第 1 章绪论 **信息**已成为一种重要的**战略资源**,信息技术也成为了衡量国家竞争力的重要标志。**信息**：事物运动的**状态和状态变化**的方式。**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（消息层次）、可用性和可控性（网络层次）等信息安全属性。机密性,完整性,可用性称为信息安全的**三要素**。四大安全属性：机密性,可认证性,不可抵赖,完整性。**机密性**：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，甚至可以保证不暴露保密通信的事实。通常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**：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。**可用性**：当突发事件（故障、攻击等）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，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。技术：访问控制。**保鲜性**：信息必须是在其时效之内的。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机密性等安全属性的能力。**信息安全威胁**：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。信息泄露(保护的信息被泄露或透露给某个非授权的实体(窃听和通信业务流分析))、非授权的篡改(信息内容被非授权地增删改破坏)、拒绝服务、非法使用（非授权访问）、假冒、抵赖、网络与系统攻击(如:缓冲区溢出)、恶意代码、自然灾害、人为失误和故意破坏。（安全威胁分别破坏不同的信息安全属性）安全是相对的，不安全才是绝对的。经济因素和时间因素是判别安全性的重要指标。过时的“成功”和“赔本”的攻击都被认为是无效的。信息安全发展 4 时期:**通信安全时期**：主要标志 1949 年香农《保密通信的信息理论》，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**:《可信计算机评估准则》，俗称橘皮书为标志。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，主要保证动态信息在传输过程中不被窃取，即使窃取了也不能读出正确的信息；还要保证数据在传输过程中不被篡改，让读取信息的人能够看到正确无误的信息。1977 年美国国家标准局(NBS)公布的国家数据加密标准(DES)和 1983 年美国国防部公布的可信计算机系统评估准则标志着解决计算机信息系统保密性问题的研究和应用迈上了历史的新台阶。**网络安全时代**：信息安全问题跨越了时间和空间，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、真实性等其他的原则和目标。防火墙、入侵检测、漏洞扫描、安全评估等技术迅速发展并普及。**信息安全保障时代**：主要标志《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，不仅是关注系统的漏洞，而且是从业务的生命周期着手，对业务流程进行分析，找出流程中的关键控制点，从安全事件出现的前、中、后三个阶段进行安全保障；面向业务的安全保障不是只建立防护屏障，而是建立一个“深度防御体系“，通过更多的技术手段把安全管理与技术防护联系起来，不再是被动保护自己，而是主动防御攻击；面向业务的安全防护已经从被动走向主动，安全保障理念从风险承受模式走向安全保障模式。信息安全阶段也转化为从整体角度考虑其体系建设的信息安全保障时代。**信息安全技术**：⑤**支撑安全技术**：信息安全保障技术框架，信息安全测评与管理技术；④**应用安全技术**：网络与系统攻击技术，网络与系统安全防护与应急响应技术，安全审计与责任认定技术，恶意代码检测与防范技术，内容安全技术；③**基础设施安全技术**：主机系统安全技术，网络系统安全技术；②**安全基础设施技术**：标识与认证技术，授权与访问控制技术；①**核心基础安全技术**：密码技术，信息隐藏技术。**信息安全保障技术框架（IATF）**：定义了对一个系统进行信息安全保障的过程，以及该系统中硬件和软件部件的安全要求，遵循这些要求可以对信息基础设施进行深度防御。其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。/深度防御策略的出现使人们清晰地意识到，实施信息安全保障的难度之所以在持续不断地增大，既源于技术革新带来的挑战，又源于操作和管理方式的调整需求，同时也时刻接受处于不间断增强过程中人类智力的挑战，必须全面考虑人、技术和操作（与管理）这三个要素。/相对于信息安全保障的丰富内涵而言，深度防御策略只是一个思路，由保护网络与基础设施、保护区域边界和外部连接、保护计算环境及支持性基础设施这四个框架域所共同组成的技术细节和渗透其中的众多操作与管理规则才是信息安全保障得以有效实施的基石。信息系统安全工程集中体现了信息安全保障的过程化需求，使信息安全保障呈现一个多维的、多角度的操作场景，将其视为信息安全保障可以遵循的基础方法论。**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。**密码算法**包括分组密码、序列密码、公钥密码、杂凑(哈希)函数、数字签名等，它们在不同的场合分别用于提供机密性、完整性、真实性、可控性和不可否认性，是构建安全信息系统的基本要素。**密码协议**是在消息处理环节采用了密码算法的协议，它们运行在计算机系统、网络或分布式系统中，为安全需求方提供安全的交互操作。**密码分析技术**指在获得一些技术或资源的条件下破解密码算法或密码协议的技术。其中，**资源条件**主要指分析者可能截获了密文、掌握了明文或能够控制和欺骗合法的用户等。密码分析可被密码设计者用于提高密码算法和协议的安全性，也可被恶意的攻击者利用。**标识与认证技术**：标识是指实体的表示，信息系统通过标识可以对应到一个实体。标识的例子在计算机系统中比比皆是，如用户名、用户组名、进程名、主机名等，没有标识就难以对系统进行安全管理。认证技术就是鉴别实体身份的技术。主要包括口令技术、公钥认证技术、在线认证服务技术、生物认证技术与**公钥基础设施(PKI)技术**等，还包括对数据起源的验证。**授权与访问控制技术**：为了使得合法用户正常使用信息系统，需要给已通过认证的用户授予相应的操作权限，这个过程被称为授权。在信息系统中，可授予的权限包括读 / 写文件、运行程序和网络访问等，实施和管理这些权限的技术称为授权技术。常用技术：访问控制技术和授权管理基础设施(PMI)技术。防火墙一般归入网络防护技术。**信息隐藏技术**：信息隐藏是指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。信息隐藏主要包括隐写、数字水印与软硬件中的数据隐藏等，其中水印又分为鲁棒性水印和脆弱性水印。保密通信中，**加密**用来掩盖保密的内容，而**隐写**通过掩盖保密的事实带来附加的安全。**网络与系统攻击技术**：攻击者利用信息系统弱点(漏洞)破坏或非授权地侵入网络和系统的技术（主要包括网络与系统调查（攻击者对网络信息和弱点的搜索与判断）、口令攻击（攻击者试图获得其他人的口令而采取的攻击）、拒绝服务攻击(DoS)（攻击者通过发送大量的服务或操作请求使服务程序出现难以正常运行的情况）、缓冲区溢出攻击（属于针对主机的攻击，它利用了系统堆栈结构，通过在缓冲区写入超过预定长度的数据造成所谓的溢出，破坏了堆栈的缓存数据，使程序的返回地址发生变化））**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，它主要包括防火墙和入侵检测技术。防火墙设置于受保护网络或系统的入口处，起到防御攻击的作用；入侵检测系统(IDS) 一般部署于系统内部，用于检测非授权侵入。“蜜罐”技术，它通过诱使攻击者入侵“蜜罐”系统来搜集、分析潜在的攻击者的信息。网络或系统遭到入侵并遭到破坏时，应急响应技术有助于管理者尽快恢复网络或系统的正常功能并采取一系列必要的应对措施。**安全审计与责任认定技术**：为抵制网络攻击、电子犯罪和数字版权侵权，安全管理部门或执法部门需要相应事件的调查方法与取证手段，这种技术被统称为..。审计系统普遍存在于计算机和网络系统中，它们按照安全策略记录系统出现的各类审计事件，主要包括用户登录、特定操作、系统异常等与系统安全相关的事件。安全审计记录有助于调查与追踪系统中发生的安全事件，为诉讼电子犯罪提供线索和证据，但在系统外发生的事件显然也需要新的调查与取证手段。**数字版权技术**在发现版权侵权后进行盗版调查和追踪。**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，这些安全技术一般被称为…从技术体系上看，主机系统安全技术采纳了大量的标识与认证及授权与访问控制等技术，但也包含自身固有的技术，如获得内存安全、进程安全、账户安全、内核安全、业务数据完整性和事务提交可靠性等技术，并且设计高等级安全的操作系统需要进行形式化论证。可信计算技术主要指在硬件平台上引入安全芯片和相关密码处理来提高终端系统的安全性，将部分或整个计算平台变为可信的计算平台，使用户或系统能够确信发生了所希望的操作。**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，统称为网络系统安全技术。分布式系统跨越地理范围一般较大，因此一般面临着公用网络中安全通信和实体认证等问题。国际标准化组织(ISO)于 20 世纪 80~90 年代推出了网络安全体系的参考模型与系统安全框架，其中描述了安全服务在 ISO 开放系统互连(OSI)参考模型中的位置及其基本组成。OSI 参考模型的影响下，有一些实用化的网络安全技术和系统（多数均已标准化）主要包括提供传输层安全的 SSL/TLS 系统、提供网络层安全的 IPSec 系统及提供应用层安全的安全电子交易 SET 系统。ESP：加密的数据包。**恶意代码检测与防范技术**：在原理上，防范技术需要利用恶意代码的不同特征来检测并阻止其运行，但不同的恶意代码的特征可能差别很大，这往往使特征分析存在困难。僵尸网络，指采用一种或多种恶意代码传播手段，使大量主机感染所谓的僵尸程序，从而在控制者和被感染主机之间形成一对多的控制，控制者可以一对多并隐蔽地执行相同的恶意行为。防范该威胁的关键：阻断僵尸程序的传播。(Mirai 僵尸网络)**内容安全技术**：内容安全技术是指监控数字内容传播的技术，主要包括网络内容的发现和追踪、内容的过滤和多媒体的网络发现等技术，它们综合运用了面向文本和多媒体的模式识别、高速匹配和网络搜索等技术。文献中：**广义**：所有涉及保护或监管内容制作和传播的技术，因此包括各类版权保护和内容认证技术；**狭义**：仅包括与内容监管相关的技术。**信息安全测评技术**：信息安全测评：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，以规范它们的安全特性。信息安全测评技术就是能够系统、客观地验证、测试和评估信息安全产品和信息系统安全性质和程度的技术。目的上一般没有攻击的含义，而在实施上一般有标准可以遵循。**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，已经成为构建信息安全系统的重要环节之一。**1.4 信息安全模型** 也被称为威胁模型或敌手模型，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。当下主要有：Shannon 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；Simmons 面向认证系统：提出了无仲裁认证模型：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。**基于密码学的保密通信系统模型**：（发送方 A 明文 M 加密算法 C=E_ke(M) **公共信道** 接收方 B 解密算法 M=D_kd(C) 明文 M） 密钥 K 包括加密密钥 Ke 和解密密钥 Kd，在**安全信道**传输，攻击者在公共信道攻击：**主动攻击**是指攻击者篡改截获的信息，再发送到接收方。为了抵抗主动攻击，必须有一种机制识别信息的篡改，这就是数字签名技术；**被动攻击**是指对密文进行分析，试图恢复出明文。为了抵抗被动攻击，密码算法必须在计算上是安全的，同时对加密后的信息必须进行重组，以抵抗统计分析。针对一般信息安全系统提出了 Dolev-Yao 威胁模型，它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。重要原则：永远不能低估攻击者的知识和能力。**1.5 信息安全保障技术框架** 《信息保障技术框架》(IATF) 美国国家安全局制定，描述其信息保障的指导性文件，建立 IATF 主要是美国军方需求的推动。信息系统生存力技术研究。IATF 前身:NSF，4.0 在编制中。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。提出这四个框架域，目的就是让人们理解网络安全的不同方面，以全面分析信息系统的安全需求，考虑恰当的安全防御机制。**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。三个主要核心要素：人(管理)、技术、操作。重视安全技术应用的同时，必须加强安全管理。IATF 其他信息安全原则：**保护多个位置**：包括保护网络和基础设施、区域边界、计算环境等。各个方位布置全面的防御机制，将风险减至最低。**分层防御**：攻击者和目标之间部署多层防御机制，每一个这样的机制（包括保护和检测措施）必须对攻击者形成一道屏障。**安全强健性**：不同信息有不同价值，丢其失和破坏有不同影响。对信息系统内每一个信息安全组件设置的安全强健性（即强度和保障），取决于被保护信息的价值以及所遭受的威胁程度。在设计信息安全保障体系时，必须要考虑到信息价值和安全管理成本的平衡。《国家网络空间安全战略》(2016.12.27) 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”。“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。个别国家强化网络威慑战略，加剧网络空间军备竞赛，世界和平受到新的挑战。攻击和防护是网络空间安全的两项核心关键技术，进攻是最好的防守。

第 2 章密码技术 密码学=编码+分析。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（密码破译学）: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。一般 Password≠Key,Pwd(口令)是一串字符，K(密钥)是加密/解密过程中的参数。密码体制(用于加解密，解决网络安全中的机密性\完整性\可用性\可控性\真实性等问题中的一个或几个)可以定义为一个五元组(P, C, K, E, D) P 称为明文空间，C 称为密文空间，K 称为密钥空间，E 和 D 表示加密算法和解密算法的集合。对称密码体制(单钥密码体制/秘密密钥密码体制)，非对称密码体制(公钥密码体制) 安全性:无法唯一确定->无条件安全;代价超出且时间超有效期->计算上安全.密码分析攻击的 4 种类型：唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击(依次增强) 对称密码包括古典密码、分组密码和序列密码。古典密码技术以字符为基本加密单元，充分体现了现代密码学的两大基本思想：置换和代换。置换(栅栏)：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 代换：将明文字母用其他字母、数字或符号替换 Caesar 密码：$C=E(k,P)=(P+k) \bmod 26$ $P=D(k,C)=(C-k) \bmod 26$。对称密码分为流密码和分组密码，流密码(stream cipher)又称序列密码，加密和解密每次只处理数据流的一个符号(如 1 个字符或 1 个比特)古典密码都属于流密码。分组密码(block cipher)又称块密码，它将明文消息划分成若干长度为 m(m>1)的分组（或块)，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 **DES（数据加密标准）已经不安全(密钥的长度和算法本身的安全性)**，受到的最大攻击是它的密钥长度仅有 **56** 比特，三重 DES 是最常用的组合密码技术(破解需要 2^112 次穷举搜索),目前，建议所有的分组加密采用 **AES.RC4**:1.初始化 S:j=0,i=0to255:j=(j+s[i]+k[i])mod256,swap(s[i],s[j]);2.生成密钥流:i,j=0,while(true):i=(i+1) mod256;(j=j+s[i])mod256; swap(s[i],s[j]);t=(s[i]+s[j])mod256;k=s[t]. k:字节，与下一字节异或。传统对称密码体制中:当通信的用户数目比较大时，密钥的产生,存储和分发是一个很大的问题.**公钥密码体制**：将加密密钥和加密密钥公开。任何人都可以加密，但只有掌握解密密钥的用户才能解密。(消息鉴别、数字签名及身份认证)数据加密:对称密码,密钥管理:公钥密码,安全性基于数学上难解的问题。**公钥算法特点**：加密/解密使用不同的密钥；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；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；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。公钥密码体制五条件：产生/加密/解密容易,公钥推私钥/密文推明文不可行。**一个单向函数**，如果给定某些辅助信息（称为陷门信息），就易于求逆，则称这样的单向函数为一个单向陷门函数，公钥密码体制就是将辅助信息(陷门信息)作为私钥而设计的。**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。算法描述：密钥计算方法：①选择两个大素数 p 和 q（典型值为 1024 位）②计算 $n=p\times q$ 和 $z=(p-1)\times(q-1)$③选择一个与 z 互质的数，令其为 d④找到一个 e 使满足 $e\times d=1 \pmod z$⑤公开密钥为 **(e, n)**，私有密钥为 **(d, n)** 加密方法：①明文:比特串,将明文划分成 k 位的块 P (k 是满足 2k<n 的最大整数)。②对每个数据块 P,密文 $C=P^e \pmod n$,对每个密文块 C,明文 $P=C^d \pmod n$。**RSA 缺点**：产生密钥很麻烦；分组长度太大，使运算代价很高。一般来说 RSA 只用于少量数据加密(对称密码)。散列函数（哈希函数）又叫做散列算法，是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。散列函数的安全性：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(输入输出,计算容易,不碰撞)、弱抗碰撞性 目前使用最多的两种散列函数是 MD5(破解)和 SHA(-2 安全)序列函数。保障消息完整性和真实性的重要手段是消息鉴别技术 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。根据鉴别符的生成方式，鉴别函数可以分为三类：基于加密函数/基于消息鉴别码(MAC)/基于散列函数。基于 **Hash** 函数导出消息鉴别码（MAC）的方法成为了主流。MAC 原理：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。数据鉴别算法，也称为 **CBC-MAC**(密文分组链接消息鉴别码)，建立在 DES 之上，是使用最广泛的 MAC 算法之一。**数字签名是手写签名的数字化形式**(完整性/真实性)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。一个数字签名体制是一个五元组(M，A，K，S，V)，其中：M 是所有可能的消息的集合(消息空间)。A:所有可能的签名组成的一个有限集(签名空间)。K 是所有密钥组成的集合(密钥空间).S:签名算法集合.V:验证算法集合,$Verk(m,a)=1$,当且仅当 $a=Sigk(m)$时。**数字签名特征**：可验证性、不可伪造性、不可否认性、数据完整性。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 RSA 数字签名方法要使用一个散列函数 H，散列函数的输入是要签名的消息，输出是定长的散列码。**密码系统的安全性就完全取决于密钥的保密程度**。**密钥管理(密钥产生/密钥存储/密钥更新/密钥分发/密钥验证/密钥使用/密钥销毁)的核心问题是**：确保密钥从产生到使用全过程的安全可靠。密钥种类：工作密钥（也叫基本密钥或初始密钥）、会话密钥、密钥加密密钥(二级密钥)、主机主密钥。

第 3 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。根据被认证实体的不同，身份认证包括两种情况：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。**3.1 用户认证** 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，即用户获得访问系统权限的第一步。用户认证的依据主要包括以下三种：**A.所知道的信息**身份证号码、账号密码、口令等/**B.所拥有的物品** IC 卡、USBKey 等/**C.所具有的独一无二的身体特征**指纹、虹膜、声音等。**3.1.1 基于口令的认证** 基于用户名／口令的身份认证是最简单、最易实现、最容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**。静态口令的认证必须解决两个问题：**1)口令存储**。如果口令以明文方式存储，则易受字典攻击。一般系统的口令文件存储的是口令的散列值，即使攻击者得到口令文件，由于散列函数的单向性，也难于得到口令明文。**2)口令传输**。在网络环境中，基于口令的身份认证系统一般采用客户 / 服务器模式，服务器统一管理多个用户账户，用户口令要从客户机传送到服务器上进行验证。为保证传输过程中口令的安全，一般采用双方协商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。②为了便于记忆，用户往往选择简单、容易被猜测的口令，攻击难度大大降低。③口令在网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。⑥口令方案无法抵抗重放攻击。⑦只能进行单向认证，用户无法对系统进行认证，攻击者可能冒充系统骗取口令。**动态口令**是指用户登录系统进行身份认证时，送入认证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（时间）)，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 **1)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。**2)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。用户登录 N 次后，必须重新初始化口令序列。**3)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，结果发送给系统。系统通过计算比对实现认证。**4)时间—事件同步机制**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。动态口令具有以下几个技术特点：①动态性，登录口令是不断变化的。②随机性，口令的产生是随机的。③一次性，每个口令只使用一次。④方便性，用户不需记忆口令。**3.1.2 基于智能卡的认证** 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。基于 USB Key 的身份认证是当前比较流行的智能卡身份认证方式。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。USB Key 具有以下 4 个主要特点。(1)**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，即所谓“双因子认证”(2)**带有安全存储空间**。USB Key 具有 8～128kB 的安全数据存储空间，可以存储数字证书、用户密钥等秘密数据，对该存储空间的读写操作必须通过程序实现，用户无直接读取。其中用户私钥是不可导出的，杜绝了复制用户数字证书或身份信息的可能性。(3)**硬件实现加密算法**。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，从而杜绝了用户密钥被黑客截取的可能性。(4)**便于携带、安全可靠**。非常便于随身携带，并且密钥和证书不可导出；USB Key 的硬件不可复制，更安全可靠。基于 USB Key 的身份认证主要方式(1)基于挑战 / 应答的双因子认证方式先由客户端向服务器发出一个验证请求，服务器接到此请求后生成一个随机数（此为挑战）并通过网络传输给客户端。客户端将收到的随机数通过 USB 接口提供给 USB Key 的计算单元，由计算单元使用该随机数与存储在安全存储空间中的密钥进行运算并得到一个结果（此为应答）作为认证证据传给服务器。与此同时，服务器也用该随机数与存储在服务器数据库中的该客户密钥进行相同运算，如果服务器的运算结果与客户端回传的响应结果相同，则认为客户端是一个合法用户。密钥运算分别在 USB Key 的硬件计算单元和服务器中运行，不出现在客户端内存中,也不在网络上传输，从而保护了用户的安全，也就保护了用户身份的安全。(2)基于数字证书的认证方式 用数字证书进行身份认证,可以实现数据加密。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。以数字证书为核心的加密技术，可以对网络上传输的信息进行加密/解密/数字签名/签名验证,确保网上传递信息的机密性/完整性,以及交易实体身份的真实性,签名信息的不可否认性,从而保障网络应用的安全性。USB Key 可以保证数字证书不被复制,并可以实现所有数字证书的功能。**3.1.3 基于生物特征的认证** 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/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/声音/虹膜/视网膜/脸形/掌纹这几方面的特征进行识别。与传统的身份认证技术相比,基于生物特征的身份认证技术具有以下优点:**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**已有的生物特征识别技术主要有指纹识别/掌纹识别/手形识别/人脸识别/虹膜识别/视网膜识别/声音识别/签名识别等。生物特征信息采集/认证装备的成本较高，只适用于安全级别较高的场所。难于抵抗指纹克隆技术的攻击！**3.2 认证协议** 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）确信对方就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。**3.2.1 单向认证**是指通信双方中，只有一方对另一方进行认证。通常单向认证协议包括三个步骤：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。单向认证既可以采用对称密码技术实现，也可以采用公钥密码技术实现。(密钥分配中心 KDC①IDa,IDb,N1,②E(Ka, [Kab,IDb,N1,E(Kb,[Kab,IDa])]③E(Kb,[Kab,IDa]))**3.2.2 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。为防止假冒和会话密钥的泄露，用户标识和会话密钥这样的重要信息必须以密文的形式传送，这就需要事先已有能用于这一目的的密钥或公钥。因为可能存在消息重放，所以及时性非常重要。在最坏情况下，攻击者可以利用重放攻击威胁会话密钥或者成功地假冒另一方。对付重放攻击的 2 种方法:在每个用于认证交换的消息后附加一个序列号，只有序列号正确的消息才能被接收 但是这种方法存在的问题，它要求每个通信方都要记录其他通信各方最后的序列号。因此，认证和密钥交换一般不用序列号，而是使用下列两种方法之一。时间戳:仅当消息包含时间戳并且在 A 看来这个时间戳与其所认为的当前时间足够接近时，A 才认为收到的消息是新消息，这种方法要求通信各方的时钟应保持同步。挑战/应答:若 A 要接收 B 发来的消息则 A 首先给 B 发送一个临时交互号(挑战),并要求 B 发来的消息(应答)包含该临时交互号。时间戳方法不适合于面向连接的应用.需要某种协议保持通信各方的时钟同步;若通信一方时钟机制出错而使同步失效,攻击成功可能性增大;无法保证各分布时钟精确同步,任何基于时间戳的程序都应有足够长的时限以适应网络延时,同时应有足够短的时限以使攻击的可能性最小。挑战/应答不适合于无连接的应用:它要求在任何无连接传输之前必须先握手，这与无连接的主要特征相违背。KDC(N1:防止攻击方通过消息重放假冒 KDC)**3.3 Kerberos**: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。**设计目的**：解决分布式网络环境下，用户访问网络资源时的安全问题。Kerberos 是为 TCP/IP 网络设计的可信第三方认证协议，利用可信第三方 KDC(密钥分配中心)进行集中的认证。Kerberos 版本 4 被广泛使用，版本 5 改进了版本 4 中的安全性问题。Kerberos 通过提供一个集中的**认证服务器**来负责**用户**对**服务器**的认证和服务器对用户的认证。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。Kerberos 的设计目的是使用户通过用户名和口令登录到工作站，工作站基于口令生成密钥，并使用密钥和 KDC 联系,以代替用户获得远程资源的使用授权。步骤 1.Kerberos 配置 2.服务认证交换:获得会话密钥和 TGT 3.服务授权门票交换:请求访问远程资源 4.客户/服务器认证交换：访问远程资源 Kerberos 版本 5 对版本 4 存在的一些缺陷进行了改进。**1)加密系统依赖性**版本 4 使用 DES,目前(2020 年)DES 已经不安全。版本 5 用加密类型标记密文,使得它可以使用任何加密技术。加密密钥也加上类型和长度标记，允许不同的算法使用相同的密钥。**2)Internet 协议依赖性**版本 4 需要使用 IP 地址,不支持其他地址类型。版本 5 用类型和长度标记网络地址,允许使用任何类型的网络地址。**3)消息字节顺序**版本 4 中,由消息的发送者用标记说明消息的字节顺序，而不遵循已有的惯例。在版本 5 中，所有消息结构遵循抽象语法表示(ASN.1)和基本编码规则(BER)的规定,提供一个明确无二义的字节顺序。**4)门票的生命期**版本 4 中,门票的生命期用一个 8 位表示,每单位代表 5 分钟。最大生命期为 28×5=1280 分钟,约 21 小时。在版本 5 中,门票中包含了精确的起始时间和终止时间，允许门票拥有任意长度的生命期。**5)向前认证**版本 4 中,不允许发给一个客户端的证书被转发到其他主机或被其他用户进行其他相关操作。**6)域间认证**版本 4 中,N 个域的互操作需要 N^2 个 Kerberos-to-Kerberos 关系,版本 5 中支持需要较少连接的方法。**7)冗余加密**版本 4 中,对提供给客户端的门票进行两次加密，**第一次**使用的是目标服务器的密钥,**第二次**使用的是客户端密钥。版本 5 取消了**第二次**加密，即用户门票进行的加密。**8)PCBC 加密**版本 4 加密使用 DES 的非标准模式 PCBC,此种模式已被证明易受攻击密码块攻击。版本 5 提供了精确的完整性检查机制,并能够用标准的 CBC 模式加密。**9)会话密钥**版本 4 中,每张门票中包含一个会话密钥,此门票被多次用来访问同一服务器,可能遭受重放攻击。在版本 5 中，客户端与服务器可以协商一个用于特定连接的子会话密钥,每个子会话密钥仅被使用一次,减少重放攻击的机会。**3.4 PKI 技术** PKI:公钥基础设施，PKI 是一种遵循标准的/利用公钥加密技术的一套安全基础平台的技术和规范。**3.4.1 PKI 体系结构**。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**。PKI 的核心技术围绕建立在公钥密码算法之上的数字证书的申请/颁发/使用与撤销等整个生命周期进行展开，主要目的就是用来安全,便捷,高效地分发公钥,为用户建立一个安全的网络运行环境,保证网络上信息的安全传输。PKI 的系统组成:IETF 的 PKI 小组制订了一系列协议,定义了**基于 X.509 证书的 PKI 模型框架,称为 PKIX**。PKIX 系列协议定义了证书在 Internet 上的使用方式，包括证书的生成,发布,获取,各种密钥产生和分发的机制，以及实现这些协议的轮廓结构。**狭义的 PKI 一般指 PKIX**。一个完整的 PKI 应用系统必须具有五种基本构成部分:**认证机构(CA)**：CA 是 PKI 的核心执行机构,是 PKI 的主要组成部分，称认证中心。CA 是数字证书生成,发放的运行实体,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。目前广泛使用的是 X.509 证书。**密钥备份及恢复系统**：PKI 提供备份与恢复密钥的机制，密钥备份与恢复只能针对解密密钥，签名私钥为确保其唯一性而不能够作备份。**证书作废系统**：作废证书一般通过将证书列入作废证书表(CRL)来完成。CA 负责创建并维护一张及时更新的 CRL 而由用户在验证证书时负责检查该证书是否在 CRL 。**应用接口(API)**: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。**3.4.2 X.509** X.509 证书包含:**(1)版本号**:区分合法证书的不同版本。目前定义了三个版本:版本 1 编号为 0,版本 2 编号 1,版本 3 编号 2。**(2)序列号**:一个整数,和签发该证书的 CA 名称一起唯一标识该证书。**(3)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。**(4)签发者**:创建,签名该证书的 CA 的 X.500 格式名字。**(5)有效期**:包含两个日期:证书的生效日期和终止日期。**(6)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。**(7)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。**(8)签发者唯一标识**:版本 2 和版本 3 中可选的域，用于唯一标识证书中心 CA。**(9)证书主体唯一标识**:版本 2 和版本 3 中可选的域,用于唯一标识证书主体。**(10)扩展**：仅仅出现在版本 3 中，一个或多个扩展域集。**(11)签名**：覆盖证书的所有其他域，以及其他域被 CA 私钥加密后的散列代码，以及签名算法标识。**3.4.3 认证机构** PKI 系统的关键是实现对公钥密码体制中公钥的管理。认证机构 CA 是一个能够提供相关证明的机构。CA 是基于 PKI 进行网上安全活动的关键,主要负责产生,分配并管理参与活动的所有实体所需的数字证书。在 PKI 系统中,CA 管理**公钥的整个生命周期**,其功能包括签发证书,规定证书的有效期限,在证书发布后,还要负责对证书进行撤销、更新和归档等操作。从证书管理的角度,每一个 CA 的功能都是有限的，需要按照上级 CA 的策略，负责具体的用户公钥的签发,生成和发布,以及 CRL 的生成和发布等职能。**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 CRL**。**⑧保存证书、CRL 信息、审计信息和所制定的策略**。**3.4.4 PKIX 相关协议** **1)PKIX 基础协议** PKIX 的基础协议以 RFC2459 和 RFC3280 为核心，定义了 X.509 v3 公钥证书和 X.509 v2 CRL 的格式、数据结构和操作等,用以保证 PKI 基本功能的实现。此外，PKIX 还在 RFC2528、RFC3039、RFC3279 等的基础上定义了基于 X.509 v3 的相关算法和格式等，以加强 X.509 v3 公钥证书和 X.509 v2 CRL 在各应用系统之间的通用性。**2)PKIX 管理协议** PKIX 体系中定义了一系列的操作，它们是在管理协议的支持下进行工作的。管理协议主要完成以下的任务:①用户注册②用户初始化③认证④密钥对的备份和恢复⑤自动的密钥对更新⑥证书撤销请求⑦交叉认证 **3)PKIX 安全服务和权限管理的相关协议** PKIX 中安全服务和权限管理的相关协议主要是进一步完善和扩展 PKI 安全架构的功能,通过 RFC3029,RFC3161,RFC3281 等定义。在 PKIX 中，不可抵赖性通过数字时间戳 DTS 和数据有效性验证服务器 DVCS 实现。在 CA/RA 中使用的 DTS，是对时间信息的数字签名，主要用于确定在某一时间某个文件确实存在或者确定多个文件的时间上的逻辑关系，是实现**不可抵赖性服务的核心**。DVCS 的作用则是验证签名文档、公钥证书或数据存在的有效性，其验证声明称为数据有效性证书。DVCS(是可信第三方)是用来实现不可抵赖性服务的一部分。权限管理通过属性证书来实现。属性证书利用属性和属性值来定义每个证书主体的角色,权限等信息。**3.4.5 PKI 信任模型** 实体 A 信任 B，即 A 假定实体 B 严格地按 A 所期望的那样行动。如果一个实体认为 CA 能够建立并维持一个准确地对公钥属性的绑定，则它信任该 CA。所谓信任模型，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。①层次模型②交叉模型③混合模型④桥 CA 模型⑤信任链模型

第 4 章授权与访问控制技术 **授权和访问控制策略的概念**:给已通过认证的用户授予相应的操作权限，这个过程被称为授权。主要有两种授权技术:**访问控制技术和 PMI 技术**。在信息系统中，资源主要指信息数据、计算处理能力和网络通信资源等。在**访问控制**中，通常将它们称为客体，而“访问”一词可以概括为系统或用户对这些资源的使用，如读取数据,执行程序,占用通信带宽等，这些“访问”通常被称为主体，也常用实体统一指代客体和主体。授权是指资源的所有者或控制者准许别的主体以一定的方式访问某种资源，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**: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(本质上:矩阵)。**主体属性**：用户的级别或种类是主要的主体属性。主体属性还可能包括相关执行程序的性质、所处的网络或物理地址等，它们也可能是授权的依据。在安全性要求更高的情况下，主体的属性还包括其安全状态。客体属性：客体的主要属性是所允许的操作及其信息级别。在安全性要求更高的情况下，客体的属性也可能包括其**安全状态**。**自主访问控制(DAC)**：在自主访问控制中，由**客体的所有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**。一般地，自主访问控制策略是基于主体的身份和授权规则来对访问进行控制的，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(可信计算机评估标准(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。**Linux, UNIX, Windows Server** 有自主访问控制。**自主访问控制概念:也称**“基于主人的访问控制”，自主访问控制实施访问控制，客体的主人(即资源所有者)全权管理有关客体的访问授权，有权泄露、修改该客体的有关信息。**一方面**,访问控制的灵活性很高;**另一方面**,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。**DAC 特点**：访问权限的管理依赖于所有对客体具有访问权限的主体。**DAC 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,不利于实现统一的全局访问控制 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。4.DAC 存在用户滥用职权的问题 5.DAC 分为三个类型(按照访问许可机制不同):**自由型**:任何主体都可以对某一客体进行操作，系统安全性很难得到保障；**等级型**(主体组织成等级结构):同时有多个主体有能力修改某一客体的访问权限,大型商用服务器操作系统位于树型结构顶端的超级用户拥有无上的权限，权限的高度集中**放大了系统的安全风险**；**宿主型**。**完善 DAC**：客体的拥有者应是唯一有权修改客体访问权限的主体，拥有者对其拥有的客体应具有全部控制权，但不允许客体拥有者把该客体的控制权分配给其他主体。从满足等级保护标准的实质上看是**宿主型**。用户需要对客体设置一个**拥有者**，并使其成为**唯一有权访问该客体访问控制表的主体**。**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。**HRU 不足**:当主体和客体发生改变时，需要依赖安全管理员对访问权限的扩散策略进行更新。**TAM**:1.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 2.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。**基于角色特征 DAC 策略**:管理角色包括 OWN_O,PARENT_O 和 PARENTwithGRANT_O。正规角色包括 READ_O,WRITE_O 和 EXECUTE_O。**核心思想：增加角色，实现更细粒度的访问控制**。**时间特征 DAC 策略**：**概念**：使得访问权限具有时间特性。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，实现了更细粒度的访问控制，适合有严格时间要求的系统。**DAC 授权管理**：**1.集中式管理**:单个管理者或组对用户进行访问控制授权或授权撤销 **2.分层式管理**：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用户访问该客体的情况进行授权访问和授权撤销 **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授权给其他用户。**访问控制实现技术**：**1.保护位机制**:常见的实现中其类别包括 Owner,Group,Other 三类,保护位分别指定这三类用户的读写执行权限。保护位与客体相关联，它可决定哪些用户对客体拥有何种访问权限和在需要时撤销权限。访问权的复制和扩展可简单地通过将访问权限的修改权限予某些用户来实现，比如 Linux 系统的文件访问控制机制。**2.能力表机制**:客体访问列表(能力表)与操作系统的主体相关联，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，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。**3.访问控制表**:访问控制表是目前最流行,使用最多的访问控制实现技术。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。这种实现技术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。**4.授权关系表**:对访问矩阵中每一个非空元素的实现技术——授权关系表。授权关系表的每一行就是访问矩阵中的一个非空元素，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**。如果授权关系表按主体排序，查询时就可以得到能力表的效率；如果按客体排序，查询时就可以得到访问控制表的效率。虽然授权关系表需要更多的资源空间，但由于它的访问的高效性，像安全数据库系统这类系统通常采用授权关系表来实现其访问控制机制。**强制访问控制(MAC)**：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。MAC 是一种多级访问控制策略，**特点**:权威制定访问规则，对所有主体及其所控制的客体实施强制访问控制。访问控制是“强加”给访问主体的,即系统强制主体服从访问控制策略,用户的程序不能改变他自己及任何其他客体的敏感标记。**概念**：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级别。**规则**：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。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。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**:权威制定访问规则,对所有用户及其所控制的客体实施强制访问控制,系统强制主体服从访问控制策略,用户的程序不能改变自己及任何其他客体的敏感标记。**策略**：多级安全策略，基于系统中主体与客体的分级来决定是否允许访问。在多级访问控制系统中所有主体和客体都被分配了安全标签，安全标签对其身份与安全等级进行了标识并用来比较。**访问方式**：1.向下读(主体高于客体)2.向上读 3.向下写 4.向上写。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,其中最著名的是 Bell-LaPadula 模型和 Biba 模型。**授权管理**：在强制访问控制中，访问控制完全是根据主体和客体的安全级别决定。主体的安全级别是由**系统安全管理员赋予**用户，而客体的安全级别则由系统根据**创建它们的用户的安全级别**决定。只有安全管理员能够改变主体和客体的安全级别。**MAC 优点不足**：去除了自主访问控制策略中由用户来自由分配的特点，而采用集中控制的方法。**优点**是安全性较高，对特洛伊木马攻击有一定的抵御作用。**不足**:1.完整性方面控制不够(比如向上写)2.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 都将主体和客体直接绑定在一起,授权时需要对每对主客体指定访问许可->达到较高的数量级后授权工作困难。**基于角色的访问控制(RBAC)**：是实施面向企业安全策略的一种有效的访问控制方式。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。**核心思想**：将权限与角色联系起来，通过角色沟通主体和客体。**基本思想**：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。管理员通过指定用户为特定角色来为用户授权，大大简化了授权管理，具有强大的**可操作性和可管理性**。**策略**：RBAC 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。基于角色的访问控制根据对合法的访问者进行角色认证来确定访问者的权限。**核心模型**：**用户集**-用户登录->会话集-角色激活与去活->**角色集**;用户集-用户分配 UA->角色集;**特权集**-特权分配 PA->角色集;特权集包括**操作集**<->**对象集**。**概念**：1.**主体**,可以对其他实体实施操作的主动实体 2.**客体**,接受其他实体动作的被动实体 3.**用户**,试图使用系统的人员,有唯一的用户标识(UID),分为普通用户,特殊用户,作废用户,作审计用户 4.**角色**,是系统中一组职责和权限的集合 5.**权限**,在受系统保护的客体上执行某一操作的许可,是指定的资源进行特定操作的许可称为权限 6.**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 7.**角色权限分配**,为角色分配一组访问权限,建立角色与访问权限的多对多关系 8.**会话**,一次会话是用户的一次活跃进程(一对多关系),它代表用户与系统进行交互 9.**活跃用户集 ARS**,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 10.**保护域**，保护域是一系列权限的集合，描述一个主体在给定时间可能访问的所有操作的集合。**授权管理**：授权是指可以授予角色或者用户的独立权限,授权是在用户和应用程序之间的应用控制**强制执行策略**。授权角色指派:依据角色指派或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，并对不同类型的用户提供不同的功能级别。**特权**在内核中**强制执行安全策略**，授权与特权之间的差别与强制执行安全策略的级别有关。**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。1.委托策略 2.SOA(信任源)策略 3.角色指派策略 4.动作策略 5.用户策略 6.目标访问策略 7.角色继承策略。**RBAC 优势**:1.简化权限管理，RBAC 只需将权限分配给角色,然后将该角色授权给用户 2.灵活表达和实现组织的安全策略 3.安全性高,该策略可以有效实现最小权限管理 4.实用性强。**实例**:1.在线购物系统:淘宝京东 2.在线教育系统:BB 系统。**基于属性的访问控制(ABAC)**：ABAC 有效解决了具有大规模、强动态性和强隐私特点的新型计算环境下的细粒度访问控制问题，为云计算、物联网等新型计算环境提供了理想的访问控制策略。**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。**四元组模型**:S 主体属性 O 客体属性 P 权限属性 E 环境属性。**ABAC 两个阶段**:1.准备阶段:主要负责收集构建访问控制系统所需的属性集合以及对访问控制策略进行描述。2.执行阶段:主要负责对访问请求的响应及对访问策略的更新。**ABAC 不足**:1.在 ABAC 中,用户的身份具有较强的匿名性,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.通过引入身份认证机制保证的可靠性及不可否认性 2.新型计算环境中用户和资源的动态特性带来了权限的频繁变动，需要实时改动。**ABE 概念**：传统的 ABAC 仅实现了对用户访问过程的控制，为了最大限度的保护数据的隐私性和安全性,实现更细粒度的访问控制,提出了基于属性的加密机制。采用**非对称**密码机制并利用属性作为加密密钥的关键要素,将属性同密文和用户密钥相结合。**ABE 也是两个阶段**。**ABE 策略方案:**基于密钥的 KP-ABE 用以描述访问控制策略的访问结构同用户私钥相结合,属性集合同密文相关联,适合付费电视,视频点播;基于密文的 CP-ABE 用以描述访问控制策略的访问结构同访问资源相结合,属性集合同用户私钥相关联适合电子医疗访问,社交网络访问。**ABE 不足**：1. 面临着传统的 ABAC 机制各阶段所面临的问题 2. ABE 机制中的权限更新问题尤为突出 3. 如何**平衡更新粒度及计算资源消耗的权限更新**机制是 ABE 中的重要问题。**PMI 技术**：权限管理基础设施或授权管理基础设施,是属性证书,属性权威,属性证书库等部件的集合体,用来实现权限和证书的产生,管理,存储,分发和撤销等。**AA**:属性权威,用来生成并签发属性证书的机构,负责管理属性证书的整个生命周期;**AC**:属性证书(进行了数字签名的数据结构),对于一个实体的权限的约束。PMI 以资源管理**为核心: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,(PKI:用户是谁;PMI:有什么权限)PMI 需要 PKI 为其提供身份认证。**PKI 和 PMI 的关系：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。**PKI 和 PMI 的关系类似于签证和护照的关系**。**PKI 和 PMI 的术语对比**:PKI 信任源有时被称为根 CA,而 PMI 信任源被称为 SOA。**PMI 授权管理模式**:授权服务体系主要是为网络空间提供用户操作授权的管理，即在虚拟网络空间中的用户角色与最终应用系统中用户的操作权限之间建立一种映射关系。授权服务体系一般需要与信任服务体系协同工作。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**：1.对象 2.权限声明者 3.权限验证者。决定访问成功/失败 4 条件:权限声明者的权限;适当的权限策略;当前环境变量;对象方法的敏感性。**PMI 基础设施的结构和应用模型**：应用系统层面有三项，访问者->**策略实施点 PEPs**->目标。权限管理授权服务平台有四项,属性权威 AA->属性库->**策略决策点 PDP**,策略库->**策略决策点 PDP**。其中两个策略点 PEPs 和 PDP 互联<->。属性证书的签发者被称为属性权威 AA，属性证书存放在属性库中。策略库主要存放着安全授权策略数据、用户资源信息和 PMI 所需的相关数据。**属性证书定义格式**：对于一个实体的权限的绑定是由一个进行了数字签名的数据结构来提供的。包括版本号,持有者,颁发者,签名算法,序列号,有效期,属性,扩展项,签名信息。**属性证书特点**:公钥证书将一个身份标识和公钥绑定,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,属性证书被分发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**:1.推模式,用户将自己的属性证书“推”给资源服务管理器 2.拉模式,属性权威或存储证书的目录服务系统“拉”回属性证书。

第 5 章信息隐藏技术 **一、信息隐藏的概念** **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，非授权者不知道这个普通的载体信息中是否隐藏了其他的信息，而且即使知道也难以提取或去除隐藏的信息。①可公开的媒体信息在版权和使用权上的安全②秘密信息在传输和存储中的安全。**信息加密**:利用密钥把明文信息变换成密文，通过公开信道传输。如果要使用这些受保护的信息,必须用正确的解密密钥,没有密钥的非法用户无法从密文中恢复原始信息,从而无法正确使用信息。换言之:信息加密是通过**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。**信息隐藏技术的分类**：按载体类型分类,有文本,图像,音频和视频的信息隐藏技术。按密钥分类,若嵌入和提取采用相同的密钥,则称为私钥信息隐藏技术,否则称为公钥信息隐藏技术。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(需要原始载体参与)算法和盲检测算法。按照保护对象分类，隐写术,数字水印,数据隐藏和嵌入,指纹和标签。比较活跃的信息隐藏技术主要有两个：**隐写术(主要需求包括难以检测和大容量)**和**数字水印(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,指纹和完整性保护,性能要求是鲁棒性和不可感知性等)**。**成功的信息隐藏通常需要满足的技术要求**：(1)透明性或不可感知性:指载体在隐藏信息前后没有明显的差别,除非使用特殊手段,否则无法感知机密信息的存在(**主要指人的感官不可感知**)(2)鲁棒性:指隐藏的信息能够抵抗各种信号处理操作而带来的信息破坏能力,即常用的信号处理操作不应该引起隐藏的信息丢失。(3)安全性:指隐藏算法有较强的抗恶意攻击能力,此外,与信息加密一样,信息隐藏技术最终也需要把对信息的保护转化为对密钥的保护。(4)不可检测性:指隐藏对象与载体对象需要有一致的特性,以便使隐藏分析者无法判断隐藏对象中是否隐藏有嵌入对象(主要指通过**技术手段**难于判断)(5)**自恢复性**:经过某些操作或变换后,可能会使隐藏对象产生较大的破坏。如果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 (6)嵌入强度(信息量):载体中应能隐藏尽可能多的信息(1,2,6 折衷)。**二、隐藏信息的基本方法** 基于图像载体的信息隐藏**技术的几种典型算法**：(1)空域或像素域算法：最典型的是将隐藏信息通过随机选择的取样点的值的最低几位上的最低有效 **LSB** 算法。在视觉和听觉上很难察觉,但算法对信道干扰及数据操作的抵抗力较差，即鲁棒性较差。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，如 **Patchwork** 算法，有较强的鲁棒性。缺陷是嵌入的信息量较低。(2)变换域（频率域）算法:大部分都基于离散余弦变换(**DCT**)和离散小波变换（**DWT**)。DCT 变换域的基本思想是：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(适合数字水印)。(3)压缩域算法:基于 JPEG,MPEG 标准的压缩域信息隐藏系统不仅节省了大量的完全解码和重新编码过程,而且在数字电视广播及 VOD 中有很大的实用价值。相应地,隐秘信息的检测与提取也可直接在数据的压缩域中进行。也就是说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。(4)**NEC** 算法:信息隐藏算法中,该算法具有较强的鲁棒性,安全性,透明性等。该算法还提出了增强隐秘信息鲁棒性和抗攻击算法的重要原则,即隐秘信息应该嵌入原载体中对人感觉最重要的部分。(5) 生理模型算法：利用视觉模型来确定与图像相关的调制掩模，然后再利用其来嵌入隐秘信息。这一方法可以同时具有好的透明性和强健性。**三、数字水印** 水印技术是将特定的标记（水印）嵌入到某一媒体信息中，以此实现对该媒体信息进行某种程度的保护或标识。水印技术主要包括**水印嵌入**与**水印提取**两个环节。**数字水印模型**：**包括水印嵌入处理,载体传输或传播,水印提取处理**三个模块。在水印嵌入模块中，系统通过密钥的控制将水印信息嵌入原始载体数据中,形成含水印载体信息,水印的嵌入不应影响载体信息的使用价值;在载体传输模块中,载体信息在公用信道中进行传输,这一过程中含水印的载体信息可能受到某种形式的信号处理或恶意攻击,形成处理或攻击后的载体信息,水印提取模块要能够从处理或攻击后的载体中正确地提取水印信息,以作为版权保护或认证的依据。**数字水印的分类与应用**：(1)鲁棒性水印和脆弱性水印。鲁棒性水印是指意在攻击处理下仍然不能被修改,去除的水印,主要用于版权标识。脆弱性水印则是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。结合鲁棒性水印,脆弱性水印和数字指纹等技术所形成的综合版权管理系统可以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。(2)可见水印和不可见水印。所谓可见水印就是嵌入的保护标识是可见的,主要目的在于明确标识版权,防止非法使用。不可见水印则是把水印信息完全隐藏起来,目的是为了获得感到盗版者的证据。(3)私有水印和公有水印。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，而不需要采用原始数据进行检测的系统称为公有水印。通常私有水印有更好的性能，往往能抵御相当强大的攻击。但从应用角度来看，公有水印系统更具优势。(4)对称水印和非对称水印。对称水印的嵌入与水印提取互逆。在水印算法公开的条件下，如果攻击者知晓密钥，就能轻易删除水印，所以目前水印密钥一般是不公开的。非对称水印要求在公开水印检测算法和密钥的同时，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。(5)多比特水印和 1 比特水印。嵌入的水印信号只表示“有水印”或“无水印”两种情况，称为 1 比特水印。而嵌入多比特有意义的信息的水印称为多比特水印。多比特水印更有实际应用价值，但其设计难度将加大。**空域水印**：(1)“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 比特目的。(2)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。(3)数字图像签名(4)量化水印算法(量化索引调制(QIM))。**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(利用人类视觉系统的掩蔽特性)。**四、数字隐写现代隐写的技术模型**：(嵌入处理模块)根据给定的算法和密钥将秘密信息嵌入到图像,音频或视频等数字多媒体信号中,(传输信道模块)使得秘密信息在传输过程中不引起第三方或者信道监督者的怀疑。(提取处理模块)接收方在得到载有秘密信息的数字载体后,可以根据提取算法和同样的密钥恢复秘密信息。秘密信息的提取一般不需要原始载体,这和一些需要载体信息作为参照的数字水印提取方法有所不同。**典型数字图像隐写算法**：(1)LSB 算法:出现较早,通用性较好,其原理几乎可以应用于所有载体。原理:用秘密信息来取代图像载体信息的最低位平面或者最低几位平面。(2)自适应嵌入的隐写算法:基于位平面复杂度分割的隐写算法 **BPCS**,将图像的多个位平面分割,对于分割所分子块的复杂度,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 方法不是直接应用像素块的空间复杂度，而是根据相邻像素的差异情况来确定隐藏的复杂程度(3)流行的 JPEG 图像隐写算法：基于 BMP 格式的 24 位真色彩图像隐写算法虽然具有优良的携密性能,但由于其自身数据量较大,很难适应带宽并不充裕的互联网络通信传输,因此,更具优势的携带性的图像隐写算法往往选择压缩后的媒体信息作为载体,基于最为流行的 JPEG 压缩编码格式的隐写算法就是典型代表(4)调色板图像的隐密算法:1.基于调色板的方法通过改变调色板中颜色的排列顺序来嵌入秘密信息 2.基于像素索引值的方法利用索引色图像的像素值来携带秘密信息(5)二值图像的信息隐密：二值图像是一种只有黑白两种像素的特殊图像格式,对这两个反差极大的色调做直接修改很容易引起视觉异常,典型的 LSB 算法并不适用。因此,针对该类载体信息,必须在信息嵌入时重点考虑视觉上的不易感知性方法（即视觉的空间屏蔽效应）目前①大块图像像素小平行移位②小范围图像像素修改③以空间分辨率换取灰度分辨率(6)文本文档信息隐密：1.利用字格,标点,回车换行等不可显示字符携带信息,这种方法主要针对纯文本载体。2.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，这种方法适用于带有格式定义的文本载体。3.利用语义，通过同义词或近义词替代的方法进行信息隐藏。**五、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)利用数字指纹来对非法用户进行跟踪,嵌入的内容**对不同购买者是不同的**。**数字指纹体制**:由两部分构成,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**。这两部分通常通过发行商、用户之间的一系列协议实现。因此数字指纹体制也可以分为**算法(编码和解码,指纹的嵌入和提取以及拷贝的分发策略等)**和**协议(实体交互等)**两部分。**数字指纹方案通常应满足以下几项基本要求**:(1)保真性:嵌入指纹后的数据拷贝与原始拷贝相对于原拷贝,其质量不应降低。这实际是信息隐藏方案的基本要求(2)**鲁棒性**:嵌入的指纹信息要能够抵抗可能遭受的处理,操作甚至是恶意攻击,使得攻击者不能从拷贝中消除(3)**嵌入量**:因为嵌入的内容要实现用户攻击后留下足够的信息使发行商能够进行跟踪,因此要求有足够的嵌入量(4)**合谋容忍性**:这是对数字指纹的一个关键要求 1.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 2.无论合谋人数的多少都不会有无辜购买者被诬陷(5)**效率**:要求指纹拷贝的生成算法和跟踪算法的实现具有很好的效率。**数字指纹编码**:发行商会对用户的指纹进行编码，以增加指纹方案的合谋容忍能力,这种编码称为合谋容忍编码。若一个数字指纹体制能够抵抗合谋攻击，则称该指纹编码方案是合谋安全的。通常包括两个部分:指纹的**编码算法**(生成带有用户指纹的拷贝)和**跟踪算法**(如何对非法用户进行跟踪)。**指纹编码方案的分类**：(1)从跟踪成功的概率来讲，分为确定性跟踪方案和概率性跟踪方案。(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)从码字是否随机而言,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。**数字指纹协议**:这是指纹体制最主要的特点是实现非法用户的不可否认性。一般由 4 个基本协议组成：(1)初始化协议（用户进行购买登记和发行商的有关初始化工作)(2)指纹添加协议（为用户生成带指纹的拷贝)(3)跟踪协议（确认非法分发者的身份)(4)审判协议（发行商向第三方提供用户有罪的证据)。为了保护购买过程的隐秘性,使用匿名数字指纹。采用这种指纹机制,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 6 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,核心内容包括操作系统安全,应用监管系统,操作系统安全增强系统和运维安全管控系统等。**主机系统安全**包括:硬件(所有实体部件和设备的统称),固件(固化的软件,BIOS 的软件),系统软件的自身安全,以及一系列附加的安全技术和安全管理措施,从而建立一个完整的主机安全保护环境。**操作系统安全**是主机系统安全的核心。数据库系统,应用软件以及网络软件都运行在操作系统之上,要保证它们的安全性,除了依赖自身的安全机制外，**关键在于其底层操作系统的安全性**。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，提供访问控制、最小特权管理和安全审计等功能,采用各种安全策略模型，在系统硬件资源和其存放的数据之上进行符合预定安全策略的调用，限制对系统资源的非法访问和阻止黑客对系统的入侵。可信计算机系统评价标准(TCSEC)于 1983 年由美国国防部发布，是计算机系统安全评价的第一个正式标准。**TCSEC 的 6 个规范性安全要求**:(1)计算机系统必须实施一种定义**清晰明确的安全策略(主客体访问)**(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**可信机制本身必须受到保护**,以避免被篡改或删除。**TCSEC 的 4 个等级、7 个级别**:D(D1:不安全的都是 D1)C:自主保护类(C1:自主安全保护,身份验证，管理员机制。C2：受控存取，覆盖 C1，且具有 DAC 机制和审计机制)B:强制保护类(B1:标签安全保护,覆盖 C2,且具有强制访问控制(MAC)机制,B1 级是**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,覆盖 B1,具有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。B3:安全区域保护,覆盖 B2 具有很强的监视委托管理访问能力和抗干扰能力,**B3 级系统必须设有安全管理员**)A:验证保护(A1:验证设计,覆盖其它所有,显著特征是**设计者必须按照一个正式的设计规范来分析系统，分析后使用核对技术来确保符合设计规范,必须经过数学验证，且对隐通道也要进行形式化分析**)。**ITSEC 和 ISO 15408**:英,法,德,荷提出了评价满足保密性,完整性,可用性要求的信息技术安全评价准则(ITSEC)后，美国又联合以上诸国和加拿大，并会同国际标准化组织（ISO) 共同提出信息技术安全评价的通用准则(CC for ITSEC),CC 已经被技术发达的国家承认为代替 TCSEC 的评价安全信息系统的标准。**中国国家标准**：网络安全等级保护评测 2.0 版本(等保 2.0)，2019 年 5 月发布,是我国网络安全方面的推荐性国家标准.**Windows 及 Unix 系统**的安全级别:C2 级。C2 的关键 4 项要求: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) **Win10 执行的安全性工作**有三大类:(1)身份标识和访问控制(2)信息保护(3)防恶意软件.**操作系统的安全**取决于安全功能在系统中实现的完整性,系统文档的清晰性,系统测试的完善性和形式化验证程度。要验证整个操作系统的安全性是十分困难的,所以应该考虑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**是安全操作系统中最关键部分。它要保证操作系统中所有可能的安全性要求都可以在安全核中实现。**基于安全核的安全操作系统具有两个方面的优势**:①减轻应用系统的负担,避免出现安全隐患;②有利于评估的进行,使之可以进行严格的形式化验证。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。引用监视器的思想是为了解决用户程序的运行控制问题而引入的,其目的是在用户(程序)与系统资源之间实施一种授权访问关系。**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。引用监视器的具体实现称为**引用验证机制**,需要同时满足**(1)必须具有自我保护能力;(2)必须总是处于活跃状态;(3)必须设计得足够小,以便分析和测试**.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。**TCB 在 TCSEC 中的定义**是:一个计算机系统中的保护机制的全体。**可信计算基(TCB)的构成**(1)固件和硬件:包括 CPU,内存,寄存器和 I/O 设备等;(2)负责安全管理的人员:他们一般具有比较大的权限,所以很容易引起系统的安全问题;(4)安全核:它为整个操作系统提供安全机制,是判断一个操作系统是否安全的基础;(5)具有特权的进程或命令。**TCB 的基本功能是提供敏感性数据的保密性和完整性**(监控三种基本行为:操作系统内部的运行,操作系统环境之间的转换以及 I/O 操作)。安全核是 TCB 的一个子集。**安全核在 TCSEC 中的定义**:一个 TCB 中实现引用监视器思想的硬件,固件和软件,它必须保护访问,必须保护自身免受修改,必须能被验证是正确的。

安全操作系统的设计方法一般有三种，如下图所示:

应用程序	应用程序	应用程序	应用程序
非安全操作系统	非安全操作系统		OS 仿真器
	安全核	安全核	安全核
硬件	硬件	硬件	硬件
原系统	分离法(虚拟机法)	安全核法(改进/增强法)	仿真法

分离法(虚拟机法)分离的办法有四种:物理分离,时间分离,密码分离及逻辑分离;智能手机的 Android 系统采用了虚拟机的方法增强系统安全;基于容器的虚拟化方法是计算虚拟化及服务微型化的主流方向之一,如 Docker 容器技术。**操作系统安全的主要目标**包括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。**硬件的安全机制**主要包括:**内存管理**(内存保护,即确保存储器被多个合法用户访问时的安全性),**运行域保护(环界)**和 **I/O 管理**。**软件的安全机制**主要包括:**标识与鉴别机制**(一般可用名称和标识符来标明用户,鉴别是对用户身份的真实性进行识别),**访问控制机制**,**最小特权管理机制**(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(给且仅给),系统只给用户执行任务所需的最少的特权,也就是用户得到的特权仅能完成当前任务),**可信通路机制**,**隐通道的分析与处理**以及**安全审计机制(独立过程)**(对系统中有关安全的活动进行记录,检查及审核,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)等。**Linux 使用**用户名和用户 ID 标识用户,使用口令来鉴别用户。root 违反“完全仲裁”和“最小特权”安全原则。从版本 2.0 开始，Linux 开始支持 LKM 机制，也就是可加载内核模块，简单地说就是在内核里动态载入代码的能力。但是由于加载以后的 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代码对内核实施加入内核空间后破坏系统。**能力机制**是通过一组比特位来实现的，该机制将特权 root 拥有的特权分割成一组特权。从 Linux2.4 开始，实现了一个称为 netfilter 的网络防火墙机制,netfilter 框架为每种网络协议(如 IPv4、IPv6 等)定义一套**钩子函数**,这些钩子函数在数据报流过协议栈的几个关键点被调用。**数据库安全性**:**机密性,完整性,可用性**。确保机密性,完整性,可用性分别指的是防止,检测,阻隔信息的非法泄露,非法篡改,非法破坏和系统的非法访问。**数据库的安全保护需求**:(1)防止不适当访问(2)级保护(3)防止推断性攻击(4)数据库的完整性(5)数据的完整性(逻辑一致)(6)数据的语义完整性(7)审计功能。**保证数据库管理系统安全的基本方法**：(1)用户身份认证;(2)存取控制(确保只授权给有资格的用户访问数据库的权限,同时:以多级强制访问控制为核心的系统安全策略);(3)数据加密;(4)审计追踪与攻击检测。**外包数据库安全**:外包服务把组织自己不擅长的东西(非核心业务)交给专业的外部组织去做,将主要精力集中于核心业务,从而优化资源配置,降低软硬件投资成本,提高组织机能和效率,充分发挥自身核心竞争力并增强自身应变能力。这种外包数据库运行模式带来的最大挑战就是安全问题。由于数据存储在非完全可信的第三方服务器中，因此，外包数据库系统的安全机制不但要防止来自外部的恶意攻击，而且要充分考虑有服务器提供者本身的恶意操作。**外包数据库系统的特定安全机制**:1.数据库加密技术(库外加密);2.密文数据查询策略;3.数据隐私保护;4.数据完整性验证(增加冗余);5.外包数据库版权保护(水印)。**云存储**是指通过集群应用、网格技术或分布式文件系统等功能,将网络中大量各种不同类型的存储设备通过应用软件集合起来协同工作,共同对外提供数据存储和业务访问功能的一个**系统**。全球网络存储工业协会(SNIA)给出的定义:“云存储是通过网络提供可配置的虚拟化的存储及相关数据的服务。云存储的内涵是存储虚拟化和存储自动化”。这两个定义都有几个共同的**特征**：首先它是基于网络的；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。云存储模式的安全问题：①身份认证和访问控制问题,由于鉴别的措施太弱,导致数据或者存储的信息可能会被假冒和窃取;②数据存储和传输的保密性问题;③数据隔离问题(越界访问/信息隔离性);④应用安全问题。**云存储安全机制**：(1)**云存储平台安全机制**：保护整个云存储系统自身的安全。其主要要有两个技术：第一个是**密码技术**，保证完整性，提供基于 PKI 的强身份鉴别以及存储节点的透明加密。另一个是**加固技术**，采用主动防御技术保障服务器,主机的安全性；采用操作系统内核加固实现对计算 / 存储节点、虚拟主机的保护，免遭病毒、木马攻击；实现主机虚拟化技术，实现对虚拟主机的保护，实现数据隔离。(2)**云存储管控安全机制**：主要解决安全管理的问题。(3)**云存储应用安全机制**：主要从以下几方面来实现：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。**可信计算技术**:**可信计算的思想**源于人类社会,是把人类社会成功的管理经验用于计算机信息系统和网络空间,以确保计算机信息系统和网络空间的安全可信。三个定义:①ISO/IEC: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②IEEE:计算机系统所提供服务的可信赖性是可论证的③可信计算组织(TCG):一个实体是可信的,如果它的行为总是以预期的方式,朝着预期的目标。TCG 的可信计算技术思路是通过在硬件平台上引入可信平台模块 TPM(trusted platform module)来提高计算机系统的安全性，这种技术思路目前得到了产业界的普遍认同。**可信计算的宗旨**是以可信计算安全芯片为核心改进现有平台体系结构，增强通用计算平台和网络的可信性。其**基本思想**是: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**主要有直接和间接两种方法。TCPA 可信计算结构(3 层):可信平台应用软件层,TPM 软件栈层,TPM 层。

第 7 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**,实质上是一系列方法和手段的**集合**。目前造成网络不安全的主要因素是系统,协议及数据库等在设计上存在漏洞和缺陷。**漏洞的 3 种常见定义**①系统安全步骤，管理控制,内部控制等处的一个缺陷,有可能被攻击者利用获取对信息的非授权访问或破坏关键任务;②物理设施,人员,管理,硬件或软件上的缺陷,这些缺陷可能被利用并给系统带来危害;是一种或一组可能使系统受到攻击的状态③系统中存在的任何错误或缺陷。**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。**网络攻击的一般流程**:**系统调查**:攻击者选取攻击目标主机后,利用公开的协议或工具**通过网络收集目标主机相关信息的过程**。这一过程并不对目标主机产生直接的影响,而是为进一步的入侵提供有用信息。**系统安全缺陷探测**:在收集到攻击目标的相关信息后,攻击者通常会利用一些自行编制或特定的软件扫描目标主机,**寻找攻击目标系统内部的安全漏洞**,为实施真正的攻击做准备。**步骤(1)和(2)也称为网络探测**。**实施攻击**:当获取到足够的信息后,攻击者就可以结合自身的水平及经验总结制定出相应的攻击方法,**实施真正的网络攻击**。这一阶段的核心任务是解决如何进入目标系统的问题，常用手段包括破解口令直接获取权限，或利用软件漏洞植入恶意程序等。**巩固攻击成果**:基于前期的侵入成果,控制目标系统,完成既定攻击任务。这一阶段中的**重点是长期隐蔽潜伏**,并完成攻击任务。常见手段是利用木马等控制软件。**痕迹清理**:在成功实施攻击后，攻击者往往会利用获取到的目标主机的控制权，清除系统中的日志记录和留下后门,**消除攻击过程的痕迹**,以便日后能不被觉察地再次进入系统。**网络探测(网络侦察)**初始信息的未知性->网络攻击具备一定难度。故探测是攻击者在攻击开始前必需的情报收集工作，攻击者通过这个过程需要**尽可能多地了解攻击目标安全相关的各方面信息**，以便能够实施针对攻击。探测可以分为三个基本步骤:踩点,扫描和查点。**网络踩点**是指攻击者收集攻击目标相关信息的方法和步骤，主要包括攻击对象的各种联系信息,包括名字,邮件地址,电话号码,传真号,IP 地址范围,DNS 服务器,邮件服务器等相关信息。其目的在于了解攻击目标的基本情况,发现存在的安全漏洞、寻找管理中的薄弱环节和确定攻击的最佳时机等,为选取有效的攻击手段和制定最佳的攻击方案提供依据**传统方法**用 whois 通过因特网实施踩点:Linux 系统内置的查询工具,可以查企业的很多在线信息,包括 Internet Registrar 数据(企业申请上网时填报的信息),企业名称数据,包括 DNS 服务器,网络地址块的分配和使用情况,POC(PointOfContact,联系人)信息.**对策**:在向因特网注册机构提供企业信息的时候一定要谨慎从事，不要把某位具体人员的直接联系方式或其他不应该暴露的信息填写出来.**现代方法**利用因特网搜索引擎执行踩点。利用搜索引擎可以查找到目标的 Web 主页，从而进一步定位到目标网络**网络扫描**攻击者常常通过扫描来发现目标系统的漏洞，然后通过漏洞来侵入目标系统。从技术上看,漏洞的来源主要包括以下方面:1 软件或协议的设计瑕疵:在很多早期的软件和协议设计过程中,基本没有考虑安全方面的因素,从而存在很多安全方面的缺陷和漏洞;2 软件或协议实现中的弱点,即使设计得非常完善的协议在实现过程中仍可能引入漏洞;3 软件或协议本身的瑕疵,如没有进行数据内容和大小检查、没有进行完整性检查等;4 系统和网络配置错误。**主动式扫描是基于网络的**：通过执行一些脚本文件模拟对系统进行攻击的行为并记录系统的反应，从中发现可能的漏洞。主动式扫描一般可以分成：活动主机探测,ICMP 查询,Ping 扫描,端口扫描,指定漏洞扫描,综合扫描等。扫描方式分成两大类:**慢速扫描**是指对非连续端口进行的,源地址不一致的,时间间隔长而没有规律的扫描;**乱序扫描**是指对连续端口进行的,源地址一致的,时间间隔短的扫描。**被动式扫描策略是基于主机的**：对系统中不合理的设置,脆弱的口令以及其他同安全规则相抵触的对象进行检查。被动式扫描不会对系统造成破坏,而主动式扫描会对系统进行模拟攻击,可能造成破坏。**网络扫描技术**包括 Ping 扫描(确定哪些主机正在活动),端口扫描(确定有哪些开放服务),操作系统辨识(确定目标主机的操作系统类型)和安全漏洞扫描(确定目标上存在着哪些可利用的安全漏洞)。信息可能包括远程服务上运行的各种 TCP/UDP 服务、操作系统版本 / 类型信息,应用程序版本 / 类型信息,系统存在的安全漏洞等**端口扫描**攻击者向目标发送探测数据包,目的主机通常会根据不同的探测数据包予以回应,攻击者通过分析受害者的回应获取大量有用的目标信息。**常见的扫描类型** **TCP 连接扫描**这是最基本的扫描方式。通过 connect()系统调用向目的主机某端口发送完整的 TCP 连接请求。如果能够顺利完成三次握手过程,则此端口开放。这种方法比较容易被操作系统检测。**TCP SYN 扫描（半连接扫描）**向目的主机只发送 TCP 连接请求(SYN 请求),如返回 SYN/ACK,则说明目的主机相应端口处于等待连接状态;如收到 RST/ACK 应答,则端口未开放。这种方法比完整连接扫描更隐蔽,操作系统一般不予记录。**TCP FIN 扫描** 扫描工具向目的端口发送 FIN 请求,如端口关闭,按照 RFC793 的要求,应该返回 RST 包。此方法适用于 UNIX 系统主机,Windows 系统(没有遵守 RFC793)不受影响 **TCP ACK 扫描**向目标端口发送 ACK 包,可以用来检测防火墙安装情况,了解防火墙类型等信息 **TCP Null 扫描**根据目标主机的响应,可以判断操作系统是 Windows 还是 UNIX**TCP RPC 扫描**用于 UNIX 系统，检查远程过程调用的端口以及对应的应用程序及其版本等信息 **UDP 扫描**向目标端口发送 UDP 包,如返回“ICMP PORT UNREACHABLE”,则端口关闭;否则端口开放 **ICMP 扫描**通过向目的主机发送 ICMP 探测包,分析应答包据可以探测目的主机操作系统类型等信息。由于 ICMP 探测包的隐蔽性，所以一般的入侵检测系统难以发现**著名的扫描工具**包括 Nmap(主机是否在线,主机端口(嗅探所提供的网络服务),主机操作系统),PortScan 等,知名的安全漏洞扫描工具包括开源的 Nessus 及一些商业漏洞扫描产品如 ISS 的 Scanner 系列产品。**缓冲区溢出攻击**是利用缓冲区溢出漏洞所进行的攻击行动。攻击者利用缓冲区溢出攻击可以导致程序运行失败,系统关机,重新启动等后果，精心设计的缓冲区溢出攻击甚至可以利用它执行非授权指令，甚至可以取得系统特权,进而进行各种非法操作。**基本原理**是攻击者通过**向目标程序的缓冲区写入超出其长度的内容**，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。**造成缓冲区溢出的原因是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**，造成程序运行出错。通常情况下，攻击者往缓冲区中填过多的数据造成溢出只会出现**分段错误**，而不能达到攻击目标主机的目的。常见的方法为:通过制造缓冲区溢出,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**。如果该受到溢出攻击的程序有管理权限的话,攻击者可以很容易地获得一个有管理员权限的 shell,从而实现对目标主机的控制。**导致缓冲区溢出漏洞的原因**在程序设计过程中，未对输入数据的合法性(如长度)进行认真检查是导致缓冲区溢出存在的重要原因;数组访问越界,序列的下标越界,都是导致缓冲区溢出漏洞的原因。**防范**①通过操作系统控制使接收输入数据的**缓冲区不可执行**,从而阻止攻击者植入攻击代码②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、利用工具进行代码检查等③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。**(DoS,DDoS)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，使被攻击主机的资源耗尽而停止服务 **UDP 泛洪攻击** 攻击者利用简单的 TCP/IP 服务，如字符发生器协议和 Echo，来传送占满带宽的垃圾数据，通过伪造与某一主机的 Chargen 服务之间的一次 UDP 连接，回复地址指向开着 Echo 服务的一台主机。这样就在两台主机之间存在很多的无用数据流，这些无用数据流会导致针对带宽服务的攻击 **Ping 泛洪攻击**由于在早期阶段，路由器对包的最大尺寸都有限制，许多操作系统对 TCP/IP 堆栈的实现在 ICMP 包上都是规定 64kB，并且在对包的标题头进行读取之后，要根据该标题头里包含的信息来为有效载荷生成缓冲区。当产生畸形时，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**是利用在 TCP/IP 堆栈中实现信任 IP 碎片中的包的标题头所包含的信息来实现自己的攻击。IP 分段含有指明该分段所包含的是原包的哪一段的信息,某些 TCP/IP(包括 Service Pack 4 以前的 Windows NT)在收到含有重叠偏移的伪造分段时将崩溃 **Land 攻击**是设计一个特殊的 SYN 包，它的源地址和目标地址都被设置成某一个服务器地址。此举将导致接受服务器向它自己的地址发送 SYN-ACK 消息，结果这个地址又发回 ACK 消息并创建一个空连接。被攻击的服务器每接收一个这样的连接都将保留，直到超时。不同的操作系统对 Land 攻击的反应不同，大多数 UNIX 系统将崩溃,Windows NT 系统则变得极其缓慢 **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,最终导致目标主机崩溃。在这种攻击方式中,攻击者不直接向目标主机发送任何数据包,而是引导大量的数据包发往目的主机,因此也被称为“**反弹攻击**”。**分布式拒绝服务攻击(DDoS)**是在传统的 DoS 攻击方式上衍生出的新攻击手段。指借助于客户 / 服务器技术，将多台计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力。攻击者使用一个主控程序预先被植入到大量傀儡主机中的代理程序。代理程序收到特定指令时就同时发动攻击，利用客户 / 服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行，因此能够产生比 DoS 攻击更大的危害后果。**拒绝服务攻击的防范**:**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(time out)时间;及时更新系统补丁 **网络设备设置**:**防火墙的设置**: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；严格限制对外开放的服务器的向外访问，这主要是防止服务器被攻击者利用。**路由器的设置**:**使用扩展访问列表**它既可以用来探测 DoS/DDoS 攻击的类型，也可以阻止 DoS/DDoS 攻击**使用 QoS** 如加权公平队列(WFQ)、承诺访问速率(CAR)、一般流量整形(GTS)以及定制队列(CQ)等**使用单一地址逆向转发**逆向转发(RPF)是路由器的一个输入功能，该功能用来检查路由器接口所接收的每一个数据包。如果路由器接收到一个数据包，但是路由表中没有为该源 IP 地址提供任何路由信息，路由器就会丢弃该数据包。因此，逆向转发能够阻止 Smurf 攻击和其他基于 IP 地址伪装的攻击**使用 TCP 拦截** Cisco 公司的路由器在 IOS 11.3 版以后，引入了 TCP 拦截功能，这项功能可以有效防止 SYN Flood 攻击内部主机**使用基于内容的访问控制**基于内容的访问控制(CBAC)是对传统访问列表的扩展，它基于应用层会话信息，智能化地过滤 TCP 和 UDP 数据包，可以防止 DoS/DDoS 攻击。使用上述的方法并不能完全避免 DoS/DDoS 攻击，但能起到一定的缓解和预防作用 **僵尸网络(Botnet)概念**是攻击者出于恶意目的,融合传统的恶意代码形式,如计算机病毒,蠕虫和木马等技术,传播僵尸程序感染大量主机,并通过一对多的命令与控制信道控制被感染主机所组成的叠加网络。**结构**：**控制者**命令的发起者,即控制僵尸网络的攻击者。控制者通过控制服务器发布攻击命令,更新僵尸程序,设置攻击类型等 **主机(bot)**俗称“肉鸡”,是一个被僵尸程序感染的主机。僵尸程序秘密运行在被感染的主机中,可以接收控制者发布的命令并执行命令。僵尸程序的本质就是一个网络客户端，会按照服务器的命令执行相应的代码 **命令与控制服务器(CommandAndControlServer,C&C server)**控制者与僵尸主机通信的平台。控制者通过命令与控制服务器发布命令，僵尸主机则通过命令与控制服务器接收命令并向控制者发送命令执行报告。命令与控制服务器通过专门的**命令与控制信道**和僵尸主机进行通信 **僵尸程序的典型结构**命令与控制模块是整个僵尸程序的核心,实现了僵尸主机与控制者的交互,使僵尸主机接受攻击者的控制命令,进行解析和执行。**传播模块**通过各种不同的方式将僵尸程序传播到新的主机,使其加入僵尸网络接受攻击者的控制,从而扩展僵尸网络的规模。(↑基本↓辅助)**信息窃取模块**用于获取受感染主机信息,以及搜索并窃取感染主机上有价值的敏感信息**僵尸主机控制模块**是攻击者利用受控的大量僵尸主机完成各种不同攻击目标的模块集合，包括 DDoS 攻击模块,发送垃圾邮件模块以及点击欺诈模块等**下载与更新模块**为攻击者提供向受控主机注入二次感染代码以及更新僵尸程序的功能**躲避检测与对抗分析模块**对僵尸程序进行多态,变形,加密等,并通过各种方式进行实体隐藏,以及检查 debugger 的