自系统中其他合法用户的威胁，而不是来自攻击者的威胁。不可否认分为原发不可否认和接收不可否认，原发不可否认用于防止发送者否认自己已发送的数据和数据内容；接收不可否认用于防止接收者否认已接收过的数据和数据内容。

1.1.3　信息安全与网络安全的关系

网络安全、信息安全从概念到内涵均存在一定区别，经常被混淆。从广义的角度看，由于信息系统的定义包含了信息的收集、存储、传输、处理、交换等各个环节，因此信息安全的范围包含了网络安全，即网络安全是信息安全的一个组成部分。从狭义的角度看，网络安全的关注焦点集中在网络的架构、协议、配置和管理等方面，更加注重的是信息在传输过程中的机密性、完整性和可用性，而信息安全则是将关注焦点集中在信息收集、存储、处理和交换等环节，也有信息安全侧重内容安全之说。

严格来说，信息安全主要涵盖物理安全、人员安全、通信传输安全、计算设备安全与电磁防护安全等。

1.2　网络与信息安全的发展历程

网络与信息安全大致经历了通信保密、信息安全、信息保障三个发展阶段。

1.2.1　通信保密阶段

1980 年以前，在通信保密(communication security, COMSEC)阶段，加密方法是主要的研究对象。1973 年，IBM 提出数据加密标准(data encryption standard, DES)算法之前，

加密技术的研究进展缓慢，没有任何加密系统比德国的 ENIGMA 更加著名，ENIGMA（源自希腊语，意为“谜”）由德国发明家阿瑟·谢尔比乌斯（Arthur Scherbius）在 1918 年提出，如果对密文进行暴力破解，解密者将面临约 1590 亿亿种可能性，在当时，这是一个不可能完成的任务，因此，ENIGMA 被认为是最保险的加密系统。

1.2.2　信息安全阶段

1980～2000 年进入了信息安全（information security，INFOSEC）阶段。计算机技术，特别是计算机网络日渐普及，各种非法访问、弱口令和恶意代码（如病毒）等成为主要的安全威胁，计算机及其信息网络的安全受到越来越多的重视。1973 年，贝尔（Bell）和拉帕杜拉（La Padula）仿照军事安全策略的思想提出了一种计算机安全操作模型，被称为 BLP（Bell-La Padula）模型，这是世界上第一个计算机多级安全模型。1985 年，美国国防部在 BLP 模型的基础上颁布了全球第一个可信计算机系统评估准则（trusted computer system evaluation criteria，TCSEC），开启了全球范围内对计算机安全及其评价标准的研究和应用。

1. 加密算法

1973 年，IBM 提出的数据加密标准（data encryption standard，DES）算法是第一个具有全球影响力的加密算法。1976 年，迪菲（Diffie）与赫尔曼（Hellman）在拉尔夫·C. 默克尔（Ralph C. Merkle）思想的基础上，提出了以单向函数与单向暗门函数为基础的全球第一个非对称加密算法，即公开密钥算法。1977 年，美国麻省理工学院的罗纳德·李维斯特（Ronald Rivest）、阿迪·萨沙米（Adi Shamir）和伦纳德·阿德曼（Leonard Aderman）共同发布了著名的 RSA 非对称密钥算法，并成为全世界最流行的公开密钥方法，被 ISO 推荐为公钥数据加密标准。非对称加密方法的出现带来了一种新的安全属性：不可否认性（或称抗抵赖性）。传统抗抵赖基本依靠验笔迹、骑缝章、骑缝签名等方法，这些方法无法应用到数字媒介上。非对称加密方法的出现为抗抵赖提供了可能，这就是数字签名。如果公开解密密钥，并用不公开的加密密钥对信息进行加密后发布，则信息接收方可用公钥进行解密，从而可以验证持有私钥方发布信息的完整性，以及确认该信息确实是私钥持有者发送。这里，私钥被称作数字签名，而公钥就是数字证书。

2. 经典的安全模型

随着密码学、访问控制技术、信息系统安全模型及评价的理论和技术的发展，以上述技术为基础构建的安全防范体系成为当时的主流，图 1-1 给出了其基础架构图。其中，密钥源 K_1 与密钥源 K_2 既可以相等，也可以不相等，EK_1 为加密算法，DK_2 为解密算法。

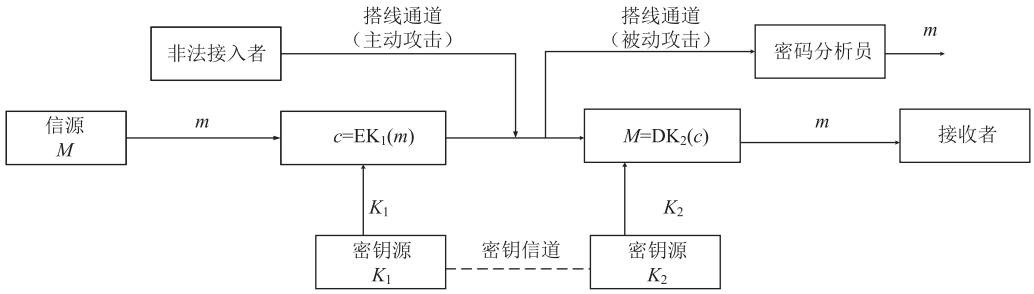

图 1-1　安全防范体系基础架构

1.2.3　信息保障阶段

20 世纪 90 年代，全球迅速进入以 Internet 为代表的信息时代，基于 Internet 的应用在各个领域不断普及和深入。同时，以 Internet 技术为背景的网络犯罪行为也日渐严重，单纯依靠加密体系“御敌于国门之外”的思想已无法应付千变万化的攻击行为。1998 年 10 月，美国国家安全局发布了“信息保障技术框架(information assurance technical framework，IATF)”1.1 版本，并在以后的几年中不断加以完善。IATF 提出了人、技术和操作是信息保障三个要素的概念，提出了纵深防御战略核心思想，确立了网络基础设施防御、区域边界防御、计算环境防御和支撑性基础设施防御等四个防御界面。网络基础设施：包括广域网络在内的交换与通信网络；区域边界：与其他公共或专用网络的边界，包括物理和逻辑边界；计算环境：进行数据处理的客户机、服务器和应用系统；支撑性基础设施：包括密钥管理、检测和响应等功能。纵深防御战略就是采用一个多层次的、纵深的安全措施来保障用户信息及信息系统的安全。

这一理念体现了信息安全不仅只是技术问题的认识。从 20 世纪 90 年代中期开始，以整体观点和复杂网络思想研究信息安全成为一个热点，并取得了一系列引人注目的成果。如流量自相似性、结构无标度性、无标度网络模型、病毒传播模型、网络拥塞相变模型等。

1.3　网络与信息安全面临的威胁与分类

安全威胁指自然的或人为的原因，使信息资源的保密性、完整性、可用性、可控性和不可否认性等属性面临的危险。

1.3.1　自然的和人为的安全威胁

有些安全威胁是不可抗拒的，称为自然的安全威胁，如地震等。对于这些安全威胁，最好的防范措施是建立适当的容灾备份系统。

绝大部分安全威胁是人(或者间接是人)造成的，称为人为的安全威胁。这种威胁又可分为无意的威胁(如误操作)和故意的威胁(如恶意攻击、病毒、木马)。精心设计的人为攻击往往威胁最大。

1.3.2　不同层次的安全威胁

ISO 提出了一个具有七层体系结构的开放系统互联参考模型(open systems interconnection reference model, OSI/RM)。由美国国防部高级研究计划局的卡恩和斯坦福的瑟夫提出的传输控制协议/网际协议(transmission control protocol/internet protocol, TCP/IP)，其四层体系结构最终成为事实上的工业标准(见表 1-1)。

表 1-1　TCP/IP 四层体系架构

OSI/RM	TCP/IP	安全威胁及处理措施
应用层	应用层	利用操作系统和网络协议上的漏洞进行的各种攻击。措施：加强安全服务，如安全协议、检测、加密等
表示层		
会话层		
传输层	传输层	身份假冒、权限滥用、路由侦听、重定向等。措施：实施安全控制技术，如身份认证、审计、网络管理等
网络层	网际层	
数据链路层	数据接口层	自然灾害、电磁辐射、数据监听、窃取、删除等。措施：物理安全技术，如容灾、屏蔽、监控等
物理层		

1.3.3　主动型和被动型安全威胁

根据攻击者的行为特征，安全威胁还可以分为主动型安全威胁和被动型安全威胁。

1. 主动型安全威胁

主动型安全威胁是指攻击者通过暴力行为或者利用相应漏洞实施的故意威胁行为。大部分的安全威胁都属于主动型的，也相对比较容易被发现。比较典型的主动型安全威胁包括伪装、重放、修改报文、拒绝服务、非授权访问、否认、信息泄露、特洛伊木马、后门或陷门、计算机病毒等。

(1)伪装：攻击者隐藏非法身份进行安全威胁。

(2)重放：重放攻击包含数据单元的被动捕获，随后再重传这些数据，从而产生非授权的效果。

(3)修改报文：修改报文攻击意味着合法报文的某些部分已被修改，或者报文的延迟和重新排序，从而产生非授权的效果。

(4)拒绝服务：拒绝服务攻击是阻止或禁止通信设施的正常使用和管理。这种攻击可能针对专门的目标(如安全审计服务)，抑制所有报文直接送到目的站；也可能破坏整个网络，使网络不可用或网络超负荷，从而降低网络性能。

(5)非授权访问：没有经过同意，就使用网络或计算机资源被看作非授权访问，例如，有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。

(6)否认：和心理学领域一样，计算机领域中的否认也是不承认已经发生的对自己不利的事件，以逃避谴责和责任。

(7)信息泄露：有意或无意地将需要保密的信息透露给无授权第三方。

(8)特洛伊木马：特洛伊木马简称“木马”，名称来源于希腊神话，有“一经潜入，后患无穷”之意，其特点是伪装成一个实用程序，诱使用户将其安装在个人计算机(personal computer，PC)或者服务器上，暗中打开端口，向指定地点发送数据，或者进行其他破坏活动。

(9)后门或陷门：可以不经安全检查进入系统的秘密入口。作为一种便于调试和测试程序的技术，已经合法地存在了很多年。但当被无所顾忌地滥用时，就变成了威胁。

(10)计算机病毒：编制或者在计算机程序中插入破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

2. *被动型安全威胁*

被动型安全威胁主要是从事信息收集而不是进行主动地访问。相较于主动型安全威胁，被动型安全威胁很难发现。被动型安全威胁包括嗅探、流量分析等攻击方法。

(1)嗅探：攻击者利用某些特殊的工具(如 sniff)监听网络上正在传输的数据包，以此获取正在传输的信息。

(2)流量分析：通过分析收集到的数据包流量的外在特征(如报文传输的频率、报文的长度、延迟抖动等)，以获得流量的类型、位置和标识等信息，为进一步的攻击提供依据。

本 章 习 题

1. 阐述信息安全的五大属性及相关的手段和技术。
2. 在 TCP/IP 模型的各个层次上分别面临着哪些安全威胁？
3. 举出两个高级持续性渗透攻击的案例。
4. 说说你听到或遇到的印象深刻的网络与信息安全事件。

第 2 章　信息安全体系及评价

信息安全体系是“免疫系统”，评价需要聚焦三方面：有效性(能否实时阻截威胁)、完整性(能否覆盖数据全生命周期)、适应性(能否随业务演进快速调整)。真正的安全不是静态高墙，而是创价值的护航能力、利共享的协同防线、永共生的动态生态。本章介绍相关常识。

2.1　信息安全体系结构

2.1.1　概述

1988 年，ISO 颁布了 ISO 7498-2 标准，提出了网络安全系统的体系结构。参照 ISO 7498-2，我国在 1995 年颁布了《信息处理系统　开放系统互连参考模型　第 2 部分：安全体系结构》(GB/T 9387.2—1995)。OSI 信息安全体系结构指出了计算机网络及信息系统需要的安全服务和解决方案，明确了各类安全服务在 OSI 模型中的位置。在不同层次满足不同的安全需求的技术路线对信息安全的发展起到了极为重要的作用。ISO 信息安全体系结构的提出对构建网络环境下的信息安全解决方案具有非常重要的指导意义，为异构机之间、进程之间的安全通信奠定了重要基础。

OSI 安全体系结构定义了五大类安全服务、八类安全机制，以及相应的安全管理，并指出可根据具体的系统需求在 OSI 七层模型中进行适当的配置(见图 2-1)。

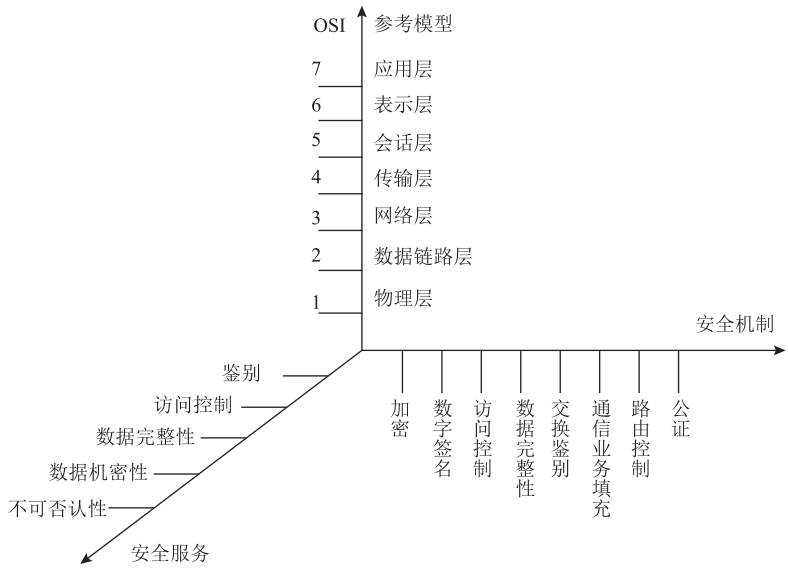

图 2-1　OSI 参考模型

表 2-1 列出了 OSI 模型各层提供的主要安全服务内容。

表 2-1　OSI 模型各层提供的安全服务

安全服务		物理层	数据链路层	网络层	传输层	会话层	表示层	应用层
鉴别	对等实体鉴别			Y	Y			Y
	数据源发鉴别			Y	Y			Y
访问控制				Y	Y			Y
数据机密性	连接机密性	Y	Y	Y	Y		Y	Y
	无连接机密性		Y	Y	Y		Y	Y
	选择字段机密性						Y	Y
	业务流机密性	Y		Y			Y	Y
数据完整性	可恢复的连接完整性				Y		Y	Y
	不可恢复的连接完整性			Y	Y		Y	Y
	选择字段连接完整性						Y	Y
	无连接完整性			Y	Y		Y	Y
	选择字段无连接完整性			Y	Y		Y	Y
不可否认性	数据原发证明不可否认							Y
	交付证明的不可否认							Y

注：Y 代表“Yes”，表示该 OSI 层能够提供对应的安全服务。

物理层：提供连接机密性和(或)业务流机密性服务，这一层没有无连接服务，物理层以上不能提供完全的业务流机密性。

数据链路层：提供连接机密性和无连接机密性服务。

网络层：可以在一定程度上提供鉴别、访问控制、数据机密性(除了选择字段机密性)和数据完整性(除了可恢复的连接完整性、选择字段的连接完整性)服务。

传输层：可以提供鉴别、访问控制、数据机密性(除了选择字段机密性、业务流机密性)和数据完整性(除了选择字段的连接完整性)服务。

会话层：不提供安全服务。

表示层：可以提供安全服务，主要包括数据机密性和数据完整性。它通过加密、数据格式转换等功能，既自身实现安全服务，也为应用层的安全机制提供支撑。

应用层：必须提供所有的安全服务，它是唯一能提供选择字段机密性服务和不可否认性服务的一层。

2.1.2　安全服务

安全服务也称为安全功能，是指为加强网络信息系统安全性和对抗网络攻击行为而采取的一系列技术措施。在 ISO 的标准中，定义的安全服务包括鉴别、访问控制、数据机密性、数据完整性和不可否认性。

1. 鉴别服务

鉴别，也称为认证，目的是保证通信双方主体的真实性和通信数据的真实性。鉴别分为标识鉴别和数据鉴别。标识鉴别是对主体的识别和证明，包括收发双方的真实性鉴别，用于防止第三者的冒名顶替；数据鉴别是对客体的鉴别，包括数据源和数据目的地的真实性鉴别，主要检查主体对客体的负责性，防止出现冒名伪造的数据，鉴别数据源的合法性。

2. 访问控制服务

访问控制是防止系统资源被非授权使用的措施，保障系统的可控性。通信双方都可以使用访问控制，也可以在通信链路上的某个中间位置进行访问控制。访问控制可以设置在通信模型的多个层次上，如应用层、传输层和网络层等。

3. 数据机密性服务

数据机密性服务可以提供不同范围的数据加密服务，以防数据泄露。防止数据泄露的措施包括连接机密性、无连接机密性、选择字段机密性、业务流机密性。

4. 数据完整性服务

数据完整性服务用于保证接收的数据未经复制、插入、篡改、重排或重放，主要用于防止非授权的篡改和破坏等行为。对遭受一定程度毁坏的数据进行完整性恢复，即带恢复的数据完整性。数据完整性可用于一个消息流、单个消息或一个消息中的所选字段。

5. 不可否认性服务

不可否认，也称为抗否认，用于防止通信双方中某一方抵赖传输的消息。源发不可否认：向数据接收者提供数据源的证据，防止发送者否认发送过这个数据；接收不可否认：向数据发送者提供数据已接收的证据，接收者事后不能否认曾收到此数据。

2.1.3　安全机制

安全机制是安全服务的技术实现手段。一种安全服务可以通过多个安全机制加以实现；同样地，一个安全机制也可以为多种安全服务的实现提供措施。

在 ISO 标准中，安全机制分为两大类，普遍安全机制不属于任何协议层或安全服务，包括可信功能度、安全标记、事件检测、安全设计和安全恢复等五种；特定安全机制在某个或某几个协议层实现，共八种。

1. 加密机制

加密机制是网络安全的核心技术，是提供数据保密最常用的方法。加密技术不仅应用于数据的存储和传输的过程中，也常应用于程序运行过程中。按密钥类型分为对称密钥加密和非对称密钥加密；按密码体制分为序列密码和分组密码。加密可以在 OSI 的不