第一章：绪论

信息：事物运动的状态和状态变化的方式 网络安全指的是网络与信息系统的信息安全 信息安全：指信息系统的软件、硬件以及系统中存储和传输的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，信息系统连续、可靠、正常地运行，信息服务不中断。

信息安全的目标是保护网络与信息系统中信息的机密性、 完整性、 不可抵赖性、 可用性和可控性等信息安全属性

信息安全的三要素：机密性、完整性、可用性 信息安全属性：**机密性**（能够确保敏感数据或机密数据在存储和传输过程中不被非授权的实体浏览，至可以保证不暴露保密通信的事实,通过访问控制阻止非授权用户获得机密信息，通过加密变换阻止非授权用户获知信息内容）**完整性**（能够保障被传输、接收、存储的数据是完整和未被非法修改的，在被非法修改的情况下能够发现被非法修改的事实和位置一般通过访问控制阻止篡改行为，同时通过消息摘要算法来检验信息是否被篡改。信息的完整性包括数据和系统的完整性）**真实性**（参与通信或操作的实体（用户、进程、系统等）身份的真实以及信息来源的是否真实。确保实体就是所声称的实体,技术：标识和认证）**不可否认性**（实体的行为或事件的结果是不能被否认的。技术：审计和日志，数字签名和安全协议）**可靠性**（信息系统运行的过程和结果是可以被信赖的。通常用平均无故障时间来描述；如果系统被黑客控制，则不可靠）**可用性**（当突发事件发生时，用户依然能够得到或使用信息系统的数据，信息系统的服务亦能维持运行，可用性是信息资源服务功能和性能可靠性的度量，涉及到物理、网络、系统、数据、应用和用户等多方面的因素，是对信息网络总体可靠性的要求）**可控性**（能够掌握和控制信息及信息系统的情况，对信息和信息系统的使用进行可靠的授权、审计、责任认定、传播源与传播路径的跟踪和监管等。技术：访问控制）保鲜性（信息必须是在其时效之内的，不能是过时的。新鲜性对保证物联网的安全尤其重要）四大安全属性：机密性，可认证性，不可抵赖，完整性 四个信息安全时期：**通信安全时期**（这个时期的安全性是指信息的保密性， 对安全

理论和技术的研究也仅限于密码学。 这一阶段的信息安全技术可以简称为通信安全， 关注如何保证数据在从一地传送到另一地时的安全性）**计算机安全时期**（信息已经分成静态信息和动态信息。人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的信息安全阶段。TCSEC）**网络安全时代**（信息安全的焦点已经从传统的保密性、完整性和可用性三个原则衍生为可控性、抗抵赖性、真实性）**信息安全保障时代**（信息保障技术框架》 (IATF)，面向业务的安全保障： 体系性的安全保障理念，深度防御体系，从整体角度考虑其体系建设的信息安全保障时代）

信息安全可被理解为信息系统抵御信息安全威胁，保证信息系统处理维护的数据以及提供的服务的安全属性的能力。信息安全威胁是对信息资源或信息系统的安全使用可能造成的危害，主要包括意外事件和人为恶意攻击两大类。精心设计的人为恶意攻击的威胁最大 **信息泄露**（保护的信息被泄露或透露给某个非授权的实体）**非授权的篡改**（信息的内容被非授权地进行增删、修改或破坏而受到损失）**拒绝服务**（信息使用者对信息或其他资源的合法访问被无条件地阻止）**非法使用/非授权访问**（某一资源被某个非授权的人或系统使用，或以非授权的方式使用）**假冒**（一个非法用户或信息系统通过冒充成为另一个合法用户或合法系统，或者特权小的用户／系统冒充成为特权大的用户／系统）**抵赖**（一种来自用户的攻击，涵盖范围比较广泛。比如，否认自己曾经发布过的某条消息，否认曾经处理过某些信息等）**网络与系统攻击**（利用网络系统和协议的缺陷和漏洞，进行恶意的侵入和破坏）**恶意代码**（开发、传播意在破坏计算机系统、窃取机密或远程控制的程序，主要包括计算机病毒、蠕虫、木马、僵尸网络等）**自然灾害**（如火灾、水灾等意外事件，损毁、破坏信息系统的硬件设备，从而使得信息和信息系统不可用）**人为失误和故意破坏**（恶意的人故意破坏，或者授权用户的操作失误，使得信息或信息系统遭到损坏）**信息安全是相对的，不安全才是绝对的。**

**①核心基础安全技术**：密码技术主要包括密码算法和密码协议的设计与分析技

术；信息隐藏技术：将特定用途的信息隐藏在其他可公开的数据或载体中，使得它难以被消除或发现 **②安全基础设施技术**：标识与认证技术：鉴别实体身份的技术 授权与访问控制技术：给已通过认证的用户授予相应的操作权限，实施和管理这些权限的技术称为授权技术 ③基础设施安全技术：主机系统安全技术：主机系统主要包括操作系统和数据库系统等。操作系统需要保护所管理的软硬件、操作和资源等的安全，数据库需要保护业务操作、数据存储等的安全；网络系统安全技术：在基于网络的分布式系统或应用中，信息需要在网络中传输，用户需要利用网络登录并执行操作，因此需要相应的信息安全措施 ④应用安全技术：网络与系统攻击技术：攻击者利用信息系统弱点破坏或非授权地侵入网络和系统的技术；网络与系统安全防护及应急响应技术：抵御网络与系统遭受攻击的技术；安全审计与责任认定技术：相应事件的调查方法与取证手段；恶意代码检测与防范技术：利用恶意代码的不同特征来检测并阻止其运行；内容安全技术：监控数字内容传播的技术 ⑤支撑安全技术：信息安全测评技术：对信息安全产品或信息系统的安全性等进行验证、测试、评价和定级；信息安全管理技术：涉及安全管理制度的制定、物理安全管理、系统与网络安全管理、信息安全等级保护及信息资产的风险管理等内容；信息安全保障技术框架：基本内容是深度防御策略、信息保障框架域和信息系统安全

信息安全模型是信息系统在何种环境下遭受威胁并获得信息安全的一般性描述，主要包括：保密通信系统的模型（描述了保密通信的收发双方通过安全信道获得密钥、通过可被窃听的线路传递密文的场景，确定了收发双方和密码分析者的基本关系和所处的技术环境）无仲裁认证模型（描述了认证方和被认证方通过安全信道获得密钥、通过可被窃听的线路传递认证消息的场景）Dolev-Yao威胁模型（定义了攻击者在网络和系统中的攻击能力，被密码协议的设计者广泛采用，重要的原则：永远不能低估攻击者的知识和能力）

信息安全保障技术框架(IATF)：将信息系统的信息保障技术层面划分成了四个技术框架焦点域：网络和基础设施、区域边界、计算环境和支撑性基础设施 核心思想：纵深防御战略（采用一个多层次、纵深的安全措施来保障用户信息及信息系统的安全。在纵深防御战略中，人、技术和操作是三个主要核心要素）信息安全(IA)原则：保护多个位置、分层防御、安全强健性

网络空间安全战略：将网络空间安全提升到国家战略的高度，习近平同志指出： “ 没有网络安全就没有国家安全”。2016年12月27日，国家互联网信息办公室发布《国家网络空间安全战略》指出，“网络空间的国际竞争方兴未艾”是我国网络空间安全面临的重大挑战之一

**第二章：密码技术**

密码学=密码编码学+密码分析学

密码编码学：研究密码变化的客观规律，设计各种加密方案，编制密码以保护信息安全的技术 密码分析学：在不知道任何加密细节的条件下，分析、破译经过加密的消息以获取信息的技术 密码学模型：明文到密文的变换法则，即加密方案，称为加密算法；而密文到明文的变换法则称为解密算法。加／解密过程中使用的明文、密文以外的其他参数，称为密钥。 密码体制：一个用于加解密并能够解决网络安全中的机密性、完整性、可用性、可控性和真实性等问题中的一个或几个的系统，定义为一个五元组(P, C, K, E, D)：P称为明文空间，是所有可能的明文构成的集合；C称为密文空间，是所有可能的密文构成的集合；K称为密钥空间，是所有可能的密钥构成的集合；E和D分别表示加密算法和解密算法的集合 2种密码体制：对称密码和非对称密码 密码体制的安全性：无条件安全：如果无论攻击者获得多少可使用的密文，都不足以唯一地确定由该体制产生的密文所对应的明文 计算上安全：破译密码的代价超出密文信息的价值且破译密码的时间超出密文信息的有效生命期 密码分析攻击：唯密文攻击：攻击者在仅已知密文的情况下，企图对密文进行解密。这种攻击是最容易防范的，因为攻击者拥有的信息量最少。已知明文攻击：攻击者获得了一些密文信息及其对应的明文，也可能知道某段明文信息的格式等。比如，特定领域的消息往往有标准化的文件头。选择明文攻击：攻击者可以选择某些他认为对攻击有利的明文，并获取其相应的密文。如果分析者能够通过某种方式，让发送方在发送的信息中插入一段由他选择的信息，那么选择明文攻击就有可能实现 选择密文攻击：密码攻击者事先搜集一定数量的密文，让这些密文透过被攻击的加密算法解密，从而获得解密后的明文。 穷举攻击：攻击者对一条密文尝试所有可能的密钥，直到把它转化为可读的有意义的明文，平均来说，要获得成功必须尝试所有可能密钥的一半。

对称密码体制也叫单钥密码体制或秘密密钥密码体制，在对称密码体制中，加密和解密使用完全相同的密钥，或者加密密钥和解密密钥彼此之间非常容易推导 对称密码分为两大类：流密码（加密和解密每次只处理数据流的一个符号）和分组密码（它将明文消息划分成若干长度为m(m>1)的分组，各组分别在长度为r的密钥K的控制下转换成长度为n的密文分组。绝大部分基于网络的对称密码应用使用的是分组密码） 古典密码：古典密码技术以字符为基本加密单元，古典密码学充分体现了现代密码学的两大基本思想：置换和代换，还将数学的方法引入到密码分析和研究中 流密码：置换技术：保持明文中的字母本身不变，但将所有字母重新排列，即仅仅改变明文字母的位置，这样的密码技术称为置换。栅栏技术是最简单的置换技术。栅栏密码把要加密的明文分成N个一组，然后把每组的第一个字符连起来，再加上第二个、第三个，以此类推。本质上，是把明文字母一列一列地组成一个矩阵，然后一行一行地读出。 代换技术在现代密码学中也得到了广泛应用。所谓代换，是将明文字母用其他字母、数字或符号替换的一种方法。 Caesar密码：对每个字母用它之后的第3个字母来代换 单表代换密码：对明文的所有字母采用同一个代换表进行加密，每个明文字母映射到一个固定的密文字母，称为单表代换密码。 密钥短语密码：选一个英文短语作为密钥字或密钥短语，如HAPPYNEWYEAR，去掉重复字母得HAPYNEWR。将它依次写在明文字母表之下，而后再将字母表中未在短语中出现过的字母依次写于此短语之后，就可构造出一个字母代换表 英语语言具有很强的统计规律 多表代换加密：为了进一步提高安全性，一种对策是对每个明文字母提供多种代换，即对明文消息采用多个不同的单表代换。这种方法一般称之为多表代换密码 Hill密码：每个字母指定为一个26进制数字：a=0，b=l，c=2，…，z=25。m个连续的明文字母被看做m维向量，与一个m\*m的加密矩阵相乘，再将得出的结果模26，得到m个密文字母。即m个连续的明文字母作为一个单元，被转换成等长的密文单元。注意加密矩阵（即密匙）必须是可逆的，否则就不可能译码。 RC4流密码算法：以一个足够大的表S为基础，用可变长度的种子密钥K对表进行非线性变换，产生密钥流 分组密码：数据加密标准(DES)：采用了S-P网络结构，分组长度为64位，密钥长度为56。加密和解密使用同一算法、同一密钥、同一结构。区别是加密和解密过程中16个子密钥的应用顺序相反——已不安全 三重DES（破解密文需要2^112次穷举搜索）高级加密标准(AES)

在传统的对称密码体制中，加密和解密使用相同的密钥，每对用户之间都需要共享一个密钥，而且需要保持该密钥的机密性。当通信的用户数目比较多的时候，密钥的产生、存储和分发是一个很大的问题。

非对称密码体制也称为公钥密码体制：在公钥密码体制中，加密和解密使用不同的密钥，而且由其中一个推导另外一个是非常困难的。这两个不同的密钥，往往其中一个是公开的而另外一个保持秘密性，任何人都可以加密，但只有掌握解密密钥的用户才能解密。公钥密码体制不仅用于加解密，而且可以广泛用于消息鉴别、数字签名和身份认证等服务。公钥密码体制并不会取代对称密码体制，原因在于公钥密码体制算法相对复杂，加解密速度较慢 实际应用中，公钥密码和对称密码经常结合起来使用，对数据的加解密使用对称密码技术，而密钥管理使用公钥密码技术。 公钥密码体制原理：①公钥算法建立在数学函数基础上，而不是基于替换和置换。其安全性基于数学上难解的问题，如大整数因子分解问题、有限域的离散对数问题、平方剩余问题、椭圆曲线的离散对数问题等 ②公钥密码是非对称的，加／解密分别使用两个独立的密钥：加密密钥可对外界公开，称为公开密钥或公钥；解密密钥只有所有者知道，称为秘密密钥或私钥，由一个密钥推知另一个密钥，在计算上是不可能的。③基于公钥密码体制，通信双方无需预先商定密钥就可以进行秘密通信，克服了对称密码体制中必须事先使用一个安全通道约定密钥的缺点。 公钥密码体制特点：①加密／解密使用不同的密钥；②发送方拥有加密密钥或解密密钥，而接收方拥有另一个密钥；③根据密码算法和加密密钥以及若干密文，要恢复明文在计算上是不可行的；④根据密码算法和加密密钥，确定对应的解密密钥在计算上是不可行的。 公钥密码体制应满足的5个基本条件：①产生一对密钥(公钥PU，私钥PR)在计算上是容易的。②已知接收方B的公钥和要加密的消息M，消息发送方A产生相应的密文在计算上是容易的③消息接收方B使用其私钥对接收的密文解密以恢复明文在计算上是容易的④已知公钥时，攻击者要确定对应的私钥PRB在计算上是不可行的⑤已知公钥和密文C，攻击者要恢复明文M在计算上是不可行的 公钥密码必须满足的条件公钥密码必须满足的条件：加密和解密函数的顺序可以交换。公钥密码体制是建立在数学中的单向陷门函数的基础之上的。 单向陷门函数：如果给定某些辅助信息（称为陷门信息），就易于求逆的函数。 目前比较流行的公钥密码体制主要有两类：一类是基于大整数因子分解问题的，最典型的代表是RSA；另一类是基于离散对数问题的，比如ECC RSA是一种分组密码体制，其理论基础是数论中“大整数的素因子分解是困难问题”的结论，即求两个大素数的乘积在计算机上时是容易实现的，但要将一个大整数分解成两个大素数之积则是困难的 密钥计算方法：①选择两个大素数p和q②计算n=p\*q 和 z=(p-1)\*(q-1)③选择一个与z互质的数，令其为d④找到一个e使满足e\*d =1 (mod z)⑤公开密钥为(e, n)，私有密钥为(d, n) 加密方法：①将明文看成比特串，将明文划分成k位的块P即可，这里k是满足2^k<n的最大整数。②对每个数据块P，计算C＝P^e (mod n)，C即为P的密文。解密方法：对每个密文块C，计算P＝C^d (mod n)，P即为明文。 RSA的缺点: ①产生密钥很麻烦，受到素数产生技术的限制，因而难以做到一次一密。②分组长度太大，为保证安全性，n至少也要600比特以上，使运算代价很高，尤其是速度较慢，相比对称密码算法慢几个数量级；且随着大数分解技术的发展，这个长度还在增加。

散列函数：一种将任意长度的消息映射到某一固定长度消息摘要（散列值或哈希值）的函数。消息摘要相当于是消息的“指纹”，用来防止对消息的非法篡改。散列函数也常常被称为Hash函数 散列函数的安全性：单向性、强抗碰撞性和弱抗碰撞性 单向性是指对任意给定的散列码H，找到满足H(x)=H的x在计算上是不可行的 强抗碰撞性是指散列函数满足下列四个条件：①散列函数H的输入是任意长度的消息M;②散列函数H的输出是固定长度的数值；③给定H和M，计算H(M)是容易的④给定散列函数H，寻找两个不同的消息M1和M2，使得H(M1)=H(M2)，在计算上是不可行的。弱抗碰撞性的散列函数满足强抗碰撞散列函数的前三个条件，但具有一个不同的条件：给定H和一个随机选择的消息M，寻找消息M'，使得H(M)=H(M')在计算上是不可行的，即不能找到与给定消息具有相同散列值的另一消息。 目前使用最多的两种散列函数是MD5和SHA序列函数

消息鉴别也称为“报文鉴别”或“消息认证”，是一个对收到的消息进行完整性和真实性验证的过程 过程：用鉴别函数产生一个鉴别符，根据收发端的鉴别符是否一致，对消息进行鉴别 鉴别函数可以分为如下三类：①基于消息加密：以整个消息的密文作为鉴别符。②基于消息鉴别码：利用公开函数和密钥产生一个较短的定长值作为鉴别符，并与消息一同发送给接收方，实现对消息的验证③基于散列函数：利用公开的散列函数将任意长的消息映射为定长的散列值，并以该散列值作为鉴别符 消息鉴别码又称密码校验和，其实现鉴别的原理是：利用公开函数和密钥生成一个固定大小的小数据块，即MAC，并将其附加在消息之后传输。接收方利用与发送方共享的密钥进行鉴别 MAC鉴别原理 基于DES的消息鉴别码：每个明文分组在用密钥加密之前，要先与前一个密文分组进行异或运算。用一个初始向量IV作为密文分组初始值 基于散列函数的鉴别：HMAC（略）

消息鉴别通过验证消息完整性和真实性，可以保护信息交换双方不受第三方的攻击，但是它不能处理通信双方内部的相互的攻击，这些攻击可以有多种形式，数字签名是解决通信双方内部相互攻击的最好方法，它的作用相当于手写签名。数字签名的基本目的是认证、核准和负责，防止相互欺骗和抵赖。数字签名在身份认证、数据完整性、不可否认性和匿名性等方面有着广泛的应用

数字签名：附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据和变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人（例如接收者）进行伪造 形式化定义：一个数字签名体制是一个五元组(M，A，K，S，V) M是所有可能的消息的集合，即消息空间；A是所有可能的签名组成的一个有限集，称为签名空间；K是所有密钥组成的集合，称为密钥空间；S是签名算法的集合；V是验证算法的集合 数字签名必须具有的4个特征：①可验证性。信息接收方必须能够验证发送方的签名是否真实有效②不可伪造性。除了签名人之外，任何人不能伪造签名人的合法签名③不可否认性。发送方在发送签名的消息后，无法抵赖发送的行为；接收方在收到消息后，也无法否认接收的行为④数据完整性。数字签名使得发送方能够对消息的完整性进行校验。即数字签名具有消息鉴别的功能 数字签名应满足的6个条件：①签名必须是与消息相关的二进制位串。②签名必须使用发送方某些独有的信息，以防伪造和否认。③产生数字签名比较容易。④识别和验证签名比较容易。⑤伪造数字签名在计算上是不可行的。无论是从给定的数字签名伪造消息，还是从给定的消息伪造数字签名，在计算上都是不可行的。⑥保存数字签名的拷贝是可行的。 数字签名算法：基于RSA的数字签名 基于公钥密码算法和对称密码算法都可以获得数字签名， 目前主要是基于公钥密码算法的数字签名

**第三章 身份认证**

身份认证：确认某个实体是所声称的实体的行为 包括两种情况：①计算机认证人的身份，称之为用户认证 ②计算机认证计算机，主要出现在通信过程中的认证握手阶段，称之为认证协议。 用户认证是由计算机对用户身份进行识别的过程，用户向计算机系统出示自己的身份证明，以便计算机系统验证确实是所声称的用户，允许该用户访问系统资源 用户认证是对访问者授权的前提 包括以下三种：所知道的信息；所拥有的物品；所具有的独一无二的身体特征 基于口令的认证：是最简单、最易实现、最易理解和接受的一种认证技术，也是目前应用最广泛的认证方法，包括静态口令和动态口令 静态口令：是指用户口令是静态的口令是一种根据“所知道的信息”实现身份认证的方法，其优势在于实现的简单性，无须任何附加设备，成本低、速度快 两个问题：口令存储（如果口令以明文方式存储，则易受字典攻击，可用散列解决）口令传输（一般采用双方协商好的加密算法或单向散列函数对口令进行处理后传输） 静态口令的认证方式存在的安全问题：①它是一种单因素的认证方式，安全性全部依赖于口令，口令一旦被泄露，用户即可被冒充②为了便于记忆，用户往往选择简单、容易被猜测的口令，如生日。这使得口令被攻击的难度大大降低③口令在网络上传输的过程中可能被截获④ 系统中所有用户的口令以文件形式存储在认证方，攻击者可以利用系统中存在的漏洞获取系统的口令文件⑤用户在访问多个不同安全级别的系统时，都要求用户提供口令，用户为了记忆的方便，往往采用相同的口令⑥口令方案无法抵抗重放攻击⑦ 只能进行单向认证，即系统可认证用户，而用户无法对系统进行认证，攻击者可能伪装成系统骗取口令 动态口令又叫做一次性口令，是指在用户登录系统进行身份认证的过程中，送入计算机系统的验证数据是动态变化的 动态口令的主要思路是在登录过程中加入不确定因素，如时间。系统执行某种加密算法E(用户名+密码+不确定因素)，产生一个无法预测的动态口令，以提高登录过程的安全性 动态口令的产生：共享一次性口令表（系统和用户共享一个秘密口令表，每个口令只使用一次。用户登录时，系统需要检查用户的口令是否使用过）口令序列（用户拥有一个长度为N、单向的、根据某种单向算法前后相关的口令序列，每个口令只使用一次。用户用第M个口令登录时，计算机系统用单向算法计算第M个口令，并与用户输入的第M个口令比对，实现对用户的认证。用户登录N次后，必须重新初始化口令序列）挑战—响应方式（用户登录时，系统产生一个随机数发送给用户。用户使用某种单向算法将自己的口令和随机数混合起来运算，结果发送给系统。系统用同样的方式进行运算，并通过结果比对实现对用户的认证）时间—事件同步机制（这种方式可以看做挑战—响应方式的变形，区别在于以用户登录时间作为随机因素。这种方式要求双方的时间要同步） 基于电子令牌卡生成口令的工作原理：①用户和计算机系统之间共享同一个用户口令。用户还拥有一种叫做动态令牌的专用硬件，内置电源、密码生成芯片和显示屏，密码生成芯片运行专门的密码算法②当用户向认证系统发出登录请求时，认证系统向用户发送挑战数据。挑战数据通常是由两部分组成的，一部分是种子值，它是分配给用户的在系统内具有唯一性的一个数值，而另一部分是随时间或次数不断变化的数值③用户接收到挑战后，将种子值、随机数值和用户口令输入到动态令牌中进行计算，并把结果作为应答发送给远程认证系统。远程认证系统使用相同的算法和数据进行计算，与从用户那里接收到的应答数据作对比，认证用户的合法性 动态口令的技术特点：动态性，随机性，一次性，方便性 智能卡是一种集成的带有智能的电路卡，内置可编程的微处理器，可存储数据，并提供硬件保护措施和加密算法，在智能卡中存储用户个性化的秘密信息，同时在验证服务器中也存放该秘密信息，进行认证时，用户输入PIN智能卡认证PIN(Personal Identification Number，个人身份识别码)成功后，即可读出智能卡中的秘密信息，进而利用该秘密信息与主机之间进行认证 USB Key是一种USB接口的硬件设备。它内置单片机或智能卡芯片，有一定的存储空间，可以存储用户的私钥以及数字证书，利用USB Key内置的公钥算法实现对用户身份的认证。由于用户私钥保存在密码锁中，理论上使用任何方式都无法读取，因此保证了用户认证的安全性 主要特点：双因子认证（每一个USB Key都具有硬件和PIN码保护，PIN码和硬件构成了用户使用USBKey的两个必要因素）带有安全存储空间（USB Key具有8～128kB的安全数据存储空间，对该存储空间的读写操作必须通过程序实现，用户无法直接读取。其中用户私钥是不可导出的）硬件实现加密算法（USB Key内置CPU或智能卡芯片，可以实现数据摘要、数据加解密和签名的各种算法，加解密运算在USB Key内进行，保证了用户密钥不会出现在计算机内存中）便于携带、安全可靠 身份认证主要方式：基于挑战／应答的双因子认证方式；基于数字证书的认证方式（数字证书是由权威公正的第三方机构（即CA中心）签发的，由用户的身份与其所持有的公钥相结合的计算机文件） 基于生物特征识别的认证方式以人体具有的唯一的、可靠的、终生稳定的生物特征为依据，利用计算机图像处理和模式识别技术来实现身份认证。生物特征识别技术目前主要利用指纹（主要包括三个过程：指纹图像读取、特征提取、比对）、声音、虹膜、视网膜、脸形、掌纹这几个方面的特征进行识别 优点：①不易遗忘或丢失②防伪性能好，不易伪造或被盗③ “随身携带”，方便使用

认证协议通过一定的过程，保证使合法的协议一方（或双方彼此）确信对方确实是其所声称的那个实体。身份认证协议的实质是抗身份欺诈 单向认证是指通信双方中，只有一方对另一方进行认证。 步骤：①应答方B通过网络发送一个挑战②发起方A回送一个对挑战的响应③ 应答方B检查此响应，然后再进行通信 KDC干预的单向认证：每个用户与密钥分配中心(KDC)共享唯一的主密钥，KDC干预进行会话建立。 双向认证指通信双方相互验证对方的身份，双向认证协议可以使通信双方确信对方的身份并交换会话密钥。保密性和及时性是认证的密钥交换中两个重要的问题 对付重放攻击的2种方法：时间戳（要求通信各方的时钟应保持同步，不适合于面向连接的应用，不可预知的网络延时）挑战／应答（不适合于无连接的应用）

Kerberos：一种基于对称密码算法的网络认证协议，允许一个非安全的网络上的两台计算机通过交换加密消息互相证明身份。一旦身份得到验证，Kerberos协议给这两台计算机提供密钥，以进行安全的通信 解决分布式网络环境下，用户访问网络资源时的安全问题 实现包括一个运行在网络上某个物理安全节点处的密钥分发中心(KDC)以及一个函数库，各需要认证用户身份的分布式应用程序调用这个函数库实现对用户的认证

PKI(Public Key Infrastructure，公钥基础设施)技术：一种遵循标准的、利用公钥加密技术的一套安全基础平台的技术和规范，简单的说，PKI是基于公钥密码技术，支持公钥管理，提供真实性、保密性、完整性以及可追究性安全服务，具有普适性的安全基础设施 主要目的就是用来安全、便捷、高效地分发公钥 狭义的PKI一般指PKIX：基于X.509证书的 PKI模型框架 组成：权威认证机构(CA，Certificate Authority)、数字证书库、密钥备份及恢复系统、证书作废系统、应用接口 认证机构(CA)：CA是PKI的核心执行机构，是PKI的主要组成部分，人们通常称它为认证中心。CA是数字证书生成、发放的运行实体，在一般情况下也是证书撤销列表(CRL)的发布点，在其上常常运行着一个或多个注册机构(RA)，具备权威性的特征 数字证书库：证书库是CA颁发证书和撤销证书的集中存放地，可供公众进行开放式查询 密钥备份及恢复系统：只能针对解密密钥，签名私钥为确保其唯一性而不能够作备份 证书作废系统：证书作废处理系统是PKI的一个必备的组件。证书有效期以内也可能需要作废，原因可能是密钥介质丢失或用户身份变更等。在PKI体系中，作废证书一般通过将证书列入作废证书表(CRL)来完成 应用接口(API)：PKI的价值在于使用户能够方便地使用加密、数字签名等安全服务，因此，一个完整的PKI必须提供良好的应用接口系统，使得各种各样的应用能够以安全、一致、可信的方式与PKI交互，确保安全网络环境的完整性和易用性 X.509证书：版本号（区分合法证书的不同版本）序列号（一个整数，和签发该证书的CA名称一起惟一标识该证书）签名算法标识（指定证书中计算签名的算法，包括一个用来识别算法的子域和算法的可选参数）签发者（创建、签名该证书的CA的X.500格式名字）有效期（包含两个日期，即证书的生效日期和终止日期）证书主体名（持有证书的主体的X.500格式名字，证明此主体是公钥的所有者）证书主体的公钥信息（主体的公钥以及将被使用的算法标识，带有相关的参数）签发者惟一标识（用于惟一标识认证中心CA） 证书主体惟一标识（惟一标识证书主体） 扩展 签名 CA用它的私钥对证书签名， 如果用户知道相应的公钥， 则用户可以验证CA签名证书的合法性 CA的主要职能：①制定并发布本地CA策略。但本地策略只是对上级CA策略的补充，而不能违背②对下属各成员进行身份认证和鉴别③ 发布本CA的证书，或者代替上级CA发布证书④ 产生和管理下属成员的证书⑤ 证实RA的证书申请，返回证书制作的确认信息，或返回已制作的证书⑥ 接收和认证对所签发证书的撤销申请⑦ 产生和发布所签发证书和CRL⑧ 保存证书、CRL信息、审计信息和所制定的策略 PKIX管理协议任务：用户注册、用户初始化、认证、密钥对的备份和恢复、自动的密钥对更新、证书撤销请求、交叉认证 在PKIX中，不可抵赖性通过数字时间戳DTS(digital timestamp)和数据有效性验证服务器DVCS(data validation and certification server)（其验证声明称为数据有效性证书）实现 信任模型：就是提供用户双方相互信任机制的框架，是PKI系统整个网络结构的基础 分类：层次模型、交叉模型、混合模型、桥CA模型、信任链模型

**第四章 授权与访问控制技术**

授权：给已通过认证的用户授予相应的权限 两种授权技术：访问控制技术和PMI技术 客体：指信息数据、计算处理能力和网络通信资源等资源 访问：系统或用户对这些资源的使用 主体：访问者 实体：统一指代客体和主体 访问控制：是实施授权的基础，它控制资源只能按照所授予的权限被访问 访问控制策略是在系统安全较高层次上对访问控制和相关授权的描述，它的表达模型常被称为访问控制模型，是一种访问控制方法的高层抽象和独立于软硬件实现的概念模型。由于访问控制涉及主体授予针对客体的权限问题，因此本质上任何访问控制策略都可以用矩阵直观表示 主体属性：用户的级别或种类（组别属性，角色属性）、相关执行程序的性质、所处的网络或物理地址等，可能还包括其安全状态 客体属性：主要是所允许的操作及其信息级别，也可能包括其安全状态

自主访问控制(discretionary access control，DAC)：由客体的所有者（或控制者）对自己的客体进行管理，由所有者决定是否将自己客体的访问权或部分访问权授予其他主体 基于主体的身份和先行规定的访问规则来对访问进行控制，也就是说，系统允许客体的所有者按照自己的意愿去制定谁以何种访问模式去访问该客体的策略 自主访问控制在(可信计算机评价标准(TCSEC)的)C2级操作系统中应用广泛，是根据自主访问控制策略建立的一种模型，允许合法用户以用户或用户组的身份访问策略规定的客体，同时阻止非授权用户访问客体，某些用户还可以自主地把自己所拥有的客体的访问权限授予其他用户 思想：根据来访主体的身份，实施访问控制。客体的主人（即资源所有者）全权管理有关该客体的访问授权，有权泄露、修改该客体的有关信息 优劣：一方面使得访问控制的灵活性很高，另一方面由于信息在移动过程中其访问权限关系会被改变，使得原本不具有访问权限的主体也可能获得访问权限，造成安全方面的隐患 EG：Linux，UNIX，Windows Server

**传统DAC策略三点不足**：①资源管理比较分散②用户间的关系不能在系统中体现出来，不易管理③ 不能对系统中的信息流进行保护，容易泄露，无法抵御特洛伊木马 HRU：将访问权限的授予改为半自主式，主体仍然有权利将其具有的访问权限授予其他客体，但是，这种访问权限的授予行为要受到一个调整访问权限分配的**安全策略**的限制，通常这个安全策略由安全管理员来制定，相当于提案及表决机制， 也就是“ 主体给出提案，管理员裁定是否通过” **问题**：当主体集和客体集发生改变时，需要依赖安全管理员对访问权限的扩散策略进行更新 TAM：每当产生新主体时，管理员就得要对新主体的访问权限和它本身所拥有权限的扩散范围进行限定，每当产生新客体时，其所属主体和管理员就需要对其每一种权限的扩散范围进行限定 ATAM：在TAM策略的基础上，为了描述访问权限需要动态变化的系统安全策略而发展出来的安全策略 基于角色的DAC策略：增加角色，实现更细粒度的访问控制 基于时间特性的DAC策略：用户只能在某个时间点或者时间区间内对客体进行访问。该方法使主体可以自主地决定其他哪些主体可以在哪个时间访问它所拥有的客体，实现了更细粒度的控制 **DAC授权管理**：①集中式管理（单个的管理者或组对用户进行访问控制授权或授权撤销）②分级式管理（一个中心管理员把管理责任分配给其他管理员，这些管理员再对用户进行访问授权和授权撤销。分级式管理可以根据组织结构实行）③所属权管理（如果一个用户是一个客体的所有者，则该用户可以对其他访问该客体的用户进行访问授权和授权撤销）④协作式管理（对于特定系统资源的访问不能由单个用户授权决定，而必须要其他用户的协作授权决定）⑤分散式管理（在分散管理中，客体所有者可以把权力权限授权给其他用户） **访问控制实现技术**：保护位机制（每个操作系统客体都附有一个位集合，以便为不同安全类别的用户指定不同访问模式，保护位与客体相关联，Linux系统的文件访问控制）、能力表机制（每一个操作系统的主体与一个客体访问列表（能力表）相联系，它指定了主体可以访问的客体以及此主体对此客体相应的访问方式，能力表与主体相关联，故在一个特定时刻判断哪些主体对一个特定客体具有访问权限比较困难，这使得访问权限的撤销变得复杂，**能力表机制提供了一种在运行期间实行访问控制的方式在**，DBMS中可能发挥作用）访问控制表机制（**最流行**，每个客体有一个访问控制表，是系统中每一个有权访问这个客体的主体的信息，实际上是按列保存访问矩阵。保护位机制就是这样一种简化形式的访问控制表）授权关系表机制（对应访问矩阵中每一个非空元素的实现技术，是某一个主体对应于某一个客体的访问权限信息，**类似于稀疏矩阵，性能高**） **DAC不足之处**：①系统管理员难以确定哪些用户对哪些资源有访问权限，不利于实现统一的全局访问控制②DAC却存在用户滥用职权的问题③用户间的关系不能在系统中体现出来，不易管理④信息容易泄露，不能抵御特洛伊木马的攻击 **DAC类型**：自由型（不同主体之间可以自由转让客体访问控制表的修改权限）、等级型（用户可以将拥有修改客体访问控制表权限的主体组织成等级型结构，优点是可以选择值得信任的人担任各级领导，从而实现对客体的分级控制，缺点是同时有多个主体有能力修改某一客体的访问权限，位于树型结构顶端的超级用户拥有无上的权限，可以对其他用户拥有的资源进行任意修改和访问。权限的高度集中，客观上放大了系统的安全风险）和宿主型 现有大型商用服务器操 作系统（如AIX、HP-UX、Solaris、Windows Server、Linux Server等）中的访问控制机制均为等级型自主访问控制

强制访问控制：用户和客体资源都被赋予一定的安全级别，用户不能改变自身和客体的安全级别，只有管理员才能够确定用户和组的访问权限，基于**系统权威**（如安全管理员）制定的访问规则来对访问进行控制，如多级安全MLS。 强制访问控制模型基于与每个数据项和每个用户关联的安全性标识。安全性标识被分为若干级别：绝密、机密、秘密、一般。数据的标识称为密级，用户的标识称为许可证级别 **规则**：①当且仅当用户许可证级别大于或等于数据的密级时，该用户才能对该数据进行读操作②当且仅当用户许可证级别小于或等于数据的密级时，该用户才能对该数据进行写操作 这两种规则的共同点在于它们禁止了拥有高级许可证级别的主体更新低密级的数据对象，从而防止了敏感数据的泄露 **主要特征**：①权威制定访问规则，对所有主体及其所控制的客体（进程、文件、段、设备等）实施强制访问控制②系统强制主体服从访问控制策略③用户的程序不能改变他自己及任何其他客体的敏感标记 多级安全策略是最为常见的强制访问控制策略，它基于系统中主体与客体的分级来决定是否允许访问，只有安全管理员能够改变主体和客体的安全级别。多级安全策略指预先定义好用户的可信任级别和资源的安全级别，当用户提出访问请求时，系统对两者进行比较以确定访问是否合法，强制式策略特征是强制规定访问用户允许或者不允许访问资源或执行某种操作。  **4种访问方式**：向下读（主体安全级别高于客体信息资源的安全级别时允许查阅的读操作）向上读（主体安全级别低于客体信息资源的安全级别时允许的读操作）向下写（主体安全级别高于客体信息资源的安全级别时允许执行的动作或是写操作）向上写（主体安全级别低于客体信息资源的安全级别时允许执行的动作或是写操作） 由于MAC通过分级的安全标签实现了信息的单向流通， 因此它一直被军方采用 **缺点**：完整性方面控制不够(比如向上写)；应用领域比较窄。由于强制访问控制的规则制定严格并且缺乏弹性，无法适应于复杂的现实环境

DAC和MAC这两种访问控制模型都存在的不足是**将主体和客体直接绑定在一起**，授权时需要对每对（主体、客体）指定访问许可，这样存在的问题是当主体和客体达到较高的数量级之后，授权工作将非常困难 基于角色的访问控制RBAC：授权给用户的访问权限，通常由用户在一个组织中担当的角色来确定。RBAC中许可被授权给角色，角色被授权给用户，用户不直接与许可关联。RBAC对访问权限的**授权由管理员统一管理**，用户不能自主地将访问权限传给他人 **基本思想**：对系统操作的各种权限不是直接授予具体的用户， 而是在用户集合与权限集合之间建立一个角色集合，每一种角色对应一组相应的权限 **RBAC的核心思想**是将权限与角色联系起来，大大简化了授权管理，具有强大的可操作性和可管理性  **RBAC访问控制策略**属于策略中立型的存取控制模型，既可以实现自主存取控制策略，又可以实现强制存取控制策略 **5个基本静态集合**：用户集包括系统中可以执行操作的用户，是主动的实体；对象集是系统中被动的实体，包含系统需要保护的信息；操作集是定义在对象上的一组操作，对象上的一组操作构成了一个特权；角色则是RBAC模型的核心，通过用户分配(UA)和特权分配(PA)使用户与特权关联起来；会话集：一个运行过程中动态维护的集合 主体：可以对其他实体实施操作的主动实体。通常是系统用户或代理用户行为的进程，也被称为访问的发起者 客体：接受其他实体动作的被动实体。通常是可以识别的系统资源，如文件。一个实体在某一时刻是主体而在另一时刻又可能成为客体，这取决于该实体是动作的执行者还是承受者 用户：试图使用系统的人员。每个用户都有一个唯一的用户标识(UID)，当注册进入系统时，用户要提供其UID，系统进行用户身份认证以确证用户身份 **分类**：普通的用户：其访问操作受到一定限制，由系统管理员分配；特殊的用户：系统管理员，具有最高级别的特权，可以访问任何资源，并具有任何类型的访问操作能力。该用户有以下权限：①可以创建和删除计算机上的用户账户②可以为计算机上的其他的用户账户创建账户密码③可以更改其他用户的账户名、图片、密码和账户类型；作废的用户：曾经有权使用系统，但当前被系统拒绝的用户；作审计的用户：负责整个安全系统范围内的安全控制与资源使用情况的审计 角色：是系统中一组职责和权限的集合，用户承担某种角色时，此角色的属性将取代所有用户属性 权限：在受系统保护的客体上执行某一操作许可，用户对特定的资源进行特定操作的许可称为权限 用户角色分配：为用户分配一定的角色，即建立用户与角色的多对多关系。系统管理员通过为用户分配角色，取消用户的某个角色等操作管理角色分配 角色权限分配：为角色分配一组访问权限，即建立角色与访问权限的多对多关系。这样通过角色把用户与访问权限联系起来。用户具有其所属诸角色的访问权限的总和 会话：一次会话是用户的一次活跃进程，它代表用户与系统进行交互。用户与会话是一对多关系，一个用户可同时打开多个会话，用户是一个静态的概念，而会话是一个动态的概念 活跃角色集：一个会话构成一个用户到多个角色的映射，即会话激活了用户授权角色集的某个子集，使子集成为活跃角色集。ARS决定了本地会话的许可权限集 保护域：一系列权限的集合，描述一个主体在给定时间可能执行的所有操作的集合 授权是指可以授予角色或用户的独立权限， 授权在用户中的应用程序级别强制执行策略。 RBAC用户间的授权关系：依据角色指派关系，运行系统中的用户自身可以对角色进行管理。通常，角色指派的权力都在系统中具有管理责任的用户手中。在增强RBAC中，授权是与安全相关的功能或者命令相关联的文本字符串。授权提供了一种机制，以便为用户授予相应的权限以执行某些特权操作，并对不同类别的用户提供不同的功能级别。 **RBAC授权策略**：授权策略规定何人在何种情况下能访问何种目标，访问控制和授权策略展示了一个机构在信息安全和授权方面的顶层控制 委托策略（规定谁可以将什么权力委托给谁）SOA(信任源)策略（它规定受信任分配角色的SOA，并允许进行角色分配的分散管理。SOA策略明确了哪些SOA是可信的，并限定了SOA委派和分配角色的方式和范围） 角色指派策略、动作策略、用户策略、目标访问策略、角色继承策略 **RBAC的优势**：简化权限管理、灵活表达和实现组织的安全策略、安全性高，该策略可以有效实现最小权限管理 、实用性强

基于属性的访问控制(ABAC)将主体和客体属性作为决策的基本依据，灵活地利用资源访问者所具有的属性决定是否授予其访问权限，能够很好地将策略管理和权限判定分离。同时，由于属性是主体和客体内在固有的，无需手工分配，使得ABAC管理上相对简单，有效解决了具有大规模、强动态性和强隐私性特点的新型计算环境下的细粒度访问控制问题。 ABAC将主体和客体属性作为决策的基本依据，灵活地利用资源访问者所具有的属性决定是否授予其访问权限，能够很好地将策略管理和权限判定分离 ABAC模型：四元组(S，O，P，E)：①S表示主体属性，即主动发起访问请求的所有实体具有的属性②O表示客体属性，即系统中可被访问的资源具有的属性③ P表示权限属性，即对客体资源的各类操作④E表示环境属性，即访问控制过程发生时的环境信息 **ABAC的不足之处**：较强的匿名性，这种匿名性导致用户可能滥用其所拥有的属性带来的权限；新型计算环境中用户和设备的动态特性带来了权限的频繁变动，需要对这些变动实时响应，更改相应的权限，保证系统安全可靠的运行；仅实现了对用户访问过程的控制 基于属性的加密机制ABE实现了对数据机密性的访问控制，其采用非对称密码机制并利用属性作为加解密的关键要素，将属性同密文和用户密钥相结合 **不足之处**：ABE机制中的权限更新问题尤为突出（如何平衡更新粒度及计算资源消耗的权限更新机制）

权限管理基础设施或授权管理基础设施(PMI)是属性证书、属性权威、属性证书库等部件的集合体，用来实现权限和证s书的产生、管理、存储、分发和撤销等 属性权威(AA, attribute authority)，是用来生成并签发属性证书的机构，它负责管理属性证书的整个生命周期 属性证书(AC, attribute certificate) 对于一个实体的权限的表示是由一个进行了数字签名的数据结构来提供的，这种数据结构称为属性证书，由属性权威签发并管理 建立在PKI基础之上的PMI，以向用户和应用程序提供权限管理和授权服务为目标，以资源管理为**核心**PMI主要进行授权管理，证明这个用户有什么权限。PKI主要进行身份鉴别，证明用户身份 **PMI技术的授权管理模式**：PMI使用属性证书表示和容纳权限信息，通过管理证书的生命周期实现对权限生命周期的管理。PMI技术通过数字证书机制来管理用户的授权信息，并将授权管理功能从传统的应用系统中分离出来，以独立服务的方式面向应用系统提供授权管理服务 **PMI模型**：包括三个实体：对象（可以是被保护的资源）、权限声称者（访问者）和权限验证者（对访问动作进行验证和决策，是制定决策的实体） 策略实施点(policy enforcementpoints，PEPs)，是指已经通过接口插件或代理所修改过的应用或服务 策略决策点(policy decisionpoint，PDP)，也叫授权策略服务器，它接收和评价授权请求，根据具体策略作出不同的决策 策略库主要用来存储安全授权策略数据、用户资源信息和PMI所需的相关数据 **属性证书的特点**：属性证书将一个标识和一个角色、权限或者属性绑定（通过数字签名）。和公钥证书一样，属性证书能被分发和存储或缓存在非安全的分布式环境中，不可伪造，防篡改 **属性证书的分发**：推/拉模式 **验证过程** ：①验证用户的身份证书，应用系统验证证书的有效性，包括查看证书是否经过CA的正确签名②根据身份信息获取属性证书③验证属性证书④最后应用程序检查属性证书中的内容，来确定是否允许此用户存取其所需的资源及服务

第五章 信息隐藏技术

信息隐藏是把一个待保护的秘密信息隐藏在另一个称为载体的信息中，起源于古代的隐写术 现代信息隐藏是一种解决媒体信息安全，这里的安全有两方面的含义：一是可公开的媒体信息在版权和使用权上的安全，二是秘密信息在传输和存储中的安全 **信息加密与信息隐藏的区别**：**信息加密**：利用密钥把信息变换成密文，通过公开信道传输。信息加密通过密钥控制信息的使用权，从而隐藏秘密信息的内容，没有密钥就无法恢复明文，但没有隐藏秘密信息存在的事实；**信息隐藏**：把秘密信息隐藏于可以公开的信息中，使攻击者难以知道秘密信息的存在，从而掩盖通信过程中存在秘密信息的事实；其主要目的并不是限制对信息的访问，而是确保宿主信息中隐藏的秘密信息不被改变或消除，从而在必要时提供有效的证明信息 **分类**：按载体类型分类，按密钥分类，按嵌入域分类（可分为空(间)域(或时域)和变换域方法），按检测是否需要原始载体信息参与分类（可分为非盲检测算法和盲检测算法）**按照保护对象分类**：隐写术：目的是在不引起任何怀疑的情况下秘密传送消息，主要需求包括难以检测和大容量；数字水印：它是指嵌在数字产品中的数字信号，目的是进行版权保护、所有权证明、指纹（追踪发布多份拷贝）和完整性保护等，因此，它的性能要求是鲁棒性和不可感知性；数据隐藏和数据嵌入：一般指隐写术，或者指介于隐写术和水印之间的应用；指纹和标签：指水印的特定用途。有关数字产品的创作者和购买者的信息作为水印而嵌入 **技术要求**：透明性或不可感知性（主要指人的感官不可感知）鲁棒性（常用的信号处理操作不应该引起隐藏对象的信息丢失）安全性（指隐藏算法具有较强的抗恶意攻击能力）不可检测性（主要指通过技术手段难于判断）自恢复性（只从留下的片断数据，仍能恢复嵌入信号，而且恢复过程不需要载体信号）嵌入强度（载体中应能隐藏尽可能多的信息，隐藏的信息越多，鲁棒性就越差） 空域或像素域算法：将隐秘信息嵌入到随机选择的取样点的值的最低几位上的最低有效位LSB算法，相当于叠加一个能量微弱的信号，因而在视觉和听觉上很难察觉，可以隐藏较多的信息但对信道干扰及数据操作的鲁棒性差；另一个常用方法是利用像素的统计特征将信息嵌入像素的亮度值中，有较强的鲁棒性。缺陷是嵌入的信息量较低 变换域算法：大部分都基于**离散余弦变换(DCT)**和**离散小波变换(DWT)** 先计算原始图像的离散余弦变换(DCT)，然后将隐秘信息叠加到变换域的系数上（不包括直流分量），这些系数通常为图像的低频分量 **改进**：按照应用条件选择变换域；预编码或变形；有目的地选择某种变换的频域系数序列 这类算法的隐藏和提取隐秘信息的过程复杂，隐藏信息量不能很大，但抗攻击能力强，很适合应用在数字作品版权保护的数字水印技术中 压缩域算法：隐秘信息的检测与提取也可直接在数据的压缩域中进行。也就是在压缩编码算法上加入隐秘信息，而不是在DCT的系数上叠加隐秘信息 NEC算法：首先以密钥为种子来产生伪随机序列，该序列具有高斯分布N(0，1)，密钥一般由作者的标识码和图像的哈希值组成，其次对图像做DCT变换，最后用伪随机高斯序列来调制（叠加）该图像除直流(DC)分量外的1000个最大的系数 具有较强的鲁棒性、安全性、透明性 **隐秘信息应该嵌入原数据中对人感觉最重要的部分** 生理模型算法：利用从视觉模型导出的JND(临界可察觉差)描述来确定在图像的各个部分所能容忍的嵌入隐秘信息的最大强度，从而能避免破坏视觉质量 包括人类视觉系统HVS，人类听觉系统HAS

**数字水印的技术模型**：水印技术主要包括水印嵌入与水印提取两个环节 **数字水印的分类与应用**：鲁棒性水印（指恶意攻击下仍然不能被修改、去除的水印，主要用于版权标识）和脆弱性水印（能够察觉载体信息的细微变化，并可根据被破坏的情况记录产品受到的攻击）->综合版权管理系统（对数字化产品同时实现版权认证、完整性认证和非法复制跟踪的保护功能）可见水印（可见水印就是嵌入的保护标识是可见的，明确标识版权，防止非法使用）和不可见水印（把水印信息完全隐藏起来，目的是为了获得惩罚盗版者的证据）私有水印（检测水印时必须采用原始数据作为参照的水印系统称为私有水印，鉴别非法复制品，有更好的性能）和公有水印（不需要采用原始数据进行检测，任何一个拥有检测软件的使用者都可以鉴别信息产品是否为盗版）对称水印（嵌入与水印的提取互逆）非对称水印（公开水印检测算法和密钥的时候，任何人都可以方便地检测水印，但却无法根据检测算法和密钥去除已嵌入的水印信息）多比特水印和1比特水印 **空域水印**：Patchwork：随机地选取一对像素(ai，bi)，通过对ai加1而同时对bi减1达到隐藏1比特的目的 纹理块编码：通过把图像的一种纹理块复制到该图像中具有相似纹理特性的区域来完成水印的嵌入，恢复时必须计算自相关特性 数字图像签名 量化水印算法 改变图像几何特征的水印算法：基于密度线模型的，伪随机地产生一密度线并用作水印，计算图像中的突变点，如利用边缘检测滤波器，改变这些突变点使得在相邻线内有足够多的点 **DCT域水印**：与空域图像水印相比，DCT域图像水印鲁棒性更强且与常用的图像压缩标准JPEG兼容利用了人类视觉系统的亮度掩蔽、边缘掩蔽及纹理掩蔽特性

**典型数字图像隐写算法**：LSB算法直接用秘密信息来取代图像像素值的最低位来实现秘密信息的传递，其他很多种流行的隐写算法大都是由LSB方法派生出来 **隐藏容量**是隐写技术一个非常重要的指标，它要求在满足视觉不可感知的前提下，尽可能多地隐藏信息。为了提高隐藏容量，很多隐写方法利用人类视觉特性进行自适应嵌入 BPCS算法：充分利用人眼视觉冗余，将图像的多个位平面分块，计算所分子块的复杂度，对于复杂度较高的块，人眼的分辨能力较低，因此可以利用这些变化复杂的块来携带秘密信息 PVD隐藏算法：原理与BPCS基本相同，只是PVD方法不是通过图像分块来确定图像的复杂度，而是根据相邻像素的差异情况来确定图像的复杂程度 JPEG图像隐写算法：修改DCT量化步长来调整载体图像的DCT系数，在调整后的DCT系数上进行秘密信息的嵌入 调色板图像的隐密算法：通过改变调色板中颜色的排列顺序来嵌入秘密信息。 优点是信息隐藏不会改变图像的视觉效果，但嵌入量不会随载体图像尺寸的增大而增大，秘密信息容易被图像处理软件覆盖 **利用索引色图像的像素值来携带秘密信息** **二值图像的信息隐密**：大块图像做微小平行移位，小范围图像做修改，有条件的以空间分辨率换取灰度分辨率，考虑视觉上的不可感知性的实现（即视觉的空间屏蔽效应） **文本文档信息隐密**：利用空格、标点、回车换行等不可显示字符携带信息；利用文档的格式，如行间距、字符间距、字符大小、字符位置等参数携带秘密信息；利用语义；注释标签中夹带秘密信息（针对HTML）

数字指纹是在原产品中嵌入与用户有关的信息，产品提供者（也称发行商）能够根据该信息对非法用户进行跟踪，嵌入的内容对不同购买者是不同的数字指纹是指与用户和某次购买过程有关的信息 数字指纹体制：一是用于向拷贝中嵌入指纹并对带指纹拷贝进行分发的拷贝分发体制；二是实现对非法分发者进行跟踪并审判的跟踪体制 **基本要求**：保真性、鲁棒性、嵌入量、合谋容忍性（在一定的合谋人数下，发行商能够确定出至少一个非法分发者，该人数称为合谋安全尺寸，无论合谋人数的多少（即使超过了上述尺寸），无辜购买者也不能受到指控）、效率 指纹编码方案：在一定假设下，将获得的与用户有关的信息按照一定的规则进行编码，生成具有一定抗攻击能力的码字的过程 指纹跟踪方案：当发行商获得盗版拷贝时，运用一定的解码规则判断出非法分发者的过程  **指纹编码方案的分类**：①从跟踪成功的概率来讲，指纹编码方案可以分为确定性跟踪方案和概率性跟踪方案（主流）②从码字的分布而言，可以分为连续指纹方案和离散指纹方案③ 从码字是否随机来讲，还可以分为随机指纹方案和利用某些特殊的组合结构构造的指纹编码方案 连续指纹编码方案：用户码字中的每一个码元取自一个连续的集合，典型代表是Cox等提出的CKLS方案 CKLS方案：用独立随机的正态采样序列作为要嵌入的水印信息，当用作指纹时，为每个用户选取不同的采样序列，序列间是独立的。这里指纹的取值不限于离散的整数值，而是服从正态分布N(0，1)的随机实数序列X 非对称指纹体制：初始化协议，指纹添加协议，跟踪协议，审判协议 匿名数字指纹：用户在购买拷贝的过程中不会泄露自己的身份信息。但如果用户进行非法分发活动，凭借非法拷贝中的信息，发行商可以识别非法者的身份

第六章 主机系统安全技术

主机系统安全，即保证主机数据存储和处理的保密性、完整性、可用性

**计算机系统的安全**可以划分为硬件安全、操作系统安全、数据库系统安全、应用软件安全以及互联网时代的网络系统安全，关键在于其底层操作系统的安全性 **操作系统安全是主机系统安全的核心，操作系统安全是所有计算机系统安全的基石和关键** 安全操作系统，是在传统操作系统的基础上实现了一定安全技术的操作系统 可信计算机系统评价标准TCSEC **安全要求**：①计算机系统必须实施一种定义清晰明确的安全策略②客体必须与其访问标签相关联，以标明其安全级别③主体在访问客体前必须通过严格的鉴别和认证④审计信息必须单独保存，并由专门人员负责⑤计算机系统必须能够独立评估用以实现上述①～④的软硬件机制本身的安全性⑥实现安全需求的可信机制自身必须受到保护，以避免被篡改或削弱 **TCSEC的4个等级、7个级别**：D1级（所有不满足任何较高安全可信性的系统，D1系统最普通的形式是本地操作系统，如MS-DOS）C类——自主保护类 C1级（自主安全保护）C2（受控存取保护，C1+DAC，Windows 及Unix系统）B类——强制保护类 B1(标签安全保护，C2+MAC，支持多级安全的第一个级别。在该级别下，不允许客体的拥有者改变其存取的许可权限) B2(结构化保护，B1+形式化的安全模型、可信通路机制、最小特权管理以及隐通道的分析和处理等安全特征) B3(安全区域保护，B2+全面的访问控制机制、审计的实时报告机制以及严格的系统结构化设计等安全特征，必须设有安全管理员) A类——验证保护 A1(验证设计，设计必须是经过数学验证的，并且对隐通道也要进行形式化分析)  **C2安全级的关键要求**：①安全登录机制②自主访问控制机制③ 安全审计机制④ 对象重用保护机制（残留信息的处理机制），ITSEC组织的E3级别，其等同于TCSEC的C2级 **Windows系统的安全机制**：C2+B的信任路径功能、B的信任机制管理 Windows 10执行的安全性工作：身份标识和访问控制；信息保护；防恶意软件 安全核：要验证整个操作系统的安全性是十分困难的。所以应该使用操作系统中尽量小的部分来提供整个操作系统的安全性，这就提出了安全核的概念，安全核是系统中与安全性的实现有关的部分，包括引用验证机制、访问控制机制、授权机制和授权的管理机制等 **基于安全核构建安全操作系统的优势**：①一方面能够减轻应用系统的负担，避免出现安全隐患②另一方面，由于对系统的安全进行评估的内容集中在安全内核，它有利于评估的进行，使之可以进行严格的形式化验证 引用验证机制：引用监视器和安全核把授权机制与能够对程序的运行加以控制的系统环境结合在一起，可以对受控共享提供支持 **原则**：必须具有自我保护能力；必须总是处于活跃状态；必须设计得足够小，以便分析和测试 可信计算基(TCB)：一个计算机系统中的保护机制的全体，它们共同负责实施一个安全策略。 **构成**：固件和硬件、与安全策略相关的文件、负责安全管理的人员、安全核、具有特权的进程或命令 **功能**：提供敏感性数据的保密性和完整性，它必须监控操作系统内部的关于进程的活动、执行域交换以及I/O操作这三种基本行为 **安全操作系统的设计方法**：分离法（也称为虚拟机法，利用物理分离、时间分离、密码分离及逻辑分离实现非安全操作系统与硬件的隔离）安全核法（在操作系统内核中加入安全功能或者先设计安全核，然后围绕它设计操作系统）仿真法（将非安全操作系统的内核进行修改使之成为安全核，然后再在安全核和原来的非安全操作系统的用户接口层中间编写一个仿真层）**操作系统安全的主要目标**有：标识用户身份及身份鉴别；按访问控制策略对系统用户的操作进行控制；防止用户和外来入侵者非法存取计算机资源；监督系统运行的安全性和保证系统自身的完整性等 **硬件系统安全机制**：内存保护（确保存储器中的数据能够被合法地访问，访问控制一般可以由硬件来实现）运行域保护（运行域是进程运行的区域。一般操作系统都会包含硬件层、内核层、应用层、用户层等层次，而每个层次又会包含子层，这种分层的设计方法是为了隔离运行域，达到运行域保护的目的，运行域可以看成是一系列的同心圆，最内层的特权最高，最外层的特权最低。）多环结构（最重要的安全概念是：**等级域机制**，环号越低，特权越高，环N对某段具有写操作的权限，那么所有0～N-1环对该段都具有写操作，因此，只要在段描述符中存入具有相应访问模式的最大环号，这样只要三个区域分别用来保存具有写、读、执行访问模式中的最大环号，这三个环号称为**环界**）I/O保护(最简单的访问控制方式是把一个I/O设备看成是一个客体) **软件系统安全机制**：标识与鉴别机制（用名称和标识符；鉴别是对用户身份的真实性进行识别）访问控制（**最小特权**指的是在完成某种操作时授予每个主体（用户或进程）必不可少的特权。它的思想是，系统只给用户执行任务所需的最少的特权，也就是用户所得到的特权仅能完成当前任务）审计机制（对系统中有关安全的活动进行记录、检查及审核，目的就是检测和阻止非法用户对计算机系统的入侵，并显示合法用户的误操作。审计是一种被信任的机制，是TCB的一个部分。审计过程一般是一个独立的过程） **Linux的安全机制**：标识与鉴别机制（Linux使用用户名和用户ID标识用户，使用口令来鉴别用户，UID为“0”是传统上被称为root的特权用户，这样是违反“完全仲裁”和“最小特权”安全原则）安全注意键（是一个键或一组键，保证用户看到真正的登录提示，而非登录模拟器，即保证是真正的登录程序）LKM机制（可加载内核模块，简单地说就是在内核里动态载入代码的能力，由于加载以后的LKM能够不受控制地使用内核的所有功能和内存，所以很容易引起恶意程序作为模块加入内核空间后破坏系统）能力机制（将root拥有的特权分割成一组特权）日志系统（Linux的日志系统是独立于Linux内核的，它是在用户态运行的守护进程，不具备安全性，不能全面表达系统的活动，日志记录的内容和格式不统一，存储效率低，容易被伪造和篡改）防火墙机制（netfilter的网络层数据包过滤框架，定义一套钩子函数）

数据库管理系统安全包括三个方面：**机密性、完整性、可用性** **需求**：防止不适当访问；分级保护；防止推断性攻击；数据库的完整性；数据的操作完整性；数据的语义完整性；审计功能 **基本方法**：用户身份认证；存取控制（确保只授权给有资格的用户访问数据库的权限，以多级强制访问控制为核心的系统安全策略）数据加密；数据加密 外包数据库运行模式带来的最大挑战就是**安全问题**，数据存储在非完全可信的第三方服务器中，要充分考虑来自服务提供者本身的恶意操作，不但要防止来自外部的恶意攻击，而且要充分考虑来自服务提供者本身的恶意操作 **安全机制**：数据库加密技术（加密解密都应在客户端完成）密文数据查询策略（一种是不用解密而直接操作密文数据，应用场合包括数据库的秘密同态加密、数据库的序列加密等；另一种是分步查询，一次查询任务分解为客户端和服务器的多次交互，以得到最优的查询树）数据库隐私保护（一方面是对以明文存储的隐私数据内容的保护；另一方面是对用户查询行为及查询结果的保护。基于推理控制的隐私内容保护；保密信息检索）数据完整性验证（数据库内容及其在网络中的传输具有正确性、一致性与有效性，实现数据完整性的主要措施就是增加攻击者所不能控制的冗余信息）外包数据库版权保护（利用数字水印实现对外包数据库的版权保护） 云存储是基于网络的；其次它是可以配置、按需分配的；同时它是一种虚拟化的存储和数据管理 **安全问题**：身份认证和访问控制问题；数据存储和传输的保密性问题；数据隔离问题；应用安全问题 **安全机制**：云存储平台安全机制（保护整个云存储平台系统自身的安全，密码技术，加固技术）云存储管控安全机制（解决安全管理的问题）云存储应用安全机制（存储加密、备份加密、交换加密、身份认证与访问控制、接口安全、手机安全以及云端数据库）

可信计算：参与计算的组件、操作或过程在任意的条件下是可预测的，并能够抵御病毒和一定程度的物理干扰（ISO/IEC）计算机系统所提供服务的可信赖性是可论证的（IEEE）行为总是以预期的方式，朝着预期的目标（可信计算组织TCG） **技术思路**是通过在硬件平台上引入可信平台模块TPM(一种SOC芯片，它是可信计算平台的信任根)来提高计算机系统的安全性 **基本思想**：首先在计算机系统中建立一个信任根，信任根的可信性由物理安全、技术安全与管理安全共同确保；再建立一条信任链，从信任根开始到硬件平台，到操作系统，再到应用。一级测量认证一级，一级信任一级，把这种信任扩展到整个计算机系统，从而确保整个计算机系统的可信 **信任的获得方法**：直接和间接两种方法

第七章 网络与系统攻击技术

网络与系统攻击是利用网络与系统中存在的漏洞和缺陷实施入侵和破坏。 软件漏洞是软件设计或配置中能被攻击者利用的错误或缺陷 网络攻击是指攻击者利用网络存在的漏洞和安全缺陷对网络系统的硬件、软件及其系统中的数据进行的攻击 **一般流程**：系统调查（通过网络收集目标主机相关信息的过程）系统安全缺陷探测（寻找攻击目标系统内部的安全漏洞）*系统调查和系统安全缺陷探测也称为网络探测* 实施攻击 巩固攻击成果（重点是长期隐蔽潜伏，并完成攻击任务）痕迹清理（留下后门，消除攻击过程的痕迹）

网络探测也称为网络侦察，尽可能多地了解攻击目标安全相关的各方面信息 **步骤**：踩点、扫描和查点 **方法**：用whois通过因特网实施踩点，搜索引擎 网络扫描：扫描来发现目标系统的漏洞（软件或协议的设计瑕疵，软件或协议实现中的弱点，软件或协议本身的瑕疵，系统和网络配置错误） **策略**：一主动式策略（基于网络，包括Ping扫描、端口扫描、操作系统辨识和安全漏洞扫描），另一种是被动式策略（基于主机） 常见的扫描类型：TCP连接扫描、TCP SYN扫描、TCP FIN扫描、TCP ACK扫描、TCP Null扫描、TCP RPC扫描、UDP扫描、ICMP扫描

缓冲区溢出：攻击者通过向目标程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。 **原因**：程序中没有仔细检查用户输入的参数，输入数据覆盖了邻近的缓冲区，有可能覆盖程序的正确返回地址，使程序转而执行攻击者通过缓冲区溢出植入内存中的特殊指令，分段错误 **防范**：通过操作系统控制使接收转入数据的缓冲区不可执行；要求程序员编写正确的代码，包括严格检查数据、不使用存在溢出风险的函数、利用Fault injection等工具进行代码检查等；利用C编译器的边界检查来实现缓冲区的保护，这个方法使得有缓冲区溢出漏洞的进程不能被控制（劫持），但是相对而言代价比较大。

拒绝服务攻击：利用网络协议的缺陷，采用耗尽目标主机的通信、存储或计算资源的方式来迫使目标主机暂停服务甚至导致系统崩溃 **常见的拒绝服务攻击**：SYN泛洪攻击（利用TCP缺陷，发送大量伪造的TCP连接请求，TCP连接无法完成第三步握手）UDP泛洪攻击（利用简单的TCP/IP服务，来传送占满带宽的垃圾数据）Ping泛洪攻击（声称自己的尺寸超过ICMP上限的包，也就是加载的尺寸超过64kB上限时，就会出现内存分配错误，导致TCP/IP堆栈崩溃，致使接收方主机宕机）泪滴攻击（收到含有重叠偏移的伪造分段时将崩溃）Land攻击（源地址和目标地址都被设置成某一个服务器地址。此举将导致接收服务器向它自己的地址发送SYN-ACK消息）Smurf攻击（通过向一个局域网的广播地址发出ICMP回应请求，并将请求的返回地址设为被攻击的目标主机，导致目标主机被大量的应答包淹没） **防范**：主机设置（关闭不必要的服务，限制同时打开的SYN半连接数目，缩短SYN半连接的超时等待时间，补丁）网络设备设置（禁止对主机的非开放服务的访问，限制同时打开的SYN最大连接数，限制特定IP地址的访问，启用防火墙的DoS/DDoS的属性，限制对外开放的服务器的向外访问）路由器的设置（使用扩展访问列表，使用QoS，使用单一地址逆向转发，使用TCP拦截，使用基于内容的访问控制）

僵尸网络是攻击者出于恶意目的，融合传统的恶意软件，如计算机病毒、蠕虫和木马等技术，传播僵尸程序传染大量主机，并通过一对多的命令与控制

信道控制被感染的主机所组成的叠加网络 **结构**：控制者（控制僵尸网络的攻击者）主机（是一个被僵尸程序感染的主机）命令与控制服务器（控制者与僵尸主机通信的平台） **僵尸程序的典型结构**：命令与控制模块（整个僵尸程序的核心，实现了僵尸主机与控制器的交互）传播模块，僵尸主机控制模块，下载与更新模块，信息窃取模块，躲避检测与对抗分析模块 **工作机制**：①感染目标主机，构建僵尸网络②发布命令，控制僵尸程序③展开攻击④攻击善后

第八章 网络与系统安全防护

安全防护是指为保护己方网络和系统正常工作，保护信息数据安全而采取的措施和行动 **主要包括**防火墙技术、入侵检测技术、“蜜罐” 技术、应急响应技术，从广义上看，病毒防护技术、数据加密技术和认证技术也属于安全防护技术

防火墙：防火墙是位于两个(或多个)网络之间执行访问控制的软件和硬件系统，它根据访问控制规则对进出网络的数据流进行过滤 防火墙是一个由软件和硬件组合而成的、起过滤和封锁作用的计算机系统或者网络系统 防火墙的**作用**是隔离风险区域（外部网络）与安全区域（内部网）的连接 **防火墙的特性**：①针对所有的通信，无论是从内部到外部还是从外部到内部的，都必须经过防火墙②只有被授权的通信才能通过防火墙，这些授权将在安全策略中规定③防火墙本身对于渗透攻击必须是免疫的 **常用技术**：服务控制（决定哪些Internet服务可以被访问）方向控制，用户控制，行为控制（控制一个具体的服务怎样被实现） **典型功能**：访问控制功能，内容控制功能，日志功能，集中管理功能，自身安全和可用性，可能还具有流量控制、网络地址转换、虚拟专用网等功能 **局限性**：不能防御不经由防火墙的攻击，不能防范来自内部的威胁，不能防止病毒感染的程序和文件进出内部网，不能防止数据驱动式的攻击 **类型**：从工作原理角度看，可分为网络层防火墙技术和应用层防火墙技术；根据实现防火墙的硬件环境不同，分为基于路由器的防火墙和基于主机系统的防火墙；根据防火墙的功能不同，可将防火墙分为FTP防火墙、Telnet防火墙、E-mail防火墙、病毒防火墙、个人防火墙等各种专用防火墙 包过滤技术：工作在网络层，将IP数据报的各种**包头信息**（源地址、目的地址、源端口、目的端口、协议类型等）与防火墙内的规则进行比较，然后根据过滤规则有选择地阻止或允许数据包通过防火墙 **基本原则**：最小特权原则 **具体实现**：①建立安全策略，写出所允许和禁止的任务，将安全策略转化为一个包过滤规则表②由规则表和数据头内容的匹配情况来执行过滤操作（默认值：丢弃/转发） **优点**：一个过滤器能协助保护整个网络；包过滤用户对用户透明；过滤路由器速度快、效率高；技术通用、廉价、有效；易于安装、使用和维护 **缺点**：安全性较差；日志功能十分有限；无法执行某些安全策略；容易受到利用TCP/IP规定和协议栈漏洞的攻击；做出安全控制决定起作用的只是少数几个因素 很少把这种包过滤技术作为单独的解决方案 代理服务技术：又称应用层网关、应用层防火墙，它工作在OSI模型的应用层，核心是运行于防火墙主机上的代理服务器程序，完全阻隔了网络通信流，能监视和控制应用层通信流，可以达到隐藏内部网结构的作用 **实现**：应用代理服务器（在网络应用层提供授权检查及代理服务功能，既可以隐藏内部IP地址，也可以给单个用户授权）回路级代理服务器（也称一般代理服务器，它适用于多个协议，但不解释应用协议中的命令就建立连接回路）智能代理服务器，邮件转发服务器 **优点**：安全性好，易于配置，能生成各项记录，能过滤数据内容，能为用户提供透明的加密机制，可以方便地与其他安全技术合成 **缺点**：速度较慢，对用户不透明，对于不同服务器代理可能要求不同的服务器，通常要求对客户或者过程进行限制，不能改进底层协议的安全性 状态检测技术：又称动态包过滤技术，使用一个在网关上实行的网络安全策略的软件模块，称为检测引擎，检测引擎将抽取的状态信息动态地保存起来作为以后执行安全策略的参考，检测引擎维护一个动态的状态信息表并对后续的数据包进行检查 **工作原理**：监视和跟踪每一个有效连接的状态，并根据这些信息决定网络数据包是否能通过防火墙 **数据包的类型**：TCP包，UDP包 **特点**：结合了包过滤技术和代理服务技术的特点，克服了包过滤技术和代理服务技术的局限性，缺点是状态检测可能造成网络连接的某种迟滞 自适应代理技术：本质上也属于代理服务技术，但它也结合了动态包过滤（状态检测）技术，结合了代理服务器防火墙的安全性和包过滤防火墙的高速等优点 防火墙的体系结构：屏蔽主机防火墙（单宿堡垒主机）（对来自Internet的通信，只允许发往堡垒主机的IP包通过，对来自网络内部的通信，只允许经过了堡垒主机的IP包通过）屏蔽主机防火墙（双宿堡垒主机）（具有至少两个网络接口，外部网络和内部网络都能与堡垒主机通信，但是不能直接通信）屏蔽子网防火墙（使用了两个包过滤路由器，一个在堡垒主机和Internet之间，称为外部屏蔽路由器；另一个在堡垒主机和内部网络之间，称为内部屏蔽路由器。每一个路由器都被配置为只和堡垒主机交换流量） **防火墙的选用**：首先要明确哪些数据是必须保护的，要注意防火墙自身的安全性，考虑用户的安全策略中的特殊需求（IP地址转换，双重DNS，虚拟专用网络，病毒扫描功能，特殊控制需求） **防火墙技术的发展**：智能化，高速度，分布式并行结构，多功能，专业化

被动防护——防火墙，主动网络安全防御——入侵检测（主动性和实时性） 入侵检测：在计算机网络或计算机系统中的若干关键点收集信息并对收集到的信息进行分析，从而判断网络或系统中是否有违反安全策略的行为和被攻击的迹象 **主要目的**：识别入侵者；识别入侵行为；检测和监视已成功的安全突破；为对抗入侵及时提供重要信息，阻止事件的发生和事态的扩大 入侵就是试图破坏网络及信息系统机密性、完整性和可用性等安全属性的行为 **方式**：未授权的用户访问系统资源；已经授权的用户企图获得更高权限，或者是已经授权的用户滥用所给定的权限等 入侵检测：监测计算机网络和系统、发现违反安全策略事件的过程；对企图入侵、正在进行的入侵或已经发生的入侵行为进行识别的过程；检测对计算机系统的非授权访问；识别针对计算机系统和网络系统、或广义上的信息系统的非法攻击 **过程**：信息收集（从网络或系统的关键点得到原始数据，这里的数据包括原始的网络数据包、系统的审计日志、应用程序日志等原始信息）数据预处理（将其转化为检测器所需要的格式，也包括对冗余信息的去除）数据的检测分析（建立检测器模型，并对输入的数据进行分析以判断入侵行为的发生与否）响应（产生检测报告，通知管理员，断开网络连接，或更改防火墙的配置等积极的防御措施）

**审计记录的方法**：原始审计记录和检测专用的审计记录 **审计记录包含的域**：主体（行为的发起者）动作（主体对一个对象的操作或联合一个对象完成的操作）客体（行为的接收者）异常条件，资源使用，时间戳 **通用入侵检测模型**：事件生成器（它是采集和过滤事件数据的程序或模块）事件分析器（事件分析器是分析事件数据和任何CIDF组件传送给它的各种数据）事件数据库（负责存放各种原始数据或已加工过的数据）响应单元（是针对分析组件所产生的分析结果，根据响应策略采取相应的行为，发出命令响应攻击）目录服务器（用于各组件定位其他组件，以及控制其他组件传递的数据并认证其他组件的使用，以防止入侵检测系统本身受到攻击） **主要功能**：监测并分析用户和系统的活动，核查系统配置与漏洞，识别已知的攻击行为并报警，统计并分析异常行为，对操作系统进行日志管理，并识别违反安全策略的用户活动 **基于检测对象的分类**：基于主机的入侵检测系统HIDS（对象是主机系统和本地用户，**优点**：能确定攻击是否成功，监控更为细致，配置灵活，适应于加密和交换的环境，对网络流量不敏感 **缺点**：无法了解发生在下层协议的入侵活动，只能为单机提供安全防护，使服务器产生额外的开销，可移植性差）基于网络的入侵检测系统NIDS（监听网络中的分组数据包 **优点**：监测速度快，能够检测到HIDS无法检测的入侵，入侵对象不容易销毁证据，实时性强，与操作系统无关  **缺点**：无法采集高速网络中的所有数据包，难以检测发生在应用层的攻击，对以加密传输方式进行的入侵无能为力，精确度较差，在交换式网络环境下难以配置，防入侵欺骗的能力较差）混合式入侵检测系统 **基于检测技术的分类**：异常检测（基于行为的检测 **思想**：任何一种入侵行为都能由于其偏离正常或者所期望的系统和用户的活动规律而被检测出来 **优点**：准确率高，能够发现新的未知漏洞的行为，较少依赖于特定的操作系统环境 **缺点**：有误报产生，实现上有一定的难度）误用检测（特征检测，建立在对过去各种已知网络入侵方法和系统缺陷知识的积累之上 **优点**：检测效率高，检测精度高，可以依据检测到的不同攻击类型采取不同的措施 **缺点**：对具体系统依赖性太强，可移植性较差，维护工作量大，同时无法检测到未知的攻击）**基于工作方式的分类**：离线检测系统（非实时工作）在线检测系统（实时联机的检测）分布式入侵检测系统：各个模块分布在网络中不同的计算机设备上，分布性主要体现在数据收集模块上，分布式入侵检测系统根据各组件间的关系还可细分为层次式DIDS和协作式DIDS **典型的分布式入侵检测系统结构**：主机代理模块：审计收集模块作为后台进程运行在监测系统上。 它的作用是收集有关主机安全事件的数据，并将这些数据传至中心管理员；局域网监视代理模块：其运作方式与主机代理模块相同。 但它还分析局域网的流量， 将结果报告给中心管理员；中心管理员模块：接收局域网监视模块和主机代理模块送来的报告， 分析报告，并对其进行综合处理用以判断是否存在入侵 层次式DIDS：定义了若干个分等级的监测区域每一级IDS只负责所监测区域的数据分析，然后将结果传送给上一级IDS 协作式DIDS将中央检测服务器的任务分配给若干个互相合作的基于主机的IDS，这些IDS不分等级，各司其职 **入侵检测系统问题**：高速网络下的误报率和漏报率，入侵检测产品和其他网络安全产品结合的问题，入侵检测系统的功能相对单一，入侵检测系统本身存在的问题 **入侵检测的研究重点**：分布式入侵检测，智能入侵检测，高效的模式匹配算法，基于协议分析的入侵检测，与操作系统的结合，入侵检测系统之间以及入侵检测系统和其他安全组件之间的互动性研究，入侵检测系统自身安全性的研究，入侵检测系统的标准化

蜜罐是防御方为了改变网络攻防博弈不对称局面而引入的一种主动防御技术，本质上是一种没有任何产品价值的安全资源，其价值体现在被探测、攻击或者攻陷的时候。蜜罐技术是一种对攻击方进行欺骗的技术 蜜网又可称为诱捕网络，是由若干个能收集和交换信息的蜜罐构成的一个网络体系架构，融入了数据捕获、数据分析和数据控制等元素，使得安全研究人员能够方便地追踪入侵到各个蜜罐中的攻击者并对他们的攻击行为进行控制和分析，了解网络系统的安全威胁。 **分类**：按系统功能分类（产品型蜜罐和研究型蜜罐）按系统交互活动级别分类（低交互蜜罐与高交互蜜罐）按服务实现方式分类（真实蜜罐和虚拟蜜罐）按服务提供方式分类（服务端蜜罐和客户端蜜罐） **技术机制**：欺骗环境构建机制，威胁数据捕获机制，威胁数据分析机制 (核心)，安全风险控制机制，配置与管理机制，反蜜罐技术的对抗机制 （辅助）

安全防护技术不能保证系统100%的安全 应急响应就是对国内外发生的有关计算机安全的事件进行实时响应与分析，提出解决方案和应急对策，保证计算机信息系统和网络免遭破坏 计算机安全应急响应组(CSIRT) **计算机安全事件**：试图获得对系统或其数据的未授权访问；意外的破坏或者拒绝服务；未授权地使用系统或者存储数据；在所有者不知情、未指示或不同意情况下，改变系统硬件、固件和软件特征 **CSIRT的类型**：内部CSIRT，国家CSIRT，协调中心CC，分析中心AC，卖方团队，应急响应提供商 **应急响应策略**：全局策略，服务特定策略，基础策略 **处理流程**：安全事件的热线响应（检查入侵来源，恢复系统正常工作，事故分析，发布安全警报、安全公告、安全建议，咨询，风险评估，安全教育培训，协助其他组织成立自己的CSIRT，建立网络应急与救援队伍）应急响应阶段（准备阶段，检测阶段，抑制阶段，根除阶段，恢复阶段，报告和追踪阶段） **应急响应技术**：漏洞检测技术、监听技术、日志分析技术、路由控制技术、反向追踪技术等 **应急响应工具**：支持CSIRT日常运作的工具，支持事件调查的工具

第九章 安全审计与责任认定技术

审计：记录和分析用户使用信息系统过程中的相关事件，本质上是一种为事后观察、分析提供支持的机制 安全审计：对系统安全的审核、稽查与计算 **主要作用**：为事后处理提供重要依据，为网络犯罪行为及泄密行为提供取证基础，事后分析及追查取证 **主要功能**：安全审计自动响应；安全审计数据生成；安全审计分析（用于入侵检测或对安全违规的自动响应）；安全审计浏览；安全审计事件存储；安全审计事件选择 **审计系统的结构**：集中式结构（**问题**：存在单点失效、可扩展性有限、难以重新配置、增加功能困难，自适应能力差）分布式结构：主机代理模块，局域网监视器代理模块，中央管理者模块 **工作过程**：主机代理模块截获审计收集系统生成的审计记录进行检查，局域网监视器代理审计主机与主机之间的连接以及使用的服务和通信量的大小，查出显著的事件；中央管理者模块接收包括来自局域网监视器和主机代理的数据和报告，控制整个系统的通信信息，对接收到的数据进行分析 **优点**：扩展能力强，容错能力强，兼容性强，适应性强 **问题**：需要处理不同的格式以实现不同节点间互操作；通信存在保证这些数据完整性和机密性的需求；分析中心设置 网络安全审计系统的数据采集的**完整性**和**准确性**是其后续分析和处理的基础 **基于主机的数据源**：操作系统日志（**首选数据源（可信，易于匹配）**，由三个元素来描述，主体、客体和行为，三个方面收集系统事件：操作系统事件、安全事件和应用程序事件）系统日志（安全性较差，作为应用程序运行，容易遭到破坏，系统日志通常以文本方式保存，且保存的目录一般也未受到保护）应用日志，基于目标的信息（面向目标的安全审计，最常见技术是完整性校验） **基于网络的数据源** **原理**：网络数据的获取（必须利用网络适配器的混杂模式，接收本网段内传输的所有数据帧） **优势**：对受保护系统的性能影响很小，无须改动原先的系统和网络结构；降低了嗅探器本身遭受入侵者攻击的可能性；更容易检测到某些基于网络协议的攻击方法；与受保护主机的操作系统无关 **其他途径的数据源**：设备产生的活动日志，带外数据源（通过人为的、非系统的方式获得的信息）

数字取证：应用计算机、通信等相关技术，发现、收集、检查、分析数据，同时保护信息的完整性，并维持严格的数据保管链 **直接目的**：得到说明或验证某个事件的证据 **作用**：就是通过调查可疑的计算机和网络系统，收集和保存证据，重建事件，评估事件的状态，获得证据，从而进行犯罪调查或者响应一个计算机安全紧急事件; 获得证据，打击违法犯罪；排除故障；日志监控；数据恢复；数据提取；完善策略 **分类**：主机取证和网络取证；事后取证和实时取证；司法取证和非司法取证 **数据媒介**：标准的计算机系统；网络设备；外部设备；存储设备；消费电子产品 **电子证据根本属性**：可接受性；完整性（真实性；可靠性） **电子证据的特点**：数字性；技术性；脆弱性（数据的修改可以在瞬间完成）；多态性；人机交互性（有不同计算机操作人员的参与，会对电子证据施加不同的影响）；复合性（电子证据是多种形式证据的集合） **原则**：及时性原则，取证过程合法性原则，多备份原则，环境安全原则，严格管理过程的原则 **过程**：收集（就是辨认、标志、记录、集中与具体事件相关的数据，并保护数据的完整性）检查（利用合适的取证技术和工具从收集来的数据中发现和提取相关信息，同样也要保证数据的完整性）分析（根据特定问题和需求对检查阶段得到的数据进行进一步的调查）报告（根据分析结果，描述某个事件如何发生，决定还要采取何种行动，提出改进安全策略、安全指南、实施步骤和取证工具的建议，以及完成取证过程的其他任务） **证据信息类别**：来自文件的数据，来自操作系统的数据，来自网络的数据，来自应用软件的数据等 来自文件的数据取证技术：**目标**：删除的文件，松弛空间，空闲区 在收集数据时，通常要产生文件或系统的多个副本：主拷贝和工作拷贝，取证工作应该在工作拷贝上进行。 **收集文件步骤**：复制文件：从媒介复制文件（逻辑备份，不能复制删除的文件或空闲区的残余数据；比特流映像，复制整盘的内容；e.g. linux dd;执行逻辑备份时，要注意在复制过程中文件会变化， 而且被一个进程打开的文件不容易复制）数据文件完整性检查（使用hash）文件的MAC属性保护（文件的三个时间戳，也称MAC times，记录最后修改时间、最后访问时间、最后状态改变时间，必须妥善保护好时间属性）其他技术问题（数据恢复，隐含数据的修复，RAID阵列数据的收集，关于数据编码和解码） **检查数据文件**：定位文件（工具和技术可以帮助自动完成这个定位过程），提取数据（首先必须知道文件的类型，通过扩展名来识别，更精确的方法是查看文件的头部信息）使用取证工具进行检测（文件查看，解压缩文件，目录结构的图形化显示，识别已知文件，执行串搜索和模式匹配，访问元数据） **操作系统的数据取证技术**：收集操作系统数据（收集易失性数据，收集非易失性数据）检查和分析操作系统数据 **来自网络的数据取证技术**：网络流量数据源（防火墙和路由器，数据包嗅探器和协议分析器，入侵检测系统，远程访问系统，安全事件管理(SEM)软件）收集网络流量数据，检查和分析网络流量数据（发现相关的事件，发现相关的事件，攻击者的确认） **来自应用软件的数据**：配置和设置，验证，日志，数据，支持文件，应用结构

第十章 Internet安全

OSI安全体系结构：核心内容是保证异构计算机之间远距离交换信息的安全 安全攻击：任何危及企业信息系统安全的活动,降级、瓦解、拒绝、摧毁计算机或计算机网络中的信息资源，或者降级、瓦解、拒绝、摧毁计算机或计算机网络本身的行为 **被动攻击**：信息收集（造成传输信息的内容泄露）流量分析（判断通信的性质） **主动攻击**：伪装（某实体假装成别的实体）重放（将攻击者获得的信息再次发送，从而导致非授权效应）消息修改（攻击者修改合法消息的部分或全部，或者延迟消息的传输以获得非授权作用）拒绝服务（攻击者设法让目标系统停止提供服务或资源访问，从而阻止授权实体对系统的正常使用或管理） 安全服务：加强数据处理系统和信息传输的安全性的一种处理过程或通信服务。 其目的在于利用一种或多种安全机制进行反攻击;一种由系统提供的对系统资源进行特殊保护的处理或通信服务 鉴别服务：与保证通信的真实性有关，提供对通信中对等实体和数据来源的鉴别，**涉及到**：在连接的初始化阶段，鉴别服务保证两个实体是可信的；鉴别服务必须保证该连接不受第三方的干扰 **分类**：对等实体鉴别；数据源鉴别 访问控制服务：包括身份认证和权限验证，防止未授权用户非法使用或越权使用系统资源 数据保密性服务：连接保密性；无连接保密性；选择字段保密性；信息流保密性 数据完整性服务：带恢复的连接完整性；不带恢复的连接完整性；选择字段的连接完整性；无连接完整性；选择字段无连接完整性 不可否认服务：具有源点证明的不可否认；具有交付证明的不可否认 安全机制：用来检测、阻止攻击或者从攻击状态恢复到正常状态的过程，或实现该过程的设备 **分类**：在特定的协议层实现；不属于任何的协议层或安全服务 加密机制：对称密钥密码体制，非对称密钥密码体制 数字签名机制：**过程**为对数据单元签名与对验证签过名的数据单元的验证 访问控制机制：**可用以下一种或多种信息类型为基础：**访问控制信息库，鉴别信息，用于证明访问实体或资源的权限的能力和属性，按照安全策略，许可或拒绝访问的安全标号，试图访问的时间，试图访问的路径，访问的持续时间 数据完整性机制：确定单个数据单元完整性（发送实体将数据本身的校验码，接收实体产生一个对应的字段，与所接收到的字段进行比较）对连接型数据传输中数据单元序列完整性的保护 鉴别交换机制：通过互换信息的方式来确认实体身份的机制，实体和通信方式两者都可信时，使用各自不同的通行字可以实现交互鉴别；通信方式不可信时，使用防止重放攻击的握手（单向两次，双向三次）不相信对等实体或通信方式时，使用数字签名或公证机制以实现不可否认服务 通信业务填充机制：对抗通信业务分析 路由选择机制 公证机制：确证两个或多个实体之间数据通信的特征：数据的完整性、源点、终点及收发时间 辅助的安全机制：可信功能，安全标签，事件检测，安全审计跟踪，安全恢复

IPSec协议：将密码技术应用在网络层，提供端对端通信数据的私有性、完整性、真实性和防重放攻击等安全服务 **体系结构**：认证头AH（提供数据的完整性、真实性和防重放攻击等安全服务，但不包括机密性）Internet密钥交换协议IKE（用于动态地认证IPSec参与各方的身份）封装安全载荷协议ESP（除了实现AH所实现的功能外，还可以实现数据的机密性） 安全关联(SA)：发送方和接收方之间的受到密码技术保护的单向关系，由**三个参数**唯一确定（安全参数索引(SPI)，目标IP地址，安全协议标识(处理与SA有关的流量时有两个数据库，即安全关联数据库SAD和安全策略数据库SPD)） **IPSec的工作模式**：传输模式（仅在IP头与数据间附加了AH或ESP域，用于在两台主机之间的端到端通信）隧道模式（IP数据包附加了AH或ESP域之后，整个数据包加安全域被当做一个新IP包的载荷，并拥有一个新的外部IP头，一般用于两个网络之间的通信） AH协议：认证基于消息鉴别码，**组成**：邻接头，载荷长度，保留，安全参数索引SPI，序列号，认证数据ICV ESP协议：提供机密性，数据完整性则由身份验证算法提供，**组成**：安全参数索引SPI，序列号，载荷数据，填充域，填充长度，邻接头，认证数据 ESP与AH的区别：ESP主要是完整性，认证，和数据部分的加密。但是ESP不能针对ip包头。只针对数据部分。AH关注ip包头的完整性，认证，而没有数据部分的加密。ESP支持两种工作模式：传输模式和隧道模式

安全套接层(SSL)协议：为Web通信协议—HTTP协议提供保密和可靠通信 SSL/TLS被设计为运行在TCP协议栈的传输层之上，使得该协议可以被部署在用户级进程中，而不需要对操作系统进行修改 **特性**：保密性，认证性，完整性 SSL分层模型：SSL记录协议，三个高层协议：SSL握手协议、SSL密码修改协议和SSL报警协议 SSL会话：一个客户端和服务器间的关联，会话是通过握手协议创建的，定义了一组密码安全参数，这些密码安全参数可以由多个连接共享 **会话状态参数**：会话标识符，对等实体证书，压缩方法，密码规范，主密码，可恢复性标志 SSL连接：连接表示的是对等网络关系，且连接是短暂的，在一个会话中可以建立多个连接 SSL记录协议：所有的SSL通信，包括握手消息、安全空白记录和应用数据，都使用SSL记录层 SSL修改密码规范协议：只包含一个值为1的单个字节 SSL报警协议：由两个字节组成，第一个字节表示消息出错的严重程度，二个字节包含描述特定报警信息的代码 SSL握手协议：由三个域组成，类型、长度、内容 SSL握手处理过程： TLS协议：类似SSL…

安全电子交易(SET)协议：保证支付信息的机密、支付过程的完整、商户及持卡人的合法身份以及可操作性，已成为事实上的工业标准 **提供的服务**：为交易各方提供安全的信道；通过使用X.509 v3数字证书提供信任；确保私密性  **SET的需求**：提供支付和订购信息的保密性；确保传送数据的完整性；持卡人账号认证；为商家提供认证；安全技术；创建一个不依赖于传输安全机制也不妨碍其使用的协议；在软件和网络提供者之间提供功能设施和互操作性 **特性**：信息保密性；数据完整性；持卡人账号认证；商家认证 **目标**：信息在公共因特网上安全传输；订单信息和个人账号信息隔离；持卡人和商家相互认证 **SET系统构成**：持卡人，商家，清算银行，支付网关，认证机构 **交易流程**：顾客开通账号，顾客申请证书，商家申请证书，顾客进行订购，商家被验证，发送订购和支付信息，商家请求支付认证，商家确认订购，商家提供商品或服务，商家请求付款 双向签名机制：将两个接收者不同的消息连接起来。 **SET支付处理**：购买请求，购买请求验证，支付认可（认可请求消息包括与购买相关的信息，与认可相关的信息，证书）支付获取

第十一章 无线网络安全

**802.11无线网络背景**：在无线局域网中，需要认证技术，以验证节点的身份；无线局域网需要隐私保护机制 **802.11的安全机制**：数据保密和完整性、身份认证 有线等效隐私(WEP)：以为无线局域网提供与有线局域网相同级别的安全保护为目的，用于保护无线局域网中的数据链路层的数据安全。WEP包含以下三个要素：共享密钥K、初始向量(IV)和RC4对称流密码算法 **WEP认证**：开放系统认证（默认，被称为“ 零认证”，认证过程以明文方式进行）共享密钥认证（采用挑战／响应方式） **WEP密钥**：802.11b以手工的方法将密钥输入到每个设备中，允许最多4个密钥存储在每个设备上 **缺陷**：静态共享密钥和IV重用（当加密的数据包个数超过2^24时，IV必然发生重复）CRC-32的漏洞，认证的漏洞（身份认证是单向的，共享密钥认证也容易导致认证伪造，挑战文本是以明文方式发送，容易根据RC4(IV，K)=C⊕ P恢复出密钥序列）WEP协议本身没有抗重放保护机制 802.11i关注无线接入点(AP)和无线工作站点(STA)之间的安全通信，引入了健壮安全网络RSN的概念，定义了以下安全服务：认证，访问控制，带消息完整性的机密性 **802.11i强安全网络操作的5个阶段**：发现，认证，密钥管理，安全通信，连接终止 **802.11i支持的安全协议**：加强的加密算法CCMP或TKIP，其中必须实现基于AES的CCMP；动态的会话密钥；具有密钥管理算法；基于802.1x的、无线接入点和无线工作站点的；双向增强认证机制；支持快速漫游和预认证；支持独立基本服务集 TKIP协议：一种对传统设备上的WEP算法进行加强的协议，目的是在不更新硬件设备的情况下，提升系统的安全性，将密钥的长度由40位增加到128位，初始化向量的长度由24位增加到48位，解决了WEP密钥长度太短的问题 新机制：每包一密钥，消息完整性校验码；具有序列功能的初始化向量IV；密钥生成及定期更新功能 **优点**：WEP缺少防止消息伪造和其他主动攻击的机制，TKIP可以有效抵抗这类攻击；使用两个阶段的混合加密函数计算得到WEP seed，可以有效地抵抗重放攻击，使密钥更安全；使用TSC，抵抗重放攻击 TKIP只是一种过渡算法 CCMP基于AES算法和CCM模式，由两个部分组成：加密模式，密码块链式消息认证码 能解决WEP中出现的所有问题 **802.11i中的认证、授权和接入控制主要是由三个部分配合完成的，分别是802.1x标准、EAP协议和RADIUS协议** 802.1x认证协议**包含**三个实体：请求者，认证者，认证服务器 认证过程：STA向它的AP发送一个请求以连接到AS。AP识别这个请求并给AS发送一个访问请求；EAP交换，STA和AS相互授权；安全密钥分发 EAP协议：EAP-TLS是一种基于TLS的认证方式 RADIUS协议：一个应用普遍的AAA协议，最初为拨号网络设计，基于IP网络 **802.11i密钥层次**：密钥层次PMK——对等临时密钥PTK——密钥确认密钥KCK/密钥加密密钥KEK/临时加密密钥TEK——AES加密密钥 **802.11i四步握手**：目的在于由STA和AP共 AP享的PMK推导单播通信密钥PTK **802.11i组密钥更新：向STA发送新组密钥GTK** 强安全网络连接RSNA：**包含**三个实体：申请者(STA)、认证者(AP)和认证服务器 **建立过程**：网络和安全能力发现；802.11认证和连接；EAP/802.1x/RADIUS认证；四步握手；组密钥握手；

移动互联网包括了：无线移动通信网络，公众互联网，移动通信终端 **移动通信系统需求**：对用户进行认证，防止未注册用户的欺骗性接入；对无线路径加密，以防止第三方窃听；移动通信系统还应能提供用户身份保护，防止用户位置泄露 GSM(2G)**安全机制**：用国际移动用户识别码IMSI唯一标识，并由网络统一分配用户认证密钥Ki。IMSI和Ki一起构成了网络籍以鉴别用户的重要“身份证件” **GSM认证方案**：采用了单钥体制，其认证协议为典型的“问—答”机制，并只对用户进行单向认证 **GSM加密算法**：A5 **GSM密钥长度**：64bit，一般认为，普通蜂窝电话的内容受保护的时间应该在星期这个数量级上，因此在现阶段A5算法应该还是能胜任的  **GSM安全服务**：用户身份认证；用户身份保密；用户数据保密以及信令数据保密 通用分组无线业务GPRS/2.5G**安全机制**：身份认证；信令数据和用户数据加密；身份保密（国际移动用户标识码(IMSI)应尽量少用，而以临时逻辑链路标识(TLLI)代替。TLLI与路由区域标识(RAI)一起使用，可以唯一确定用户）SIM卡的使用（SIM卡实质上是一个智能卡，卡中实现了A3、A8和GEA算法，与安全相关的运算都在SIM卡中进行，以防止密钥的泄露） **安全缺陷**：身份认证问题（认证过程是单向的，可能存在攻击者利用假的SGSN对用户进行欺骗）；信令及数据加密问题（不提供端到端的加密，加密算法GEA密钥长度太短）SIM卡问题（通过监视边信道，攻击者可以在几分钟内获得SIM卡中的密钥信息）其他安全问题（IP网络的所有安全问题在GPRS网络中仍然存在） **在利用GPRS进行安全通信时，不能只依靠GPRS系统本身的安全机制，还应在应用层上加强安全保护** 3G系统**的安全体系**：3GPP(WCDMA), 3GPP2(cdma2000) **3GPP安全体制的总体结构**：网络接入安全（提供安全接入3G服务网的机制并抵御对无线链路的攻击）网络域安全（保证网内信令的安全传送并抵御对有线网络的攻击）用户域安全（主要保证对移动台的安全接入。包括用户与智能卡间的认证，智能卡与终端间的认证及其链路的保护）应用域安全（使用户域与服务提供商的应用程序间能够安全地交换信息）安全特性的可视性及可配置能力（主要指用户能获知安全特性是否在使用以及服务提供商提供的服务是否需要以安全服务为基础） **4G 安全架构与 3G 安全架构的不同之处**：加强了网络接入安全，通过强制要求双向认证彻底杜绝伪基站；加强了网络域安全，通过取消电路域彻底杜绝了运营商假冒的问题 **4G缺点**：存在拜访域欺骗归属域的风险；空口业务防护仍然只提供可选的机密性保护，业务数据仍然容易被篡改 **4G/5G安全机制**：身份认证; 用户隐私保护；空口业务防护；网络域安全 **5G 安全架构与 4G 安全架构的不同之处**：加强了网络接入安全，增加了非 3GPP 接入，同时增强了AKA协议，堵上了拜访域欺骗归属域的漏洞；面向垂直行业需求，新增了二次认证，在满足垂直行业差异化需求的同时增强了安全性；新增了SBA域的安全，考虑了服务化网元的安全交互；应用域安全，新增了空口可选的完整性保护手段 5G 面向垂直行业应用的安全不足：接入认证；隐私保护；签约信息；业务防护 6G的安全需求：面向接入认证高效性需求；面向业务加密高效性需求；面向行业应用开放性需求 安全架构需要具备融合性、 内生性和自适应性的特点

第十二章 恶意代码攻击

恶意代码：定义一：恶意代码是任何的程序或可执行代码，其目的是在用户未授权的情况下更改或控制计算机及网络系统；定义二：恶意代码又称恶意软件。这些软件也可称为广告软件、间谍软件、恶意共享软件。是指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行、侵犯用户合法权益的软件；定义三：恶意代码是指故意编制或设置的、对网络或系统会产生威胁(或潜在威胁)的计算机代码  **分类**：代码是否独立，可以将其分成独立的和寄生的恶意代码；根据其是否能自我复制(自动传染)，可以将其分成广义病毒及普通的恶意代码 自我复制过程就是将自身嵌入宿主程序的过程，这个过程也称为感染宿主程序的过程 狭义病毒指同时具有寄生和传染能力的恶意代码 后门：也被称为陷阱，它是某个正常程序的秘密入口，通过该入口启动程序，可以绕过正常的访问控制过程 逻辑炸弹：包含在正常应用程序中的一段恶意代码，当某种条件出现，如到达某个特定日期、增加或删除某个特定文件等，将触发这一段恶意代码 间谍软件：有些商业软件产品在安装到用户机器上的时候，未经用户授权就通过Internet让用户方软件与开发商软件进行通信，这部分通信软件就叫做谍件 特洛伊木马：包含在正常应用程序中的一段恶意代码，一旦执行这样的应用程序，将触发恶意代码。木马的功能主要在于削弱系统的安全控制机制，尤其是访问控制机制 远程访问特洛伊RAT是安装在受害者机器上，实现非授权的网络访问的程序。RAT可以伪装成其他程序，迷惑用户下载安装 病毒：狭义病毒，即传统意义上的病毒，指那种既具有自我复制能力（区别于后门，逻辑炸弹），又必须寄生在其他程序(或文件)中的恶意代码 蠕虫：和**狭义病毒的最大不同**在于自我复制过程。病毒的自我复制过程需要人工干预，无论是运行感染病毒的实用程序，还是打开包含宏病毒的电子邮件，都不是由病毒程序自我完成的。蠕虫的传播不需要人工干预也是一种病毒，自我复制过程不需要人工干预，他其实是能完成特定攻击过程的自治软件 僵尸：一种在被入侵者控制的系统上安装的、能对某个特定系统发动攻击的恶意代码，存在符合狭义病毒的定义和蠕虫定义的Zombie P2P系统 RootKit：一种恶意程序，用于获取目标主机root权限之后隐藏攻击者访问痕迹，使得攻击者不被发现，从而能够长期拥有管理员权限 **分类**：用户级RootKit和核心级RootKit **恶意代码攻击流程**：寻找目标；将自身保存在目标之中；触发目标系统中的恶意代码执行；让自身长期存活于目标系统之中 **恶意代码攻击技术**：代码注入技术；缓冲区溢出攻击技术；三线程技术；端口复用技术；端口反向连接技术 **恶意代码生存技术**：反跟踪技术（反静态跟踪技术，反动态跟踪技术）加密、加壳技术；变形技术 **恶意代码长期存在的原因**：利益驱使；系统和应用软件存在漏洞

**病毒的分类**：引导型病毒（主要感染计算机系统的引导部分）文件型病毒，混合型病毒（既能感染引导区，又能感染文件的病毒）变形病毒（病毒传染到目标后，病毒自身代码和结构会发生变化）脚本病毒，宏病毒（感染办公自动化程序编制的文档） **脚本病毒和宏病毒保存在文档中，而文档是允许经常被修改的，前四类病毒因为要改变可执行文件或引导区的内容，而正常程序一般是不会修改另一个可执行程序的，所以较难查杀脚本病毒和宏病毒** **病毒的特性**：感染性（病毒具有把自身的拷贝放入其他程序(或文档)的特性这是计算机病毒最根本的属性）非授权性，潜伏性（隐蔽自己、使人难以发现），可触发性，破坏性（破坏文件或数据，扰乱系统正常工作，早期的计算机病毒以删除文件、格式化磁盘、破坏分区表等极端的恶意攻击为主，最终目的是获取经济利益） **病毒的结构**：引导模块（将病毒代码引导到内存中的适当位置，其次调用感染模块进行感染，然后根据触发模块的返回值决定是调用病毒的破坏模块还是执行正常的程序）感染模块（负责完成病毒的感染功能，这是病毒最核心、最关键的代码）触发模块（对预先设定的条件进行判断，如果满足则返回真值，否则返回假值）破坏模块（完成具体的破坏作用，其破坏形式和表象由病毒编写者的目的决定）

U盘病毒也称AutoRun病毒，通过U盘的AutoRun.inf文件利用“Windows自动播放”的特性进行传播 PE病毒：步骤：判断目标文件是否为PE文件，是否感染，插入病毒代码，更改入口指针，更改PE头

网络蠕虫**实现机理**：侦察模块（向可能的攻击目标发送扫描数据报，探测有用信息）攻击模块（在非授权情形下侵入系统、获取系统信息，必要时可在被入侵系统上提升自己的权限。其内容包括标准的远程攻击，如缓冲区溢出、利用cgi-bin错误、木马植入等。分为两个部分：一部分执行感染主机的任务，一部分在被感染的主机上运行）通信模块（用于实现与蠕虫制作者及其它蠕虫之间的信息交互）命令接口模块（通过该命令接口我们可以采用手工方式控制传播出去的某些蠕虫，进而可以控制受害主机）数据库支持（蠕虫将自身的一些信息存入数据库中，以方便攻击者进行管理）**蠕虫的传播**：利用系统漏洞主动传播；利用电子邮件系统传播；通过局域网传播；通过即时工具传播；多种方式组合传播 经典蠕虫：莫里斯蠕虫、雷曼蠕虫、CodeRed蠕虫、Nimda蠕虫、冲击波、震荡波

木马目标：是在用户毫不知情的情况下远程控制目标系统, 不会自我繁殖， 也并不“刻意” 地去感染其他文件， 属于一种独立的恶意代码 **特洛伊木马**：服务端（服务器部分）和客户端（控制器部分）。植入对方电脑的是服务端，而黑客正是利用客户端进入运行了服务端的电脑 采用反弹端口的形式，内网到外网的连接是不会被防火墙封堵 木马的最关键特性是隐蔽性 **隐藏和伪装方法**：绑定到程序中，隐藏在配置文件或注册表中，伪装在普通文件中

恶意代码检测与分析系统：技术模块（搜集、提取代码的静态结构、表现出有恶意的行为与与操作系统的交互行为）分析模块 **恶意代码静态分析方法**：基于特征码检测（误报率低，容易实现，漏报率都非常高，工作量大，滞后性，特征库的维护困难，过多的特征码影响检测效率）基于代码语义检测（准确率很高，花费大量的人力）启发式扫描方法 **恶意代码动态分析方法**：系统监控法，动态跟踪法（基于用户态的行为监测技术，基于内核态的行为监测技术，基于指令模拟器的行为监测技术） **恶意代码分类方法**：基于相似性计算的分类方法，基于数据挖掘的分类方法 **恶意代码的防御**：人是最根本最重要的因素，提高人员的安全防范意识和水平，建立完善的防护系统，对系统要经常性的维护和升级，定期对重要的资料进行备份，正确处理受到恶意活动代码攻击的系统

第十三章 内容安全技术

在信息科技中，“信息”和“内容”的概念是等价的，一般认为，内容更具轮廓性和主观性，而信息更具细节性和客观性，可以认为内容是人们可感知的信息或较高层次的信息，因此多个信息可以对应一个内容。如果压缩程度不是太高，可以认为它们表达的内容是相同的 内容安全就是指内容的复制、传播和流动得到人们预期的控制和监测 **内容对象**：前述内容与信息的细微差别，数字内容，应用层或应用中的数据和消息 **需求**：数字版权侵权及其控制（指影视和音乐）不良内容传播及其控制，敏感内容泄露及其控制（包括保密文件和与知识产权相关的资料等）内容伪造及其控制（人们需要能够核实数字内容的真伪） 主动的内容安全技术：对被监管的内容先进行预处理，在内容中添加验证信息，在以后的监管中，它通过分析所获得内容中添加的验证信息来判断内容的性质，并实施相应的控制 被动内容安全技术不预先处理被监管的内容，它通过分析获得的内容本身判断内容的性质，并实施相应的控制策略 广义内容安全技术指与内容及其应用特性相关的所有信息安全技术 狭义的内容安全技术主要包括广义内容安全技术中涉及内容搜索、过滤和监控的部分

**不良文本过滤主要方法**：基于关键字的过滤方法（早期常用的方法，编制一个不良文本关键字词库，当匹配超过一定阈值之后，系统就认为这篇文本是不良文本 **问题**：很难建立完整的不良文本关键字词库，关键字词有可能在正反两类文本中都频繁出现；不良文本关键字词库的滞后性；不良文本关键字词变形的难识别性）基于分级标签过滤方法（对不同的网页根据内容赋予不同的级别，以实现过滤 **问题**：目前还是一个自愿采用的分级系统；技术上存在着很大的问题；应根据不同年龄有不同的约束内容）基于地址库过滤方法（IP地址过滤，封锁指定网站的IP地址，但粒度太粗，容易被代理绕过；URL过滤，直接定位不良文本在互联网上的具体位置，直接对该网页进行屏蔽，性能差；IP和URL相结合的过滤，对于一个网站下大部分的网页都是不良信息的情况，则采用IP过滤；如果是一个网站下只有极少一部分是不良文本这种情况，则采用URL过滤）基于内容的动态过滤法（使用关键字过滤方法进行不良文本过滤过程中，会有很高的误判率 基于内容的过滤方法主要有：K近邻法，贝叶斯方法，神经网络算法，潜在语义索引法等） 中文分词：将文本中连续的字符串按照一定的算法将其划分为独立的、有实际意义的词 话题发现：报道（包含两个或多个独立陈述某个事件的字句的新闻片段）事件（由某些原因、条件引起，发生在特定时间、地点，涉及某些对象，并可能伴随某些必要结果的一个特例）活动（一个互相关联的事件集，这些事件发生在特定的时间、地点，有共同的焦点或目的）话题（一个核心事件或活动以及与之直接相关的事件或活动） **话题自动发现的流程**：信息采集阶段利用网络爬虫工具，从指定的Internet网站把Web网页等互联网信息资源抓取到计算机本地进行存储；网络文本处理也称预处理，即把互联网网页源码信息进行处理，包含剔除无关字符清洗源码、提取正文和必要的附带信息；文本内容分词是在汉语文本处理，且选择词语作为文档特征表达的特定情况下必要的一个步骤；文本向量化是汇总分词后文本中的词语，将这些词语作为空间向量的维度构建文本表示的多维向量；网络文本聚类采取一定的组织策略调度文本向量参与相似度计算，并建立话题的向量表示方法；话题热度评估综合考虑话题中所有报道的点击数、回帖数、报道频率和时间频率等参数，来评估该话题受到关注的程度

内容安全分级监管 **信息内容分级标准**：包括内容分级的词汇表、分级标记和分级操作方法 **分级信息的发布**：信息的分级标记，对标记信息自身需要采取保护措施，防止标记信息被篡改 **分级信息的使用**：在信息服务提供层面上，主要是针对不同的信息受众群体的需要，对信源提供的信息进行分级过滤和组合；在信息服务使用层面上，主要是根据单个信息受众自身的需要，同时结合有关管理手段的需要对所接收的信息进行分级过滤处理

多媒体内容安全技术：对数字媒体产品进行有效的权利管理和保护，维护数字多媒体的内容安全，保护数字媒体避免未经授权的访问、复制和发行 面临的问题：如何鉴别一个数字媒体作品的创建者；如何确定数字媒体作品创建者的版权声明；如何公证一个数字作品的签名与版权声明；如何控制用户访问数字媒体作品的权限 数字权益管理DRM提供从数字内容的创作者，到发行者，到消费者的整个价值链的权益保护 第一代DRM技术侧重于数字内容的加密、防止未授权的使用，即保证只把内容传递给付费用户，没有实现全面的数字权益管理 第二代DRM管理所有相关的权益，而不是局限于数字内容的访问控制











