**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) mod 26 P=D(k**，**C)=(C-k) mod 26。**对称密码分为流密码和分组密码，流密码(stream cipher)又称作序列密码，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多时,密钥的产生,存储和分发是一个很大的问题.公钥密码体制：将加密密钥和加密函数公开。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、 数字签名和身份认证)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/公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×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＝ (mod n),对每个密文块C,明文P＝ (mod 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：基于消息加密/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/密钥分发/密钥验证/密钥使用/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。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。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，用户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，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**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（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运算，结果发送给系统。系统通过结果比对实现认证。**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，从而保护了密钥的安全，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与数据加密。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/数字签名和签名验证,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/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/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。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 但是这种方法存在问题，它要求每一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规定消息的字节顺序,而不遵循已有的惯例。在版本5中，所有消息结都遵循抽象语法表示(ASN.1)和基本编码规则(BER)的规定,提供一个明确无二义的消息字节顺序。**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，即用用户密钥进行的加密。**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交换密码块攻击。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环境,保证网络上信息的安全传输。PKI应用系统的组成:IETF的PKI小组制订了一系列的协议,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名称一起惟一标识该证书。**(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)签发者惟一标识**:版本2和版本3中可选的域，用于惟一标识认证中心CA。**(9)证书主体惟一标识**:版本2和版本3中可选的域,用于惟一标识证书主体。**(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。’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“访问者”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，主体的属性可能还包括其安全状态。**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。**Linux, UNIX, Windows Server**有自主访问控制功能。**自主访问控制概念:也称**“基于主人的访问控制”，自主访问控制来实施访问控制，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。**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**:任何主体都有可能对某一客体进行操作，系统安全性很难得到保障；**等级型**(主体组织成等级型结构)：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，但是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“主体给出提案管理员裁定是否通过”。**HRU不足:**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:**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。**基于角色特性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：**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，则该用户可以对其它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：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自主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此客体的保护位的修改权限授予某些用户来实现，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：**对应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，像安全数据库这类系统通常采用授权关系表来实现其访问控制安全机制。**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证级别。**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,对所有主体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他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，安全标签对其自身的安全等级进行了标识用来比较。**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许可，用户对特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执行的所有操作的集合。**授权管理：**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**。授权角色指派关系: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。**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只需将权限分配给特定角色,然后将该角色授权给相应用户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、强动态性和强隐私性特点**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设备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安全,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解密的关键要素,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,属性集合同待访问资源相关联,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待访问资源相结合,属性集合同用户私钥相关联适合电子医疗访问,社交网站访问。**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表示。**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;对象的敏感度. **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，属性证书被存放在属性库中。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属性证书来提供的。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:**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,必须有正确的解密密钥,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,数据隐藏和数据嵌入,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,指纹和完整性保护等,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:指隐藏对象抗拒常用的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对象的信息丢失。(3)安全性:指隐藏算法具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**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，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:信息隐藏算法中占有重要地位,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数据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的某种程度的保护或监控。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,并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。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。(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的提取互逆。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。(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比特的目的.(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信道监控者的怀疑。(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媒体。原理: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(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(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,很难适应带宽并不十分宽裕的互联网络信道传输.因此,更具伪装特性的图像隐写算法往往选择通用性强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可感知性的实现（即视觉的空间屏蔽效应）目前①大块图像做微小平行移位②小范围图像做修改③以空间分辨率换取灰度分辨率(6)文本文档信息隐密：1.利用空格,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)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受到的处理,操作甚至是恶意攻击,使得提取出的信息足以跟踪出非法分发者(3)嵌入量:因为嵌入的内容要实现用户攻击后能留下足够的信息使发行商进行跟踪,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无辜购买者也不能受到指控(5)效率:要求带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，以增加该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**。数字指纹协议：**非对称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,核心内容包括安全应用交付系统,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,要保证的它们的安全性,除了依靠自身的安全性以外，**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机制，采用各种安全策略模型，在系统硬件和资源以及用户和应用程序之间进行符合预定义安全策略的调用，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**: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系统符合设计规范，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：网络安全等级保护技术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,系统测试的完备性以及形式化验证程度。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**是安全操作系统设计的最关键问题。它必须能够保证系统中所有的访问控制要求都满足系统的安全策略。基于安全核构建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的访问关系。**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)与安全策略相关的文件:比如安全策略库,标识与鉴别的数据库等;(3)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:操作系统内部的关于进程的活动,执行域交换以及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,它必须仲裁所有访问,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：

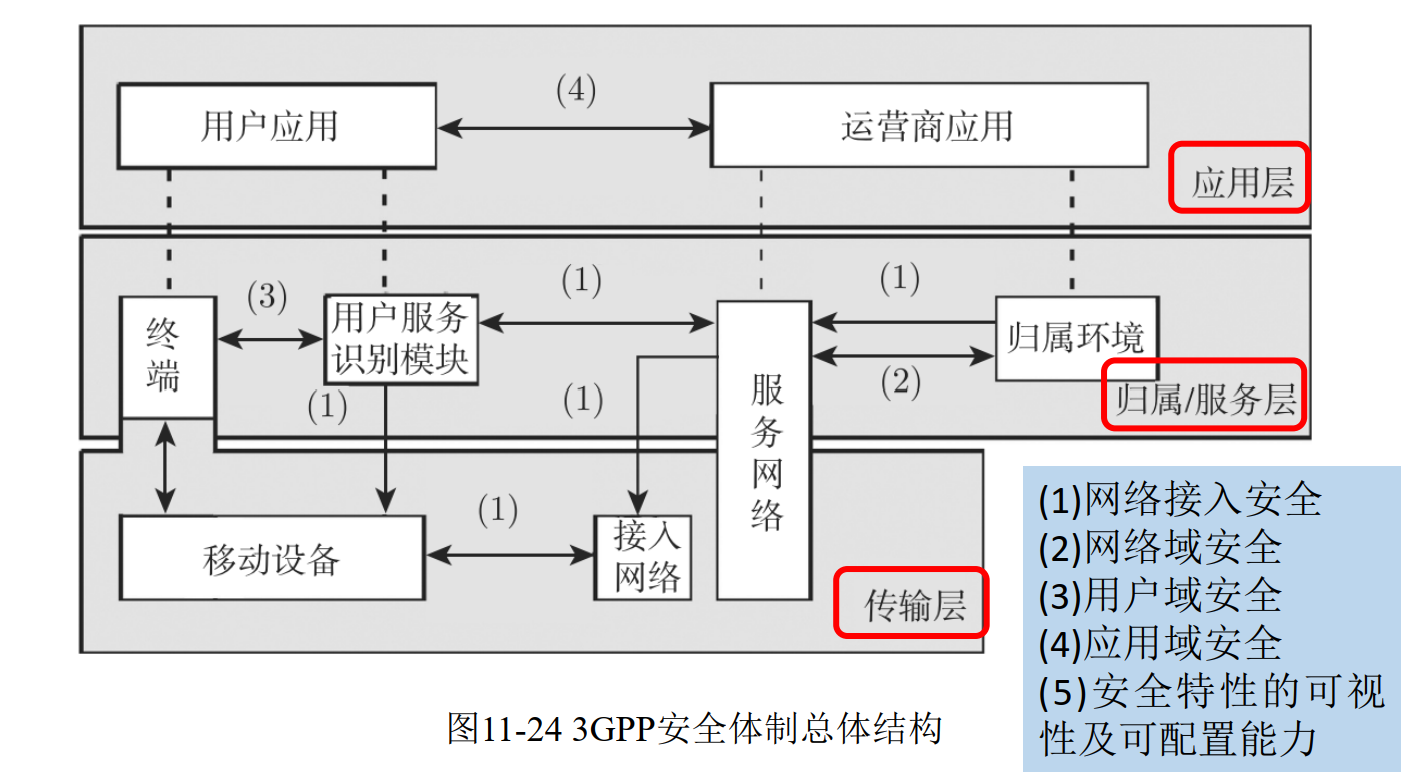
|应用程序 |应用程序 |应用程序 |应用程序 |

|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的安全;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,即确保存储器中的数据能够被合法地访问),**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,也就是用户所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程序作为模块加入内核空间后破坏系统。能力机制是通过是一组比特位来实现的，该机制将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的网络层数据包过滤框架,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,非法篡改以及系统拒绝信息的访问服务。数据库的安全保护需求:(1)防止不适当访问(2)分级保护(3)防止推断性攻击(4)数据库的完整性(5)数据的操作完整性(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,我国: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，而且要充分考虑来自服务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.数据库隐私保护;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**：保护整个云存储平台系统自身的安全，其中主要有两个技术：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攻击目标,**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软件。**巩固攻击成果:**基于前期的侵入结果，控制目标系统,完成既定攻击任务。这一阶段的**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),企业各职能部门的组织结构信息,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法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,即使设计得非常完美,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)。信息可能包括远程机器上运行的各种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**攻击者向受害者发送探测数据包，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主机信息。**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，分析应答包数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**，而不能达到控制目标主机的目的。常见的攻击方法: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转入数据的**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。此举将导致接收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，将多台主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控制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，利用客户机／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**命令的发起者,即控制僵尸网络的攻击者。控制者通过控制程序给僵尸网络发布攻击命令,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器的交互,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的存在,识别虚拟机环境,杀死反病毒进程,阻止反病毒软件升级等功能,使得僵尸程序能够躲避受控主机使用者和反病毒软件的检测。**工作机制①感染目标主机，构建僵尸网络**攻击者会通过各种方式侵入主机，植入僵尸程序来构建僵尸网络。传播方式主要有远程漏洞攻击、弱口令扫描入侵、邮件附件、恶意文档、文件共享等②**发布命令，控制僵尸程序,推模式**是指僵尸主机在平时处于等待状态,僵尸控制程序主动向僵尸主机发送命令,僵尸主机只有被动接收到控制端命令后才进入下一步动作。**拉模式**是指控制端程序会将命令代码放置在特定位置,僵尸程序会定期从该位置主动去读取代码,作为进行下一步动作的命令③**展开攻击**本地攻击指发起针对僵尸网络内部被控主机的攻击,比如对用户隐私信息的窃取等。远程攻击指攻击非僵尸网络内部的主机,根据目的不同又分为两类:(1)扩展僵尸网络规模,**目的**是让外部主机感染同样的僵尸程序,最终成为僵尸网络的一部分。(2)打击,渗透方式,比如分布式拒绝服务,垃圾邮件等④**攻击善后**主要目的是隐藏攻击痕迹，防止被追踪溯源。**缓冲区溢出漏洞原理**由于函数里局部变量的内存分配是发生在栈帧里的，所以如果在某一个**函数内部**定义了缓冲区变量，则这个缓冲区变量所占用的内存空间是在该函数被调用时所建立的栈帧里。由于对缓冲区的潜在操作(比如字串的复制)都是从内存低址到高址的,而**内存中所保存的函数返回地址往往就在该缓冲区的上方(高地址)**这就为覆盖函数的返回地址提供了条件。当用大于目标缓冲区大小的内容来填充缓冲区时，就可以**改写**保存在函数栈帧中的**返回地址**,从而改变程序的执行流程,**执行攻击者的代码** (A=esp;B=$esp,offset=A-B;ret中esp) **方法一:**将Shellcode放置在跳转地址(函数返回地址所在的栈)之前:如果被攻击的缓冲区较大,足以容纳Shellcode。Offset为被攻缓冲区(buffer)首地址与函数的返回地址所在栈地址的距离，需要通过gdb调试确定(foo函数入口处esp减strcpy前esp指向的地址）**方法二:**将Shellcode放置在跳转地址之后:如果被攻击的缓冲区的长度小于Shellcode的长度,不足以容纳shellcode。**第8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(管理和技术结合)。**安全防护的涉及面很宽,**从技术层面上讲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。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。**防火墙的定义：** 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,网络防火墙隔离了内部网络和外部网络，**防火墙的设计目标：**(1)针对所有的通信 (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.**防火墙的常用技术(1)服务控制** 决定哪些Internet服务可以被访问，无论这些服务是从内而外还是从外而内**(2)方向控制** 决定在哪些特定的方向上服务请求可以被发起并通过防火墙**(3)用户控制** 根据用户正在试图访问的服务器，来控制其访问**(4)行为控制** 控制一个具体的服务怎样**被实现** **防火墙具有的典型功能：(1)访问控制功能:**最基本且重要,通过禁止或允许特定用户访问特定资源,保护内部网络的资源和数据。防火墙定义了单一阻塞点,它使得未授权的用户无法进入网络,禁止潜在的,易受攻击的服务进入网络 **(2)内容控制功能** 根据数据内容进行控制，比如过滤垃圾邮件、限制外部只能访问本地Web服务器的部分功能等**(3)日志功能** 防火墙需要完整地记录网络访问的情况，包括进出内部网的访问。一旦网络发生了入侵或者遭到破坏，可以对日志进行审计和查询，查明事实**(4)集中管理功能** 针对不同的网络情况和安全需要，指定不同的安全策略，在防火墙上集中实施，使用中还可能根据情况改变安全策略。防火墙应该是易于集中管理的，便于管理员方便地实施安全策略**(5)自身安全和可用性** 防火墙要保证自己的安全,不被非法侵入,保证正常的工作。若防火墙被侵入,安全策略被破坏,则内部网络就变得不安全。防火墙要保证**可用性**,否则网络就会中断,内部网的计算机无法访问外部网的资源**(6)另外,防火墙可能还具有流量控制,网络地址转换(NAT),虚拟专用网(VPN)等功能。防火墙的局限性：(1)不能防御不经由防火墙的攻击(2)不能防范来自内部的威胁(3)不能防止病毒感染的程序和文件进出内部网(4)不能防止数据驱动式的攻击 防火墙分为不同的类型：A.**从工作原理角度看，防火墙技术主要可分为网络层防火墙技术和应用层防火墙技术。这两个层次的防火墙技术的具体实现有包过滤防火墙,代理服务器防火墙,状态检测防火墙和自适应代理防火墙。**B.**根据实现防火墙的硬件环境不同，可将防火墙分为基于路由器的防火墙和基于主机系统的防火墙。包过滤防火墙和状态检测防火墙可以基于路由器,也可基于主机系统实现;而代理服务器防火墙**只能**基于主机系统实现。**C.**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。通常也将几种防火墙技术**结合**在一起使用以弥补各自的缺陷,增加系统的安全性能 **1.包过滤技术1)包过滤原理** 包过滤技术是最早的防火墙技术,工作在**网络层**.**原理**是将IP数据报的各种包头信息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。常用的包头信息包括源地址,目的地址,源端口,目的端口,协议类型等. 包过滤防火墙要遵循的一条基本原则就是**“**最小特权原则”,即明确允许管理员希望通过的那些数据包,禁止其他的数据包。包过滤的**核心技术**是安全策略及过滤规则的设计.包过滤防火墙一般由路由器充当，要求路由器在完成路由选择和数据转发之外，同时具有包过滤功能.**包过滤防火墙的具体实现: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。过滤规则的设计主要依赖于数据包所提供的包头信息:源地址,目的地址,TCP/UDP源端口号,TCP/UDP目的端口号,标志位,用来传送数据包的协议等**2.**由规则表和数据头内容的匹配情况来执行过滤操作。如果有一条规则和数据包的状态匹配，就按照这条规则来执行过滤操作;如果没有一条规则匹配，就执行默认操作。默认的策略可能是:**1默认值:丢弃:**那么所有没有被规定允许转发的数据包都将被丢弃。**2默认值:转发:**那么所有没有被规定需要丢弃的数据包都将被转发**2)包过滤防火墙的优点(1)一个过滤器能协助保护整个网络(2)包过滤用户对用户透明(3)过滤路由器速度快、效率高(4)技术通用,廉价,有效(5)易于安装使用维护3)包过滤防火墙的缺点(1)安全性较差(2)由于防火墙可用的信息有限，它所提供的日志功能也十分有限(3)无法执行某些安全策略(4)这种防火墙通常容易受到利用TCP/IP规定和协议栈漏洞的攻击，**例如网络层地址欺骗**(5)**在这种防火墙做出安全控制决定时**，起作用的只是少数几个因素，**包过滤器防火墙对由于不恰当的设置而导致的安全威胁显得十分脆弱**。**很少把这种包过滤技术作为单独的解决方案 **2.代理服务技术1)代理服务技术原理** 代理服务器防火墙又称应用层网关,应用层防火墙，它工作在OSI模型的应用层,掌握着应用系统中可用作安全决策的全部信息。代理服务技术的核心是运行于防火墙主机上的代理服务器程序,这些代理服务器程序直接对特定的应用层进行服务。代理服务器防火墙完全阻隔了网络通信流,通过对每种应用服务编制专门的代理服务程序，实现监视和控制应用层通信流的作用。从内部网用户发出的数据包经过这样的防火墙处理后，就像是源于防火墙外部网卡一样，从而可以达到隐藏内部网结构的作用。**2)代理服务器的实现(1)应用代理服务器**可以在网络应用层提供授权检查及代理服务功能**(2)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**(3)智能代理服务器**可提供比其他方式更好的日志和访问控制能力**(4)邮件转发服务器3)代理服务器防火墙的特点** (1)安全性好(2)易于配置(3)能生成各项记录(4)能完全控制进出的流量和内容(5)能过滤数据内容(6)能为用户提供透明的加密机制(7)可以方便地与其他安全技术 **合成代理服务技术的缺点**(1)速度较慢(2)对用户不透明(3)对于不同服务器代理可能要求不同的服务器，可能需要为每项协议设置一个不同的代理服务器(4)通常要求对客户或者过程进行限制(5)代理不能改进底层协议的安全性。**3.状态检测(动态包过滤技术)技术1)工作原理** 它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**。检测引擎在不影响网络正常运行的前提下，采取抽取有关数据的方法对网络通信各层实时监测。**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，一旦发现任何连接的参数有意外的变化，连接就被终止。状态检测技术**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。2)通过状态检测防火墙数据包的类型** (1)TCP (2)UDP **3)状态检测技术的特点和应用** 状态检测技术**结合了包过滤技术和代理服务技术的特点**。状态检测技术**克服了包过滤技术和代理服务技术的局限性**，能根据协议,端口及源地址,目的地址的具体情况决定数据包是否通过。状态检测技术的**缺点是状态检测可能造成网络连接的某种迟滞**,但运行速度越快,这个问题就越不易察觉。**自适应代理防火墙技术**,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(屏蔽主机防火墙(单/双宿堡垒主机),屏蔽子网防火墙(最安全))**1. 防火墙的应用** 选用防火墙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, 也要考虑用户的安全策略中的特殊需求：**(1) IP**地址转换**(2)**双重**DNS(3) VPN(4)**病毒扫描功能**(5)**特殊控制需求 **2. 防火墙技术的发展1)智能化(识别防御攻击,调整连接端口,流量分配,自动检测修复,自主学习)2)高速度3)分布式并行结构4)多功能5)专业化(特定服务)** 传统的安全防护技术包括防火墙件等,也称为**被动防护**技术 **入侵检测**是一种从更深层次上进行**“主动”**网络安全防御的措施。具有**主动性和实时性**的特点。**1.入侵检测的概念**入侵检测是指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。它是对入侵行为的发觉。**主要目的**在于:1识别入侵者;2识别入侵行为;3检测和监视已成功的安全突破;4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。**入侵检测的概念**:入侵检测是监测计算机网络和系统,发现违反安全策略事件的过程。**定义:**是对企图入侵,正在进行的入侵或已经发生的入侵行为进行识别的过程；其他定义:①检测对计算机系统的非授权访问识别②对系统的运行状态进行监视,发现各种攻击企图,攻击行为或攻击结果;③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。**入侵检测的典型过程：**①信息收集是指从网络或系统的关键点得到原始数据②数据预处理是指对收集到的数据进行预处理,转化格式③数据的检测分析是指利用各种算法建立检测器模型,并对输入的数据进行分析以判断入侵行为的发生与否④响应是指产生检测报告,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 **审计记录的两种方法 (1)原始审计记录 (2)检测专用的审计记录 审计包含：1.主体(行为的发起者)2.动作(主体对一个对象的操作或联合一个对象完成的操作)3.客体(行为的接收者)4.异常条件5.资源使用6.时间戳 入侵检测系统是完成入侵检测功能的软件,硬件的组合(事件生成器,事件分析器,事件数据库,响应单元,目录服务器(定位,控制,认证))** **入侵检测系统实体**:①事件生成器(采集和过滤事件数据)②事件分析器(分析事件数据和任何CIDF组件传送给它的各种数据)③事件数据库(存放原始或已加工的数据)④响应单元(针对分析结果,根据响应策略采取相应的行为,发出命令响应攻击)⑤目录服务器(定位,控制,认证,防止受到攻击)**主要功能**(1)监测并分析用户和系统的活动(2)核查系统配置与漏洞(3)识别已知的攻击行为并报警(4)统计并分析异常行为(5)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 **1.基于检测对象的分类** 1)基于主机的入侵检测系统(HIDS)(**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,额外开销,缺乏对平台的支持,可移植性差)2)基于网络的入侵检测系统NIDS(**优点**: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,与操作系统无关性;**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,防入侵欺骗的能力较差) 3)混合式入侵检测系统(综合了网络和主机两种结构特点的**IDS**) **2.基于检测技术的分类1)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(有一组正常调用数据)(**优点**:准确率高,能够发现任何..,较少依赖于特定的操作系统环境;**缺点**:有误报,统计方法进行模糊匹配->在实现上有一定难度)**2)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**有检测过程简单,检测效率高，针对已知入侵的检测精度高,**缺点**有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。**3.基于工作方式的分类 1)离线检测系统(非实时工作) 2)在线检测系统(实时联机的检测) 分布式入侵检测**系统的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,如环境复杂，则数据分析模块也会分布 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**。**入侵检测(目前存在问题:**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**)研究重点:**1.分布式入侵检测2.智能入侵检测3.高效的模式匹配算法4.基于协议分析的入侵检测5.与操作系统的结合6.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7.入侵检测系统自身安全性的研究8.入侵检测系统的标准化 **Snort**是一个基于**libpcap**的轻量级网络入侵检测系统 一个基于Snort的网络入侵检测系统由以下5个部分组成:解码器;预处理器;检测引擎;输出插件;日志/警报子系统.Snort中包含了三类预处理器,分别实现包重组/协议解码/异常检测 **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,对行为捕获和分析,了解工具方法,推测意图动机,了解安全威胁,增强安全防护能力 **蜜网**又可称为诱捕网络 **分类1.**按系统功能分类产品型蜜罐和研究型蜜罐两类。**2**.按系统交互活动级别分类根据系统允许与黑客交互活动的级别,蜜罐可分为低交互蜜罐与高交互蜜罐**3**.按服务实现方式分类为了欺骗攻击者,蜜罐需要提供与真实的主机相似的操作系统和服务根据服务实现方式将蜜罐系统分为**真实蜜罐**和**虚拟蜜罐**。**4**.按服务提供方式分类根据服务提供方式将蜜罐分为服务端蜜罐和客户端蜜罐 **蜜罐技术的核心机制** 1.欺骗环境构建机制(安全资源)2.威胁数据捕获机制(全面记录)3.威胁数据分析机制**辅助机制**1.安全风险控制机制2.配置与管理机制3.反蜜罐技术的对抗机制**。应急响应技术** 概念:**Why?** 安全防护技术不能保证系统100%安全,由于安全事件的突发性,复杂性与专业性,在组织体系以及协调机制方面都存在很多不和谐不规范的问题。为了有备无患,需要建立计算机安全事件的快速响应机制,“**计算机安全应急响应组(CSIRT)**”便应运而生。**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。**CSIRT**是一种服务组织,其职责就是接受,分析,响应有关计算机安全报告和活动,其服务对象通常为一个固定实体 1.**固定的**:把履行应急响应作为主要工作2.**临时的**:在需要时召集起来以响应(处理)一个计算机安全事件**CSIRT定义的计算机安全事件** 任何真实的或者可疑的,与计算机系统或计算机网络的安全相关的敌对事件,或者任何违反明显的或者隐含的安全策略的行为。可能包括(1)试图(不管成功与否)获得对系统或其数据的未授权访问(2)意外的破坏或者拒绝服务(3)未授权地使用系统或者存储数据(4)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类型**(1)内部..:为其所在的组织或机构提供应急响应服务(2)国家..:为其所在的国家提供应急响应服务(3)协调中心:协调和推动各种不同的CSIRT之间的应急响应工作(4)分析中心AC:专注于综合各种来源的数据以决定应急响应的趋势和类型,其提供的信息用来帮助预报未来的活动或者提供某些行为的早期报警(5)卖方团队:处理他们自己的软件,硬件产品的漏洞报告,采用开发补丁,进行补救或提出缓解的办法(6)应急响应提供商:为其他机构提供付费的应急处理服务 应急响应策略指导CSIRT正确,有效运作的主要原则。按照策略的作用范围,一般可以把策略**分为以下几种:**①全局策略:人员培训策略,道德规范策略,运行评价策略等②服务特定策略,反病毒策略,电子邮件策略,口令保护策略等③基础策略,操作代码策略,信息分类策略,信息披露策略,媒体策略,安全策略,人为过失策略等。应急事件处理流程**1)安全事件的热线响应**•如果网络受到攻击者入侵,病毒感染,或者发生了其他安全相关的事件,可以CSIR报告,CSIRT根据事件的紧急程度提供相应的帮助.**包括**(1)检查入侵来源(2)恢复系统正常工作(3)事故分析(4)发布安全警报,安全公告,安全建议(5)咨询(6)风险评估(7)安全教育培训(8)协助其他组织成立自己的CSIRT,建立网络应急与救援队伍。**2)应急响应的主要阶段**(1)准备阶段:建立合理的防御/控制措施,适当的策略和程序,获得必要的资源和组建响应队伍等(2)检测阶段:做出初步的动作和响应。根据获得的初步材料和分析结果,估计事件的范围和发展势态,制定进一步的响应战略,并且保留可能用于司法程序的证据。(3)抑制阶段:抑制的目的是限制攻击的范围。可能的抑制策略一般包括:关闭所有的系统;从网络上断开相关系统;修改防火墙和路由器的过滤规则;封锁或删除被攻破的登录账号;提高系统或网络行为的监控级别;设置陷阱;关闭服务;反击攻击者的系统等。(4)根除阶段:在事件被抑制之后,通过对有关恶意代码或行为的分析结果,找出事件根源并彻底清除。(5)恢复阶段:恢复阶段的目标是把所有被攻破的系统和网络设备彻底还原到它们正常的运行状态。恢复工作应该十分小心,避免出现误操作导致数据的丢失。另外,恢复工作中如果涉及机密数据,需要额外遵照机密系统的恢复要求。(6)报告和追踪阶段:这个阶段的目标是回顾并整理发生事件的各种相关信息,尽可能地把所有情况记录到文档中。这些记录的内容,不仅对有关部门的其他处理工作具有重要意义,而且对将来应急工作的开展也是非常重要的积累 应急响应技术及工具 **1)应急响应技术**包括漏洞检测,监听,日志分析,路由控制,反向追踪技术等**2)支持CSIRT日常运作的工具和技术**(1)执行CSIRT运作流程:事件跟踪和报告;事件分类和归档;通信(2)提供安全远程访问:远程网络访问,远程拨号访问,安全隧道(3)前置工具,支持审计/检测漏洞/预防事件:网络审计,主机审计,软件审计,网络监控,网络入侵检测**3)支持事件调查的工具**(1)证据收集工具:检查存储媒体,检查系统(2)证据调查工具:分析证据,校验同一性(3)证据处理工具(4)系统恢复工具**第9章安全审计与责任认定技术 安全审计**概念:**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,稽查与计算安全审计及主要功能:①通过对系统事件的记录,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;②通过事后分析及追查取证,保证系统的安全 **安全审计(..)主要功能(1)..自动响应**:指当审计系统检测出一个安全违规事件(或潜在安全攻击)时做出的响应,是管理审计事件的需要,这些需要包括报警甚至阻断。根据审计事件不同系统做出不同响应**(2)..数据生成:**规定了对与安全相关的事件进行记录,包括鉴别审计层次,列举可被审计的事件类型,以及鉴别由各种审计记录类型提供的相关审计信息的最小集合(系统可定义可审计事件清单,每个可审计事件对应于某个事件级别,至少应包含:事件发生时间,事件类型,主题标识,执行结果,引起事件的用户标识以及对每一个审计事件与该事件有关的审计信息**(3)..分析**:定义了分析系统活动和审计数据,来寻找可能或真正的安全违规操作:可用于入侵检测或对安全违规的自动响应,当一个审计事件集出现或累计出现一定次数时,可确定一个违规的发生,并执行审计分析,事件集合能由经授权的用户进行增加,修改或删除**(4)..浏览**:指经过授权的管理人员对于审计记录的访问和浏览,审计系统需要提供审计浏览的工具**(5)..事件存储**:指对审计记录的维护,如何保护审计、如何保证审计记录的有效性,以及如何防止审计数据的丢失(需要对审计记录,审计数据进行严密保护,防止未授权的修改,还需要考虑在极端情况下保证审计数据的有效性.审计系统存储的问题通常是磁盘空间用尽:单纯采用覆盖旧记录的方法是不够的,审计系统应当能够在审计存储发生故障或者在审计存储即将用尽时采取相应的动作**(6)..事件选择**:指管理员可以选择接受审计的事件.**审计系统结构(1)集中式结构**•集中收集和分析来自于多台主机的源审计记录,所有事件信息均要传送到中央处理机上,分析并做出响应•系统通过多个数据采集点收集数据,经过简单的过滤处理,将数据通过网络传输到中央处理机**面临挑战**:(1)所有事件信息分析工作由中央处理机完成,其负担非常重,且难以适应大量用户的增容(2)不能容括各种空间上分布的组件及公共服务(3)单点失效,可扩展性有限,难以重新配置,增加功能困难等问题(4)系统自适应能力差,不能根据环境变化而进行自动配置。通常配置的改变和增加是通过编辑配置文件来实现的,往往需要重新启动系统以使配置生效**(2)分布式结构**安全审计任务由分布于网络各处的审计单元协作完成,这些单元还能在更高层次结构上进一步扩展,从而能够适应网络规模的扩大.**结构:(1)主机代理模块:**在受监视系统中,作为后台进程运行的审计信息收集模块,主要**目的**是收集主机上与安全相关的事件信息,并将数据传送给中央管理者**(2)局域网监视器代理模块**分析局域网上的通信信息,并根据需要将结果报告给中央管理者**(3)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。**工作过程**•①主机代理模块截获审计收集系统生成的审计记录,应用过滤器去掉与安全无关的记录,然后将这些记录转化成一种标准格式以实现互操作。然后代理中的分析模块分析记录,并与该用户的历史映像相比较,当检测出异常时,向中央管理者报警②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,以查出显著事件,监视出异常时向中央管理者报警。**分布式结构优点**(1)扩展能力强:通过扩展审计单元来实现网络安全范围的扩张(2)容错能力强:解决了单点失效问题(3)兼容性强(4)适应性强.当网络和主机状态改变时,分布式审计系统可以容易地作相应修改。**设计分布式系统时考虑的问题**(1)需要处理**不同的格式**以实现不同节点间**互操作**。(2)存在保证这些**数据完整性和机密性**的需求:保证**完整性**是为了防止入侵者通过修改传输的审计信息来掩盖其行为,保证**机密性**是因为传输的审计信息可能是有价值的(3)**分析中心设置**问题:**集中式结构**,存在对所有审计数据进行收集和分析的中央点,方便了关联输入报告的工作,但造成了潜在的瓶颈和单点故障;**分散式结构**,存在多个分析中心,但它们必须能够协调各自的行为并交换信息。审计的数据来源 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,其数据源可以分为三类:基于主机、基于网络和其他途径。**(1)基于主机的数据源**目的:检查对系统的可疑操作,防止非法入侵,并分析操作系统的系统记录和安全记录,发现可疑操作或者非法操作,修补系统漏洞。**数据源**四类:**1)操作系统日志:由三个元素来描述,主体(**用户或者代表用户的操作行为**)、客体(**受保护的系统资源**)和行为(**系统服务和上层的程序应用行为**)**。任何一种事件都可表示为主体对客体进行的操作。**Windows事件日志**从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**。每种类型的事件使用特殊格式记录在单独的日志文件中,通常只可以通过操作系统提供的事件查看器读取。操作系统日志是基于主机的审计系统或入侵检测系统(下称A)的**首选数据源**,原因在于:(1)操作系统为A及其产生的审计记录提供了实质性保护,提高了数据源可信度(2)A从操作系统层次上获取系统信息,没有经过高层的抽象,因此可得系统事件的细节,易实现精确模式匹配。(3)若入侵者试图通过插入伪造的审计记录来破坏审计信息,这种低层次系统审计数据也使入侵者行动更为困难**2)系统日志**:反映各种系统事件和设置的文件。UNIX通用审计服务syslog,用于产生和更新事件日志**安全性较差,原因:**1.产生系统日志的软件通常作为应用程序运行,容易遭到破坏;2.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。由于syslog使用简单,许多系统应用和网络服务用它作日志数据**3)应用日志** 应用日志通常代表系统活动的用户级抽象信息,相对于系统的安全数据来说,**去除了大量的冗余信息**,更易于浏览和理解;通常有某种特定格式.**4)基于目标的信息**只对系统的部分进行审计,即**面向目标的安全审计**;**方法**:评估出系统中关键的或是有特殊价值的对象,针对每一个对象制定信息收集和监视机制,该对象即为审计目标。对于审计目标每一次状态转变,与系统的安全策略进行比较,所出现的任何异常都进行记录或响应。最常见基于目标的审计技术是**完整性校验**:审计对象多为文件,采用消息摘要算法计算需要保护的系统对象的校验值,并存储在安全区域,周期性对目标进行检查,可发现目标是否被改变,从而提供一定级别保护。**(2)基于网络的数据源** 基本原理:采用特殊的数据采集技术收取网络中传输的数据作为数据源**1)网络数据的获取** 网卡通常有**正常模式**和**混杂模式**。正常模式下主机仅处理以本机为目标的数据帧;混杂模式下网络适配器可接收本网段内所有数据帧。基于网络的安全审计系统必须利用网络适配器的混杂模式,获得经过本网段的所有数据信息,从而实现获取网络数据的功能。**2)采用网络数据源的优势**(1)对受保护系统的性能影响很小或几乎没有,无须改动原先的系统和网络结构(2)网络嗅探器对用户是透明的,降低了嗅探器本身遭受入侵者攻击的可能性(3)网络监听相对基于主机的安全审计更容易检测到某些基于网络协议的攻击方法.如检测DoS(4)网络监听可针对一个网络的数据进行分析,与受保护主机的操作系统无关.与之相比,基于主机的IDS必须首先保证操作系统的正常工作,并且需要针对不同的操作系统开发不同的版本**(3)其他途径的数据源** (1)路由器,交换机等网络设备产生的活动日志•可通过syslog实现方便的转发和处理•一个典型的syslog记录包括生成该记录的进程名字,文本信息,设备和优先级范围等•对防火墙,IDS等安全设备所产生的活动日志其格式则没有统一标准•一般将网络及其安全设备的活动日志作为审计数据源可提高安全审计系统的性(2)带外数据源:通过人为,非系统方式获得信息,这些信息对于事后的分析可能起重要作用。**2.数字取证**概述: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;**作用**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响应一个计算机安全紧急事件.**主要作用**:获得证据,打击违法犯罪(1)发现和归档证据和线索(2)固定其他途径发现的证据(3)帮助揭示事件模型(4)关联攻击和受害的计算机(5)展现端到端侵害事件的路径,不管侵害是否已遂(6)提取隐藏、删除或者其他不能直接得到的数据**其他作用**(1)排除故障(2)日志监控:实时取证需要监视各种日志文件,分析和关联各种系统的日志记录(3)数据恢复:从系统中恢复丢失的数据(4)数据提取:帮助从加密,隐含,分散的文件及系统区域提取,还原数据(5)完善策略:调查用户违反安全策略的行为,针对取证的结果,提出完善安全策略的方法。**数字取证的分类**:按照不同的分类方法,可以分成不同类型(1)主机取证和网络取证(2)事后取证和实时取证(3)司法取证和非司法取证.**数字取证的数据媒介**①标准的计算机系统②网络设备③外部设备④存储设备⑤消费电子产品.**电子证据的特点和取证基本原则:直接目的:**得到说明或验证**某个事件的证据**;计算机取证得到的证据称为电子证据或数字证据。必须满足**两个根本属性①可接受性**在技术上或者法律上可以接受**②完整性**数据是真实,可靠的。**真实性:**数据来源于它本来的地方并且没有被污染**可靠性:**数据所说明的事实可信和一致,需要将数据与其结果关联 **电子证据的特点(1)数字性(2)技术性**(产生,储存和传输及其采集,分析和判断均依靠技术)**(3)脆弱性(**数据的修改可以在瞬间完成,并且可以不留痕迹,这使电子证据脆弱不可靠)**(4)多态性**(电子证据的表现形式多种多样)**(5)人机交互性**:其形成的不同环节有不同计算机操作**人员参与**,且**会对电子证据施加不同影响(6)复合性**电子证据是多种形式证据的集合。计算机**取证应该遵循的原则(1)及时性原则**:时效性**(2)取证过程合法性原则**:取证过程须按法律规定公开进行**(3)多备份原则**:对含电子证据的媒介至少应制作两个副本(提取分析)**(4)环境安全原则**:取证过程应在安全环境中进行**(5)严格管理过程的原则** **数字取证的过程:四阶段分别对应媒介,数据,信息,证据:①收集:**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;主要任务是发现潜在数据源并从中获取数据(1)发现潜在的数据源:事先要做出一份列表,以免遗漏(2)获取数据1.制定获取方案2.获取数据3.检验数据完整性**②检查:**用合适技术和工具从收集的数据中发现和提取相关信息,也要保证数据的完整性,检查阶段一般结合取证工具用**手工**方式进行;通过评估数据与特定事件的关联性从收集的数据中提取信息。1.涉及消除操作系统或者应用软件的影响2.发现硬盘大量文件中值得关注的数据是极为费时的工作.这时就必须使用过滤器以及其他方法来加快**③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调查;分析提取的数据进而依据系统的方法得出结论。分析工作包括辨别是谁,地点,物品和事件,决定这些元素如何关联并导出结论**④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。依据分析写出报告,写报告要考虑下面的因素:**(1)不同解释**:当一个事件有多个合理的解释时,报告中都应给出可信的解释说明**(2)不同听众 3.数字取证关键技术和工具 证据信息类别**按照其数据来源划分为:①来自文件的数据②来自操作系统的数据③来自网络的数据④以及来自应用软件的数据等。取证要综合以上各种来源的数据。**来自文件的数据取证技术**除了标准文件还有一些特殊数据在取证中有时也可以起到极为重要的作用**(1)删除的文件**通常文件被删除时,其数据没有在媒介擦除,只是被标记为删除。这就意味着文件仍存储在媒介上,但不再被操作系统列出**(2)松弛空间**如果一个文件需要的存储空间小于分配单元(簇或块),操作系统仍然为它分配整个分配单元**(3)空闲区**分区上未分配的空间,可能含以前文件数据的片断**1.收集文件:** 1)从媒介复制文件:收集数据时产生副本:主拷贝和**工作拷贝**。取证工作应在**工作拷贝**上进行。两种技术:**(1)逻辑备份:**从逻辑卷复制文件和目录,但不能复制删除的文件或空闲区的残余数据**(2)比特流映像:**也称磁盘映像,逐位复制整个原始媒介,包括空闲区和松弛区数据.可以是磁盘到磁盘或磁盘到文件的复制。对一个**正在运行**的系统,不可执行**整个**物理设备的比特流映像,因为这个系统在不断变化,但可以执行某一逻辑区域的比特流映像。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易复制2)数据文件完整性 保证原始媒介的完整性,确保数据不会更改,写保护能实现。执行完备份和映像操作后需要校验副本是否是原始媒介的精确复制,通常使用MD5和SHA-1,一些复制设备和软件本身内建了计算消息摘要值功能。**确保完整性步骤**A.首先计算和记录原始媒介的消息摘要值,再执行备份或映像,并计算和记录副本的消息摘要值,比较这两个值来保证数据完整性得到保护B.然后再次计算原始媒介的消息摘要值并和先前计算的值比较,确保备份或映像过程没有破坏原始媒介数据。3)文件的MAC属性:文件的时间属性和其他属性,是文件的重要属性,是取证中必须特别关注的文件属性。UNIX维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,最后状态改变时间等信息;Windows同样为每个文件维持着这样三个时间戳,分别是创建时间,最后写/修改时间,最后访问时间。如果要建立整个事件发生的精确的时间戳,就必须妥善保护好时间属性。因为并不是所有的收集工具都会保存文件的时间。映像一般会保存文件的时间,但一些工具的逻辑备份操作在复制和计算消息摘要值的同时会改变文件的最后访问时间。4)其他技术问题(1)数据恢复:虽然可以使用工具来恢复被删除的文件和硬盘的数据残留,但如果媒介被专用的反取证软件处理或者被物理破坏,那么数据恢复就必须借助于更复杂和更昂贵的技术,如磁显微镜(2)隐含数据的修复:一些计算机系统会允许用户隐藏文件,目录和分区。这时对磁盘结构的仔细分析就非常必要(3)RAID阵列数据的收集:对于硬件RAID有**两种技术收集数据**:一种是使用专门的软件来重组RAID,这时必须记录并使用原先RAID卡的参数配置;另一种就是利用取证的引导盘启动系统,直接使用原系统的RAID阵列并保证数据的完整性。对于软件RAID,要通过查看磁盘上保存的RAID参数来重建RAID(4)关于数据编码和解码:字符集是指文字的集合,数据编码则是根据一定的算法将数据转换成需要的格式**2.检查数据文件**:将数据收集并保存在另外媒介之后就要对其进行检查分析。这时使用只读锁连接计算机和存放数据的媒介仍是必需的,可以防止对数据不小心的修改。检查技术涉及定位包含相关信息的所有文件,包括删除的文件,在松弛区和空闲区残留的文件以及隐藏的文件等,加密和口令保护使这项工作变得复杂。(1)定位文件:手工定位和发现包含相关信息的文件和碎片极为费时,而且必须对文件系统有透彻的了解。一些工具和技术可以帮助自动完成这个定位过程。例如,将空闲空间的数据转换为文件保存,恢复删除的数据,恢复回收站的数据等。(2)提取数据:要提取文件内容首先必须知道**文件类型**,一般通过扩展名来识别。但文件扩展名可被删除、修改和隐藏,所以仅依靠扩展名来辨别文件类型不可靠,**更精确的方法是查看文件的头部信息**;另一种方法是使用**直方图**了解文件类型,依靠显示文件中所有字符的ASCII码分布的比例判定类型。(3)使用取证工具进行检测(1)文件查看(2)解压缩文件(3)目录结构的图形化显示(4)识别已知文件(5)执行串搜索和模式匹配(6)访问元数据(数据的数据,如图象建立时间,版权等)**3.分析文件**:分析提取数据,以确定事件,按照时间和路线重建整个事件发生,发展的时间序列和因果关系。**来自操作系统的数据取证技术:1.收集操作系统数据**:对于非易失性数据的收集,类似于文件系统的收集,而易失性数据的收集,一定要在系统关机或重新启动之前进行。**1)收集易失性数据(网络连接,登录会话,内容,运行的进程,打开的文件等):**从正在运行的系统中收集易失性数据存在固有的风险。**2)收集非易失性数据**:在易失性数据收集完成后,就可以收集一些非易失性的操作系统数据(用户名,口令,日志)**2.检查和分析操作系统数据:** 对于正在运行的系统的进程检查和分析,分为日志文件分析、列出计划任务、检查非法服务和自启动进程和查看网络连接的端口等方面。**来自网络的数据取证技术1.网络流量数据源**:可分别从网络协议的各个层捕获①防火墙和路由器②数据包嗅探器和协议分析器③入侵检测系统④远程访问系统⑤安全事件管理软件⑥其他来源(DHCP服务器,网络监控软件,ISP记录)**2.收集网络流量数据:**网络流量数据记录在日志文件或者数据包捕获文件里,所以收集网络流量数据就如同收集日志文件或者数据包捕获文件一样简单**3.检查和分析网络流量数据**1)发现相关的事件2)检查数据源:高效方法是从少数基本数据源开始调查。3)攻击者确认。**来自应用软件的数据:**所有应用软件都包含各种形式的可执行文件或脚本,此外还包括一些组件:1)配置和设置:通过修改配置设置文件,应用软件允许用户定制它的某方面行为2)验证用户身份3)日志4)数据5)支持文件6)应用结。**1.收集应用软件数据**:哪些数据要收集取决于哪些应用软件值得关注,此外同样类型数据不同应用软件可能保存在不同地方**2.检查和分析应用软件数据**:如果应用软件是特殊的,数据分析工作就会遇到困难,另外应用软件可能有安全机制保护敏感数据。**第10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;**安全机制(机理):**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**;**安全服务(服务方式)**: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.**目的**在于利用一种或多种安全机制进行反攻击。网络攻击是指降级,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。安全攻击分成两类:**被动攻击:**试图收集,利用系统的信息,不影响系统的正常访问;**主动攻击:**是攻击者访问所需信息的故意行为,一般会改变系统资源或影响系统运作。被动攻击:信息收集:造成传输信息的内容泄露.流量分析:可以判断通信的性质.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。安全服务定义为(RFC2828),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.安全服务通过安全机制来实现安全策略。OSI安全体系结构定义5大类,共14个安全服务。**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.1.在单条消息的情况下,鉴别服务的功能是向接收方保证消息来自所声称的发送方2.对于正在进行的交互,鉴别服务涉及两个方面:首先,在连接的初始化阶段,鉴别服务保证两个实体是可信的;其次,鉴别服务必须保证该连接不受第三方的干扰.1.对等实体鉴别:该服务在数据交换连接建立时提供,识别一个或多个连接实体的身份,证实参与数据交换的对等实体确实是所需的实体.2.数据源鉴别:该服务对数据单元的来源提供确认,向接收方保证所接收到的数据单元来自所要求的源点.它**不能防止重播或修改数据单元**.**访问控制服务**: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.该服务可应用于对资源的各种访问类型或对资源的所有访问.**数据保密性服务**:数据保密性服务为防止网络各系统之间交换的数据被截获或被非法存取而泄露,提供机密保护.保密性是为防止传输的数据遭到被动攻击:(1)连接保密性:对一个连接中所有用户数据提供机密性保护(2)无连接保密性:为单个无连接的N-SDU(N层服务数据单元)中所有用户数据提供机密性保护(3)选择字段保密性:为一个连接上的用户数据或单个无连接的N-SDU内被选择的字段提供机密性保护(4)信息流保密性:提供对可根据观察信息流而分析出的有关信息的保护,从而防止通过观察通信业务流而推断出消息的源和宿主,频率,长度或通信设施上的其他流量特征等信息.**数据完整性服务**:(1)带恢复的连接完整性:为连接上的所有用户数据保证其完整性.检测在整个SDU序列中,任何数据的修改,插入,删除和重播,并予以恢复(2)不带恢复的连接完整性:差别仅在于不提供恢复(3)选择字段的连接完整性:保证一个连接上传输的用户数据内选择字段的完整性,并以某种形式确定该选择字段是否已被修改,插入,删除或重播(4)无连接完整性:提供单个无连接的SDU的完整性, 并以某种形式确定接收到的SDU是否已被修改(5)选择字段无连接完整性:提供在单个无连接SDU内 选择字段的完整性,并以某种形式确定选择字段是否已被修改.**不可否认服务:**不可否认服务用于防止发送方在发送数据后否认发送,以及接收方在收到数据后否认收到或伪造数据的行为. (1)具有源点证明的不可否认:为数据接收者提供数据源证明,防止**发送者**以后任何企图否认发送数据或它的内容的行为. (2)具有交付证明的不可否认:为数据发送者提供数据交付证明,防止**接收者**以后任何企图否认接收数据或它的内容的行为。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**。在特定的协议层设置的一些**安全机制**主要为以下几种:-加密机制:提供对数据或信息流的保密,并可作为其他安全机制的补充.加密算法分为两种类型:对称密钥密码体制,加密和解密使用相同的秘密密钥;非对称密钥密码体制,加密使用公开密钥,解密使用私人密钥.网络条件下的数据加密必然使用密钥管理机制.-数字签名机制:数字签名是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,这种数据或变换允许数据单元的接收方确认数据单元来源和数据单元的完整性,并保护数据,防止被人伪造.数字签名机制的两个过程:对数据单元签名:使用签名者专用的保密信息作为私用密钥,加密一个数据单元并产生数据单元的一个密码校验值.对验证签过名的数据单元的验证:使用公开的方法和信息来确定签名是否是使用签名者的专用信息产生的。数字签名的基本特点是,签名只能使用签名者的专用信息产生.-访问控制机制:当实体试图使用非授权资源或以不正确方式使用授权资源时,访问控制功能将拒绝这种企图,产生事件报警并记录下来作为安全审计跟踪的一部分. 访问控制机制可用以下一种或多种信息类型为基础(1)访问控制信息库(2)鉴别信息(3)用于证明访问实体或资源的权限的能力和属性 (4)按照安全策略,许可或拒绝访问的安全标号(5)试图访问的时间(6)试图访问的路径(7)访问的持续时间.-数据完整性机制:包括两个方面:一是单个数据单元或字段的完整性;二是数据单元或字段序列的完整性1.确定单个数据单元完整性,包括两个过程:一是发送实体将数据本身的某个函数量(称为校验码字段)附加在该数据单元上;二是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以确定在传输过程中数据是否被修改(无法防止重播)2.对连接型数据传输中数据单元序列完整性的保护,要求附加明显的次序关系.对于无连接型数据传输,使用时间戳可提供一种防止个别数据单元**重播**的限定形式.-鉴别交换机制:鉴别交换机制是通过互换信息的方式来确认实体身份的机制。鉴别交换机制的选择:(1)当对等实体和通信方式两者都可信时,一个对等实体的验证可由通行字实现.通行字可以防错,但不能防止蓄意破坏(2)当每一实体信得过各自的对等实体,而通信方式不可信时,对积极攻击的防护由通行字和加密相结合实现.防止重放攻击的单向鉴别需两次 “握手” ,而具有重放防护的相互鉴别可由三次 “握手”实现(3)当一实体不能(或感觉到将来不能)相信对等实体或通信方式时,应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:通信业务填充机制能用来提供各种不同级别的保护,对抗通信业务分析.这种机制产生伪造的信息流并填充协议数据单元以达到固定长度,只有当信息流**受加密保护,本机制才有效**.-路由选择机制:路由能动态地或预定地选取;在检测到持续的操作攻击时,端系统可以指示网络服务的提供者经不同的路由建立连接,带有某些安全标记的数据可能被安全策略禁止通过某些子网络,中继站或链路;根据安全策略,禁止带有安全标号的数据通过一般的(不安全的)子网络,链路或中继站.-公证机制:这种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. 这种保证由通信实体信赖的第三方公证员提供.在可检测方式下,公证员掌握用以确证的必要信息.公证机制提供服务还使用到数字签名,加密和完整性服务.-辅助的安全机制(1)可信功能:系统的软硬件应是可信的.获得可信的方法包括形式证明、检验和确认、对攻击的检测和记录,以及在安全环境中由可信成员构造实体(2)安全标签:给资源附上安全标签,表示其安全敏感程度(3)事件检测:包括检测与安全有关的事件,以及检测”正常”事件(4)安全审计跟踪:独立地回顾和检查系统有关的记录和活动,以测试系统控制的充分性.它提供安全性违反的检测与调查,保证已建立的安全策略和操作过程的一致性.帮助评估损害, 并推荐有关改进系统控制,安全策略和操作过程的指示(5)安全恢复:受理事件检测处理和管理职能机制的请求,并应用一组规则来采取恢复行动.恢复行动有三种:一是立即行动. 立即中止操作,如切断连接；二是暂时行动.使实体暂时失效；三是长期行动.使实体进入”空白表”或改变密钥. IPSec协议:IPSec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.IPSec对于IPv4可选,对于IPv6强制性.IPSec通过**多种手段**提供IP层安全服务:允许用户选择所需安全协议,允许用户选择加密和认证算法,允许用户选择所需的密码算法的密钥.IPSec可以安装在**路由器**或**主机**上:若IPSec装在**路由器**上,则可在不安全的 Internet上提供一个安全的通道;若是装在**主机**上,则能提供主机端对端的安全性。**认证头(AH)协议:**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**;**封装安全载荷(ESP)协议:**除了实 现 AH 所 实 现的功能外,还可以实现数据的**机密性**;Internet密钥交换(IKE)协议:用于动态地认证 IPSec 参与各方的身份.安全关联(SA):一个安全关联是发送方和接收方之间的受到密码技术保护的**单向关系**,该关联对所携带的通信流量提供安全服务.如果需要双向安全交换,则需要建立**两个**安全关联, 一个用于发送数据,一个用于接收数据。一个安全关联由三个参数唯一确定(1)安全参数索引(SPI):一个与SA相关的位串,仅在本地有意义.这个参数被分配给每一个SA,并且每一个SA都通过SPI进行标识. SPI并非全局指定,因此,SPI要与目标IP地址,安全协议标识一起来唯一标识一个SA(2)目标IP地址:目前,IPSec SA管理机制中仅仅允许单播地址.它决定了关联方向(3)安全协议标识:标识该关联是一个AH安全关联或ESP安全关联.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).**SAD**包含了与每一个安全关联相联系的参数,**SPD**则指定了主机或网关的所有IP流量的流入和流出分配策略.IPSec的2种工作模式:1)传输模式(IP头-IPsec头-TCP头-data):传输模式主要为直接运行在IP层之上的协议(如TCP,UDP,ICMP)提供安全保护,一般用于在两台主机之间的**端到端**通信. 2)隧道模式(新IP头-IPsec头-原IP头-TCP头-data):隧道模式对整个IP包提供保护.为了达到这个目的,当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:IP认证头(AH)协议为IP数据包提供数据**完整性校验**和**身份认证**,还有可选择的**抗重放攻击保护**, 但不提供数据加密服务. 认证确保进行认证,并相应地提供流量过滤功能,同时还能防止地址欺诈攻击和重放攻击.认证基于消息鉴别码(MAC),双方必须共享同一个密钥;**AH传输**:原IP头-AH-TCP-data/原IP头-跳,目的地址,路由,分段-AH-目的地址-TCP-data;**AH隧道**:新IP头-AH-原IP头-TCP-data /新IP头-扩展头-AH-原IP头-扩展头-TCP-data (认证:all)ESP协议:封装安全载荷(ESP)协议为IP数据包提供**数据完整性校验,身份认证和数据加密**,还有可选择的**抗重放攻击保护**.ESP用一个密码算法提供机密性,数据完整性则由身份验证算法提供.通过插入一个唯一的,单向递增的序列号提供抗重放服务.保密服务可以独立于其他服务而单独选择,数据完整性校验和身份认证用作保密服务的联合服务.只有选择了身份认证时,才可以选择抗重放服务.ESP传输:原IP头-ESP头-TCP-data-ESP尾-ESP认证/原IP头-跳,目的地址,路由,分段-ESP头-目的地址-TCP-data-ESP尾-ESP认证;ESP隧道:新IP头-ESP头-原IP头-TCP-data-ESP尾-ESP认证/新IP头-扩展头 -ESP头-原IP头-扩展头-TCP-data-ESP尾-ESP认证;**认证(头->尾);加密(头(->尾))**IKE协议:IPSec的密钥管理包括密钥的建立和分发.IPSec体系结构文档要求支持两种密钥管理类型.手动:系统管理员手动地为每个系统配置自己的密钥和其他通信系统密钥.这种方式适用于小规模、相对静止的环境;自动:在大型分布系统中使用可变配置为SA动态按需创建密钥. IKE用于动态建立SA和会话密钥.IKE的目的是使用某种长期密钥进行双向认证并建立会话密钥,以保护后续通信.IKE代表IPSec对SA进行协商,并对SAD进行填充。安全套接层(SSL)协议主要目标是为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.**三个特性**(1)保密性:在初始化连接后,数据以双方商定的密钥和加密算法进行加密(2)认证性:协议采用非对称密码体制对端实体进行鉴别,使得客户端和服务器端确信数据将被发送到正确的客户机和服务器上(3)完整性:协议通过采用散列函数来处理消息,提供数据完整性服务.SSL协议分层模型(HTTP/TCP之间)①SSL记录协议②三个高层协议:SSL握手协议,SSL密码修改协议和SSL报警协议.**握手协议**允许客户端和服务器彼此认证对方,并且在应用协议发出或收到第一个数据之前协商加密算法和加密密钥.SSL会话是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.在握手协议中,创建了**读挂起**状态和**写挂起**状态;在握手协议成功完成后,挂起状态成为当前状态.一个**会话状态**由以下参数定义:**会话标识符:**一个由服务器生成的数值,用于标识活动的或恢复的会话状态;**对等实体证书**:对等实体的一个X509.v3证书,此状态元素可以为空;**压缩方法**:在加密前使用的压缩数据的算法;**密码规范:**描述了大量数据的加密算法和用于计算MAC的散列算法,同时也定义了密码学属性;**主密码:**一个由客户端和服务器共享的48字节的秘密数值,提供用于生成加密密钥、MAC秘密和初始化向量IV 的秘密数据;**可恢复性标志:**一个标志,表明会话能否用于初始化一个新的连接.SSL连接:连接是提供合适服务类型的一种传输.对SSL来说,连接表示的是对等网络关系,且连接是短暂的;而会话具有较长的生命周期,**在一个会话中可以建立多个连接**,每个连接与一个会话相关.连接状态可用以下参数定义.服务器和客户端随机数,服务器写MAC密码,客户端写MAC密码,服务器写密钥(服务器加密客户端解密),客户端写密钥(…解密…加密),初始化向量IV,序列号。**SSL协议流程:** ①A发起会话请求,并发送自己支持的密码算法的列表和一个随机数;②B把自己的证书以及另一个随机数发送给A,同时在消息1的密码算法列表中选择自己能够支持的算法响应给A; ③A选择一个随机数S,根据S,和计算会话密钥(主密钥)K.然后A 用B的公钥加密S后发送给B,同时发送的还有会话密钥K和握手消息的散列值,用来证明自己的身份.用于加密这个散列值的加密密钥同时也是对将来的会话数据进行加密的密钥,它是根据主密钥K、和计算出来的.用于数据发送的密钥称为写密钥,用于数据接收的密钥称为读密钥.发送,接收两个方向都需要加密密钥,完整性保护密钥和初始向量IV,因此共需要6个密钥.这6个密钥都是通过会话主密钥生成的;④B也根据S,和计算会话密钥K.B发送此前所有握手消息的散列值,此散列值用B的写加密密钥进行加密保护,用B的写完整性保护密钥进行完整性保护.通过这个消息,B证明自己知道会话密钥,同时也证明自己知道B的私钥,因为K是从S导出的,而S是使用B的公钥加密的。SSL记录协议:保密性+消息完整性.在SSL协议中,所有的传输数据都被封装在记录中.记录是由记录头和长度不为0的记录数据组成的. 所有的SSL通信都使用SSL记录层.**SSL记录协议的操作过程:**数据片段,压缩数据,增加MAC,加密数据和MAC,增加SSL记录头。SSL修改密码规范协议:由一条消息组成,该消息只包含一个值为1的单个字节;SSL报警协议:报警协议用于向对等实体传递SSL相关的报警.如果在通信过程中某一方发现任何异常,就需要给对方发送一条警示消息通告,此协议的每个消息由两个字节组成,第一个字节表示消息出错的严重程度,值“1“表示警告,值“2“表示致命错误,第二个字节包含描述特定报警信息的代码 SSL握手协议: 握手是指客户端与服务器端之间建立安全连接的过程.握手协议在传递应用数据之前使用.握手协议由客户端和服务器间交换的一系列消息组成(类型,长度,内容)阶段一:建立安全能力,包括协议版本、会话标识,密码组,压缩方法和初始随机数;阶段二:服务器发送证书,交换密钥,证书请求,hello完成消息;阶段三:如果接受到消息,客户端发送证书;发送交换密钥,也可以发送证书验证消息;阶段四:改变密码组,结束握手协议。TLS协议:传输层安全(TLS)是IETF标准的初衷,其目标是成为SSL的互联网标准,TLSv1与SSLv3的差别并不是非常大。安全电子交易:安全电子交易(SET)协议是设计用于保护基于信用卡在线支付的电子商务的安全协议,成为事实上的工业标准。SET提供三种服务(1)为交易各方提供安全的信道(2)通过使用X.509v3数字证书提供信任(3)由于信息只在需要的时间和地方提供,因而要确保**私密性**SET的需求(1)提供支付和订购信息的保密性(2)确保传送数据的完整性(3)持卡人账号认证(4)为商家提供认证(5)安全技术(6)创建一个不依赖于传输安全机制也不妨碍其使用的协议(7)在软件和网络提供者之间提供功能设施和互操作性SET需要具有以下特性(1)信息保密性(2)数据完整性(3)持卡人账号认证(4)商家认证SET要达到的主要目标(1)信息在公共因特网上安全传输(2)订单信息和个人账号信息隔离(3)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(加密消息,认证,转换SET消息格式),认证机构CA。基于SET的交易流程:(1)顾客开通账号(2)顾客申请证书(3)商家申请证书(4)顾客进行订购(5)商家被验证(6)发送订购和支付信息(7)商家请求支付认证(8)商家确认订购(9)商家提供商品或服务(10)商家请求付款双向签名机制:双向签名的目的在于将两个接收者不同的消息连接起来.客户想给商家发送订购信息(OI),给银行发送支付信息(PI).支付授权交换由两个消息组成:认可请求和认可应答;**商家向支付网关发送的认可请求消息**包括:与购买相关的信息,与认可相关的信息,证书.**支付网关执行的如下任务:**(1)验证所有的证书(2)解密认证分组的数字信封,获得对称密钥，解密认证分组(3)验证认证分组的商家签名(4)解密支付分组的数字信封,获得对称密钥,解密支付分组(5)验证支付分组的双向签名(6)验证从商家接收到的交易标识,与从客户端接收(间接)的PI的交易标识比较(7)请求和接收来自于发卡机构的认证;支付网关返回的认证应答消息:与认证相关的信息,获取标记信息,证书。**第11章无线网络安全11.1 IEEE 802.11无线网络安全11.1.1 IEEE 802.11无线网络背景:**IEEE 802是开发局域网(LAN)标准的委员会,802.11则是成立于1990年的工作组,负责开发无线局域网(WLAN)的协议与传输规范。802.11有多种扩展名,其中IEEE 802.11是原始标准,规定了无线局域网的物理层和MAC层的内容(1)在无线局域网中,需要认证技术,以验证节点的身份;而在有线局域网中“与网络相连”这个可见行为起了某种程度的认证作用(2)无线局域网需要隐私保护机制;而在有线局域网中“信息的接收节点必须与网络相连”提供了一定程度的隐私性.与有线局域网相比,无线局域网对安全服务和机制有**更高的要求**。IEEE 802.11定义的安全机制:数据保密和完整性,身份认证。1999年发布的802.11b标准里定义了WEP协议,为数据提供**机密性和完整性**保护,并基于WEP协议设计了共享密钥认证机制,协议旨在提供和有线局域网同级的安全性,但WEP存在较大的安全缺陷。因此,IEEE于2001年成立了802.11i任务组,以制定新的安全标准,来增强无线局域网的安全性.在802.11i完善之前,国际Wi-Fi联盟组织提出了WPA标准,作为802.11i完备之前替代WEP的过渡方案;2004年6月,完整的802.11i标准通过,Wi-Fi联盟也随即公布了与之相对应的WPA第二版(WPA2)。**11.1.2 WEP:**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,包含以下三个要素:共享密钥K,初始向量(IV),RC4流密码算法。1.WEP数据**加密及解密**:WEP采用对称加密算法RC4(一种对称流密码体制算法),可以采用64比特或者128比特两种长度的密钥;IEEE 802.11b规定,WEP使用64比特的加密密钥:由两部分组成:40比特WEP用户密钥K和24比特初始矢量IV。WEP数据加密流程(1)数据校验阶段:对消息M计算完整性校验值(ICV),使用的算法是CRC32:ICV=CRC32(M):将ICV与M串接,得到明文P=ICV||M(2)密钥生成阶段:选取一个24比特的初始化向量IV,将初始化向量 IV和40比特的用户密钥K串接起来。以IV||K作为伪随机数发生器的种子,应用RC4算法,生成密钥序列(KS),即KS=RC4(IV||K),一个与P等长的伪随机序列(3)数据加密阶段将KS与P作异或运算即可产生密文C=KS⊕P。发送时传输IV||C。WEP的数据解密过程(1)提取IV和密文C(2)将IV和密钥K一起送入,采用RC4算法的伪随机数发生器得到解密密钥流(3)将解密密钥流与密文相异或,得到明文消息M以及完整性校验值ICV(4)对得到的明文进行处理,采用相同的算法计算完整性校验值ICV(5)比较两个完整性校验值结果,如果相等则说明协议数据正确.WEP的MPDU(MAC协议数据单元)结构:WEP帧中KeyID决定具体使用哪个WEP用户密钥,WEP的MPDU(MAC协议数据单元),结构为从左到右一行:IV:3;KeyID:1;payload(空着不填);ICV:4;(payload和ICV:**RC4 encrypted**)。2.WEP**认证**1)开放系统认证:开放系统认证是IEEE 802.11的缺省认证方式,被称为“零认证”,本质:空认证机制,认证过程没有采用密码技术,安全性较差.认证过程以明文方式进行①无线站点发送一个包含自身ID的认证请求,其中未包含涉及认证的任何与客户端相关的信息②若无线接入点的认证算法标识也为开放系统认证,则它返回一个包含认证成功或认证失败的认证响应(2)共享密钥认证:采用挑战/响应方式,整个**认证过程包括四步骤**(1)认证请求(2)挑战文本(3)加密的挑战文本(4)接入成功/失败(1,3主机->无线站点;2,4相反）3.WEP**密钥**:IEEE 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,每个WEP信息在传送时必须包括密钥编号(key ID),只有发送设备和接收设备都采用相同的共享密钥,信息才能被正确地传送和解码.实际中WEP共享密钥后就永远不会变增加加密方案被破解的可能4.WEP的**缺陷**:1)静态共享密钥和IV重用;WEP没有密钥管理的方法,使用静态共享密钥,通过IV/shared key来生成动态密钥,静态密钥的安全强度较低。IV的取值空间为[0,]。当加密的数据包个数超过时,IV必然发生重复,如果此时没有更换密钥的话,会出现种子密钥重复,从而很容易被破解2) CRC-32的漏洞CRC算法是线性的,所以CRC校验体现出了很强的数据关联性,违背了密码学的随机性原则:攻击者只要在信息流中插入一定比特位后再调整CRC校验与其相符,就可以做到破解密钥3)认证的漏洞:WEP协议中规定的身份认证是单向的,协议中规定的共享密钥认证也容易导致认证伪造。如果攻击者同时截获了挑战文本和加密挑战文本,就很容易根据RC4(IV,K)=C⊕P恢复出密钥序列,从而获得认证数据中的有用信息,以此通过接入点的验证而获得网络资源的访问。WEP协议本身没有抗重放保护机制,接收方无法识别该报文是发送方发送的还是攻击者重放的。**11.1.3 802.11i:**IEEE 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**:A.认证:定义用户和网络的交互,以提供**相互认证**,并生成用于STA和AP之间无线通信的短期密钥B.访问控制:对认证功能的增强,能与多种认证协议协同工作C.带消息完整性的**机密性**:MAC层数据与消息完整性校验码一起加密以提供机密性和完整性。**IEEE802.11i强安全网络操作的5个阶段**:(1)发现阶段(2)认证阶段(3)密钥管理阶段(4)安全通信阶段(5)连接终止阶段**802.11i协议结构**:第一行:扩展认证协议EAP;第二行802.1x;第三行:前一半TKIP,后一半CCMP:两种数据加密机制,增强了WLAN中的数据加密和认证性能。IEEE 802.11i**支持的安全协议**:①加强的加密算法CCMP或TKIP,其中必须实现基于**AES**的CCMP②动态的会话密钥③具有密钥管理算法④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⑤支持快速漫游和预认证⑥支持独立基本服务集IBSS)。1.TKIP(数据加密和完整性) TKIP是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.TKIP与WEP一样基于RC4加密算法,但相比 WEP算法,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。TKIP对与WEP引入了四种新机制以提高加密强度:(1)每包一密钥(2)消息完整性校验码(MIC)(3)具有序列功能的初始化向量IV(4)密钥生成及定期更新功能TKIP从如下几个方面**加强**WEP协议(1)WEP缺少防止消息伪造和其他主动攻击的机制,TKIP中设计MIC以保证MSDU数据单元的完整性,从而可以有效抵抗这类攻击(2)TKIP中使用两个阶段的混合加密函数计算得到WEP seed.同WEP中的静态密钥和24位的IV相比较,混合函数把密钥和数据包的属性结合起来,可以有效地抵抗**重放攻击,**使密钥更安全(3) TKIP使用TSC给它所发送的MPDU来排序,接收者会丢掉那些不符合序列的 MPDU。这提供了一种较弱的抵抗重放攻击的方法.TKIP的总体安全性取决于WEP核心机制,WEP算法的安全漏洞是由于机制本身引起的,因此,TKIP只是一种**过渡算法**2. CCMP协议:CCMP基于 AES算法和CCM模式,由两个部分组成:①加密模式,用于保证数据的**私密性**;②密码块链式消息认证码(CBC-MAC)模式,用于**数据完整性**校验.CCMP能解决WEP中出现的所有问题。3.认证协议: 1) 802.1x认证模型包含①请求者:STA② 认证者:AP③认证服务器(AS).802.1x认证**过程**(1)连接到AS: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(2) EAP交换:这个交换让STA和AS相互授权(3)安全密钥分发:一旦认证完成,AS和STA产生一个主会话密钥(MSK),此密钥也被称为AAA密钥,STA和AP进行安全通信所需的加密密钥都从MSK产生2) EAP 802.1x 专门定义了在LAN上运行EAP的报文格式EAPoL。EAPoL在原有的EAP报文外面增加了一层封装,使得EAP报文适合在局域网传输,802.11i并没有限制采用哪些协议作为上层认证协议,但规定了高层认证协议必须满足双向认证的要求,并推荐采用EAP-TLS方法(基于TLS的认证方式,认证服务器与请求者采用TLS协议协商会话密钥,该协议要求双方都要有公钥证书)3) RADIUS(远程用户拨号认证)协议是一个应用普遍的 AAA (Authentication, Authorization, Accounting)协议,最初为拨号网络设计,基于IP网络4.密钥管理1)密钥层次:在802.11i中,存在多个层次的密钥。认证成功后,无线工作站STA和认证服务器AS 各自生成32字节的对等主密钥(PMK),PMK生成的方法与认证方式相关。如果是EAP认证,则由认证过程得到EAP主密钥 (主会话密钥MSK),再由MSK派生出对等主密钥 PMK。认证服务器AS将密钥材料安全地传送到认证者AP,从而使AP生成相同的PMK,PMK处于**密钥层次的第一级**.AES密钥导出层次:对等主密钥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)由 PMK导出PTK (PTK=PRF-384(PMK,Len(PMK),"Pairwisekey expansion”,MIN (AA,SA)|[MAX (AA,SA) ||MIN (AN, SN)||MAX (AN,SN)) )。Len()是求长度函数,AA和SA分别代表AP和STA的MAC地址,AN和SN则 是AP和STA产生的Nonce(伪随机数)。PTK从左到右分别为EAPOL KCK L(PTK,0,128),EAPOL KEK L(PTK,128,128),CCMP TEK L(PTK,256,128);再由TEK根据CBC-MAC算法导出AES加密密钥2)四步握手 图片描述:STA和AP为两端。(1)AP端产生AN;AP指向STA端传AN(2)STA端产生SN和PTK;STA端指向AP端,传SN,MIC,STA RSN IE;(3)AP端产生PTK;AP端指向STA端,传AN,MIC,AP RSN IE;(4)STA端指向AP端,传MIC。四次握手的目的在于由STA和AP共享的PMK推导单播通信密钥PTK3)组密钥更新 STA和AP为两端。AP端产生GMK和GNonce,并用KEK加密GMK;从AP端到STA端,箭头上有GNonce,GMK,MIC;STA端解密GTK,从STA端到AP端,箭头上有MIC.组密钥握手机制用来向 STA发送新组密钥GTK。5. RSNA建立过程IEEE 802.11i的强安全网络连接(RSNA)建立过程包含三个实体:申请者(STA),认证者(AP)和认证服务器（如Radius服务器）。大体上,RSNA建立过程可分成6个阶段(1)网络和安全能力发现(2)802.11认证和连接(3)EAP/802.1x/RADIUS认证(4)四步握手(5)组密钥握手(6)安全数据传输**11.2 移动通信系统的安全**移动互联网包括了以下几个要素:I.无线移动通信网络Ⅱ.公众互联网III. 移动通信终端移动互联网比传统互联网具有更高的安全性要求**11.2.1 GSM的安全(2G)**移动通信系统首先必须解决两个问题①对用户进行认证,防止未注册用户的欺骗性接入;②对无线路径加密,以防止第三方窃听。此外,移动台的位置更新过程也将成为系统的安全薄弱环节。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**1.GSM安全机制:每个GSM用户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认证与加密方案的一个设计要点就是保证这一“身份证件”永远无需在无线路径上传输(除非是在网络数据库故障之类的特殊场合)1.GSM安全机制(突发脉冲为传输单位)**1)用户身份认证**SIM卡,MS(移动台),被访MSC(移动交换中心)(RAND,SRES,)在被访侧,1.被访传RAND到MS侧2.MS传RAND到SIM 3.SIM利用A3/A8算法计算,Sim传SRES,到MS 4.MS传到SIM,SIM存储;传SRES到被访,判断与原SRES是否相同,通则认证成功**2)用户数据保密,信令及数据保密** 帧号22bit,64bit进入A5算法输出block1和block2均114bit,MS侧block2到加密发送数据,1到解密接受数据;BTS侧相反。**3)用户身份保密**MS与被访MSC两端 首先TMSI重分配命令(被访指向MS),再重分配完成(反向)(GSM为每个用户分配临时移动用户识别码TMSI)2.认证方案GSM的认证方案采用了单钥体制,认证协议为 “问—答”机制,只对用户进行单向认证。由于公钥体制具有较高的安全性,且更易于密钥的管理,较单钥体制有许多优点。目前限制公钥体制应用的主要因素是其计算量大但随着发展采用双钥体制将会是一种趋势。通过采用更复杂的认证协议,双向认证也将成为可能3.加密算法A5 即使是不采用任何A5算法,GSM也远比模拟蜂窝系统安全4.密钥长度 A5算法的密钥长度只为64比特,并且如果其有效密钥长度果真仅为40比特的话,则只能在短时间内对信息提供保护。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。**11.2.2 GPRS的安全**通用分组无线业务(GPRS) GSM网络向第三代移动通信系统过渡的一项:2.5代(2.5G)通信技术。GPRS的安全机制在GSM的基础上得到了加强,包括身份保密,身份认证,用户数据加密,信令数据加密以及其他由GPRS系统提供的GSM标准之外的安全机制。1. GPRS**网络结构**GPRS网络是在现有GSM网络中增加分组控制单元(PCU),服务GPRS支持节点(SGSN)和网关GPRS支持节点(GGSN)而实现的,使得用户能够在端到端分组方式下发送和接收数据GPRS业务的基本流程①电脑或其他数据设备通过串行或无线方式连接到 GPRS移动台上;②GPRS移动台与基站通信,分组是从基站经分组控制单元处理后发送到SGSN;③SGSN与 GGSN进行通信,GGSN对分组数据进行相应的处理,再发送到目的网络;④来自因特网且标识有移动台地址的IP包,由GGSN 接收,再转发到SGSN,继而传送到移动台上。2.GPRS网络的安全机制 认证过程:从左到右:移动台,SGSN,HLR/AUC三端(竖线)1.移动台到SGSN接入请求2.SGSN到H/A认证数据请求3.H/A到SGSN认证数据响应4.SGSN到移动台认证请求5.移动台到SGSN认证响应6.移动台到SGSN加密的数据通信。1) GPRS系统的身份认证由移动、SGSN和HLR/AUC 共同完成,认证是基于移动台和HLR/AUC之间的共享密钥Ki 。2)信令数据和用户数据加密 GPRS-,输入,方向信息进行GEA运算得到输出与明文生成密文或密文生成明文3)身份保密4) SIM卡的使用 GPRS系统的用户终端利用SIM卡保存用户信息,包括用户的密钥Ki及国际移动用户标识IMSI。**SIM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。认证中心在用户注册时,将用户的密钥Ki和 IMSI分配给用户并装入到SIM卡中,并同时存入 AUC的数据库中。Ki只在SIM卡和 AUC中使用,永远不会在网络中传输,可以有效避免密钥的泄露。3.安全缺陷分析 1)身份认证问题 认证过程是单向的,即只是网络对移动用户认证,用户对SGSN不做认证。可能存在攻击者利用假的SGSN对用户进行欺骗,使用户的敏感信息被窃取或无法正常地访问网络资源。2)信令及数据加密问题 GPRS系统中的加密范围是从移动台到SGSN,不提供端到端的加密;GPRS加密算法GEA密钥长度太短,只有64比特,无法抵抗穷举攻击3) SIM卡问题 IBM的研究人员发现了SIM卡的一个漏洞,分割攻击,攻击者可以在几分钟内获得SIM卡中的密钥信息,而GSM及GPRS系统的安全性都是基于私钥密码。从终端用户的角度来说,要防止别人获得自己的终端。4)其他安全问题 GPRS系统的骨干网是基于IP的网络,所以IP 网络的所有安全问题在GPRS网络中仍然存在 5)结论 GPRS网络继承了GSM网络有效的安全特征,同时GPRS网络在安全方面比GSM网络有所提高。但是GPRS网络毕竟是在GSM网络基础上通过增加特定的网络设备构建起来的,所以必然存在GSM网络在安全方面的一些缺陷,所以在利用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。**11.2.3 第三代移动通信系统(3G)的安全**3G 系统的安全体系主要有两个系列:3GPP(WCDMA)和3GPP2 (cdma2000).3GPP2的认证协议也采用了‘请求-响应‘的形式,认证方式与3GPP类似,但其认证是以基站为核心的,只有其增强认证和加密模式才可提供用户和网络的相互认证。

1. 3GPP安全体制的总体结构:

**(1)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.安全性最为重要,因为无线链路最易遭受各种攻击。功能包括:用户身份保密、认证和密钥分配、数据加密和完整性等.认证和密钥分配是基于USIM和HE/AuC共享秘密信息K的相互认证。认证过程中也融合了加密,完整性保护等措施**(2)网络域安全**:保证网内信令的安全传送并抵御对有线网络(核心网部分)的攻击**(3)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**(4)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**(5)安全特性**的可视性和可配置能力: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。**第12章恶意代码攻击及检测** **概述:恶意代码**最初是指最传统意义上的病毒和蠕虫。木马,后门,恶意脚本,广告软件,间谍软件等都是恶意代码。**定义:**1.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2.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3.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。最常见的恶意代码有计算机病毒(简称病毒),特洛伊木马(简称木马),计算机蠕虫(简称蠕虫),后门,逻辑炸弹等。最近有人把不需要的代码也归类为恶意代码。是指没有作用却会带来危险的代码,包括所有可能与某个组织安全策略相冲突的软件。**分类：**1.根据其代码是否独立，可以将其分成独立的和寄生的恶意代码。**独立的恶意代码**能够独立传播和运行,是一个完整的程序,它不需要寄宿在另一个程序中;**非独立的恶意代码**只是一段代码，必须寄生在某个程序(或文档)中,作为该程序的一部分进行传播和运行2.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。对于非独立恶意代码，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。对于独立恶意代码，自我复制过程就是将自身传播给其他系统的过程。不具有自我复制能力的恶意代码必须借助其他媒介进行传播。传统意义上的病毒是狭义病毒，指同时具有**寄生和传染能力**的恶意代码。**具体类别:(1)**后门: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。因此，获悉后门的人员可以绕过访问控制过程，直接对资源进行访问。**目的**:最初的作用是程序员开发具有鉴别或登录过程的应用程序时，为避免每一次调试程序时都需输入大量鉴别或登录过程所需要的信息，通过后门启动程序的方式来绕过鉴别或登录过程。当程序正式发布时，程序员会删除该后门。后来程序员有意在程序中留下后门，以防止非授权用户的盗用。再后来，某些(尤其是免费的共享)软件故意留下后门，以窃取目标系统的敏感信息**(2)**逻辑炸弹:逻辑炸弹是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，执行这一段恶意代码将导致非常严重的后果，如删除系统中的重要文件和数据,使系统崩溃等。**目的**:最初是程序员用于保护版权而采取的手段，一般不破坏目标系统。后来被用于讹诈和报复非授权用户，会对系统造成破坏**(3)**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.**目的:**大多在于扫描系统，取得目标系统的一些状态信息，以更好地改进软件产品**(4)**特洛伊木马:是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。**目的:**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(RemoteAccessTrojan)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**(5)**病毒:这里的病毒是狭义病毒，即传统意义上的病毒，指那种既具有自我复制能力，又必须寄生在其他程序(或文件)中的恶意代码。它和陷阱门,逻辑炸弹的最大不同在于自我复制能力。通常情况下，陷阱门,逻辑炸弹不会感染其他实用程序,而病毒会自动将自身添加到其他实用程序中**(6)**蠕虫:蠕虫也是一种病毒，但它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，他其实是能完成特定攻击过程的自治软件,它**自动完成以下任务**①查找攻击对象:利用网络侦察技术查找下一个存在漏②入侵目标:利用漏洞入侵目标系统.洞的目标③复制自己:复制自己到被攻击的系统,并运行它**(7)**僵尸(Zombie):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。Zombie主要用于定义恶意代码的功能,并没有涉及该恶意代码的结构和自我复制过程**(8)P2P**系统:P2P程序可以通过HTTP或者其他公共端口穿透防火墙,直接连接到企业的内部网。这种连接如果被利用，就会给组织或者企业带来很大的危害**(9)RootKit:**是指一组能帮助使用者获取系统root权限的工具包，这里的**RootKit**是一种恶意程序,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，具有很好的隐蔽性和潜伏性。一般情况下，RootKit不负责root权限的获取，只是**辅助**恶意代码长期存活于目标系统中.**攻击过程:**攻击者首先通过使用其他远程攻击软件或者安全漏洞来获得系统的最高访问权限,成功侵入系统后,接着需要在目标主机中安装上RootKit,完成远程命令和操作之后,RootKit会将自身和其他攻击进程等相关文件都隐藏起来，并清除系统日志中的有关信息，这样能够保证指定的恶意程序能够长期运行从而持续性窃取机密信息。**用户级RootKit**侵入系统通常是通过修改普通用户或者管理员执行的程序来实现的，这种方法比较容易实现，但同时隐蔽性不够高，容易暴露;**核心级RootKit**一般是侵入操作系统内核，伪装成内核的一部分来进行隐藏和创建后门。**恶意代码攻击流程：(1)**寻找目标**(2)**将自身保存在目标之中**(3)**触发目标系统中的恶意代码执行**(4)**让自身长期存活于目标系统之中(静态:文件,启动项文件;动态:进程,服务,端口)**恶意代码攻击技术:1)**代码注入技术**2)**缓冲区溢出攻击技术**3)**三线程技术(主线程,监视线程和守护线程)**4)**端口复用技术**5)**端口反向连接技术.**恶意代码生存技术：1)**反跟踪技术(静态(分块加密,装载到不同内存;伪指令使代码变形)&动态(破坏单步中断,断点中断或者破坏调试工具的运行环境))**2)**加密,加壳技术**3)**变形技术。**恶意代码长期存在的原因:(1)**利益驱使**(2)**系统和应用软件存在漏洞。在此讨论的计算机病毒是指狭义病毒,即同时具有寄生性和感染性的恶意代码**分类(1)**引导型病毒(读写操作时传播)**(2)**文件型病毒(感染可执行文件)(如感染Windows系统的PE病毒和感染Linux系统的ELF病毒)**(3)**混合型病毒(1+2)**(4)**变形病毒(以上4种存活率低)**(5)**脚本病毒**(6)**宏病毒。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,故反病毒软件难于区分是正常修改还是病毒感染文件**病毒的特性(1)**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(根本属性)**(2)**非授权性**(3)**潜伏性**(4)**可触发性**(5)**破坏性(破坏文件或数据,扰乱系统正常工作的特性,最终目的:获取经济利益)**病毒的结构：(1)**引导模块:引导模块首先将病毒代码引导到内存中的适当位置,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。**(2)**感染模块(是病毒最**核心,**最**关键**的代码):寻找要感染的目标文件,判断该文件是否已经被感染了(通过判断该文件是否被标上了感染标志)如果没有被感染,则进行感染,并标上感染标志**(3)**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**(4)**破坏模块:完成具体的破坏作用,由病毒编写者的目的决定。**(3)常见恶意代码Eg:(1)**脚本病毒:VBScript (windows)JavaScript(Linux)可以是独立的文件(比如VBS文件),也可以附加在其他非可执行文件之中，或者同时以这两种方式存在.Eg:**“**欢乐时光**”(2)**宏病毒:感染Office等文档的一类病毒**(3)**浏览器恶意代码(脚本语言编写)**(4)**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。避免这种病毒一个有效的方法是“关闭自动播放”**(5)**PE病毒:感染PE格式文件(\*.exe,\*.dll,\*.ocx)的Windows病毒;感染模块步骤(1.判断是否PE,2.判断是否感染,3.添加病毒,4.修改入口指针,5.根据新文件实际情况修改一些信息) **(4)**网络蠕虫(不需要或很少需要人为干预)网络蠕虫自动实现扫描,入侵,感染目标等攻击的全过程,通过网络从一个节点传播到另一个节点,代替攻击者实现一序列的攻击过程。**组成:侦察功能模块(**扫描,探测有用信息:主机活动状态,开放端口**),攻击功能模块(**侵入系统获取信息…**),通信功能模块(**发给特定用户或与制作者通信**)**;更高级的蠕虫具有**命令接口模块(**提供接口手工控制**)**和**数据库支持模块(**实现协同操作和数据存储**)**。**传播：**(1)利用系统漏洞主动传播(2)利用电子邮件系统传播(3)通过局域网传播(nimda)(4)通过即时工具(qq)传播(5)多种方式组合传播Eg:(1)莫里斯蠕虫(黑客从此真正变黑)(2)雷曼蠕虫(3)CodeRed蠕虫(4)Nimda蠕虫(5)SQLSnake蠕虫(6)“冲击波”(WORM\_MSBlast.A)(7)震荡波(Sasser)**木马：**一种隐藏在目标系统中的恶意程序,常用于绕过系统的正常访问控制机制,以获得目标系统的敏感信息或直接控制目标系统。木马一般采用客户/服务器结构,其中一个作为控制端,存放在攻击的电脑中,由攻击者直接控制;另一个是被控制端,被植入并隐藏在被攻击的系统中。木马和后门具有类似的功能，但其功能更强大,且一般以**独立程序**的形式存在。大部分的木马不会自我繁殖,也并不“刻意”地去感染其他文件,属于一种独立的恶意代码。它通过将自身伪装为正常程序吸引用户下载执行,向施种木马者提供打开被种主机的门户,使施种者可以任意毁坏,窃取被种者的文件,甚至远程操控被种主机。(服务端/客户端)最关键特性是**隐蔽性**.**反弹端口型木马:**客户端被植入到目标系统,而服务端在攻击者的电脑中运行，木马客户端运行后主动连接服务端,而由内网到外网的连接是不会被防火墙封堵的.**隐藏和伪装方式(1)**绑定到程序中**(2)**隐藏在配置文件或注册表中**(3)**伪装在普通文件中**常见的木马:**网游木马;网银木马;下载类;代理类;FTP木马;通讯软件类;网页点击类;攻击型的木马。**恶意代码检测与分析技术：(1)**技术模块:从恶意代码中搜集,提取有用数据(比如特征码)供分析模块分析使用**(2)**分析模块:根据这些数据(代码的静态结构,代码的静态结构,与操作系统的交互行为)建模,比较来判断一个程序是否符合某个或者某类恶意代码的特征,从而判断该程序是否为恶意代码。**恶意代码静态分析方法：**指不实际运行恶意程序，只是通过反汇编、反编译等技术来查看代码进行分析1)基于特征码检测(误报率低漏报率高,滞后)2)基于代码语义检测3)启发式扫描方法(阈值)。**恶意代码动态分析方法：**在代码运行时，通过监视程序的行为,比较运行环境的变化来进行检测与分析。**1)**系统监控法(文件监控,进程监控,网络监控,注册表监控)**2)**动态跟踪法：基于用户态的行为,内核态的行为,指令模拟器的行为的监测技术。**恶意代码分类方法:1)**基于相似性计算的分类方法**2)**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)1)**提高人员的安全防范意识和水平**2)**建立完善的防护系统**3)**对系统要经常性的维护和升级**4)**定期对重要的资料进行备份**5)**正确处理受到恶意活动代码攻击的系统**第13章内容安全技术内容**:“信息”和“内容”的概念等价,均指与具体表达形式,编码无关的知识、事物、数据等含义,相同的信息或内容分别可以有多种表达形式或编码。在一些特别的场合具有区别，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”**.也可以认为**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**内容安全**:内容的复制,传播和流动得到人们预期的控制和监测。**内容定义三方面**:内容与信息的细微差别(见**内容**);当前国际上将数字视频、音频和电子出版物等称为数字内容;一些文献中的“内容”专指应用层或应用中的数据和消息。**内容安全四需求**：**①数字版权侵权及其控制**(影视和音乐)对数字版权的侵权管制仅仅依靠非技术手段是不够的,数字内容制作企业,内容制作者及管理部门也迫切需要有遏制版权侵权的技术手段**②不良内容传播及其控制**:不良内容的**肆意传播**是另外一个与内容相关的安全问题,在各种动机的驱动下,造成了不良内容大量传播,垃圾邮件泛滥的情况**③敏感内容泄露及其控制**:敏感信息主要包括保密文件和与知识产权相关的资料等,为了制约这类现象,信息安全的管理者希望根据工作人员对外传输或接收的内容对网络通信进行控制**④内容伪造及其控制**:人们需要能够核实数字内容的真伪,并且这种核实也能针对普通数字内容进行,而不依赖于这个内容曾经被数字签名过.**内容安全技术的主动/被动**:**主动内容安全技术**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**:与内容及其应用特性相关的所有信息安全技术，包括数字版权保护,数字水印,多媒体加密,内容取证,内容过滤和监控,垃圾邮件防范,网络敏感内容搜索,舆情分析与控制,信息泄露防范等.**狭义内容安全技术**: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,如网络多媒体内容的非授权散布监控,内容过滤和监控,垃圾邮件防范,网络敏感内容搜索,舆情分析与监测等.**文本过滤主要方法**：**①基于关键字的过滤方法**:早期常用,根据事先编制的**不良文本关键字词库**以及比较简单的布尔逻辑匹配运算,认定匹配**超过一定阈值**的文本为不良文本并过滤,**不足**:很难建立完整的不良文本关键字词库;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**②基于分级标签过滤方法**:通过对不同的网页根据内容赋予不同的级别以实现过滤,可分为普通级,一般限制级,严格限制级,**不足**:网络分级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;分级应根据不同年龄有不同的约束内容**③基于地址库过滤方法**:分为IP地址过滤(**封锁指定网站的IP地址**),URL过滤(**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**)以及IP和URL相结合的过滤(大部分不良信息使用IP过滤,少部分不良信息使用URL过滤)**不足**:新增信息多难以维护**④基于内容的动态过滤法**:进一步根据文本的具体内容来判断指定文本的具体类别属性(K近邻法,贝叶斯方法,神经网络算法,潜在语义索引法) 文本的表示形式具体化,通过指定的过滤算法划分类别属性,过滤。**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。**话题相关定义**:**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,可以简单地将话题理解为若干关于同一事件的报道。**话题自动发现流程①信息采集**: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;**②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;**③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;**④文本向量化**: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,然后将各词的文档词频统计值和逆文档词频统计值运用**TFIDF**公式转换为一个权重值,用以表示文本在这个词语代表的维度上的值,进而将文本表示为一组关键词及其词频为权重的空间向量;**⑤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;**⑥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,s并结合刊载源的级别,传播力,影响力来衡量话题的重要程度，综合两者共同表征报道和话题的热度。**网络安全分级监管**:**①信息内容分级标准**:是整个信息内容主动监管系统的基础，包括内容分级的词汇表,分级标记和分级操作方法;**②分级信息的发布**:信息的分级标记体现了发布方对信息内容分级处理的责任,对标记信息自身需要采取保护措施,防止标记信息被篡改;**③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**:未经授权的访问,复制,发行具有知识产权的数字产品使得数字媒体业遭受了巨大的损失。如何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，成为十分迫切的研究课题。**数字多媒体内容安全面临的问题**:①如何鉴别一个数字媒体作品的创建者②如何确定数字媒体作品创建者的版权声明③如何公证一个数字作品的签名与版权声明④如何控制用户访问数字媒体作品的权限。数字权益管理(DRM)技术在这种背景下应运而生，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,并且结合了新的商业模式为数字媒体业增加了新的机会。