**信息安全概论复习提纲**

1. **绪论**
2. **信息安全的六个属性**

机密性、完整性、可用性、非否认性、真实性、可控性（前三者为经典CIA模型）

机密性：能够确保敏感或机密数据的传输和存储不遭受未授权的浏览，甚至可以做到不暴露保密通信的事实。

完整性：能够保障被传输、接受或存储的数据是完整的和未被篡改的，在被篡改的情况下能够发现篡改的事实或者篡改的设置。

可用性：即在突发事件下，依然能够保障数据和服务的正常使用。

非否认性：能够保证信息系统的操作者或信息的处理者不能否认其行为或者处理结果，这可以防止参与某次操作或通信的一方事后否认该事件曾发生过。

真实性：真实性也称可认证性，能够确保实体身份或信息、信息来源的真实性。

可控性：能够保证掌握和控制信息与信息系统的基本情况，可对信息和信息系统的使用实施可靠的授权、审计、责任认定、传播源追踪和监管等控制。

1. **从多个角度看待信息安全问题**

个人：隐私保护、公害事件

企事业单位：知识产权保护、工作效率保障、不正当竞争

军队、军工、涉密单位：失泄密、安全保密的技术强化

运营商：网络运行质量、网络带宽占用（P2P流量控制）、大规模安全事件（DDOS、大规模木马病毒传播）、新商业模式冲击（非法VOIP、带宽私接）

地方政府机关：敏感信息泄露、失泄密、网站篡改、与地方相关的网络舆情

职能机关：案件侦破、网上反恐、情报收集、社会化管理

国家层面：基础网络和重要信息系统的可用性、网上舆情监控与引导、失泄密问题、巩固政权、军事对抗、外交对抗、国际斗争

1. **威胁、脆弱点和控制**
2. 信息安全威胁(threat)：指某人、物、事件、方法或概念等因素对某信息资源或系统的安全使用可能造成的危害。包括信息泄露、篡改、重放、假冒、否认、非授权使用、网络与系统攻击、恶意代码、灾害故障与人为破坏。

其他分类：暴露、欺骗、打扰、占用；被动攻击、主动攻击；截取、中断、篡改、伪造。

1. 脆弱点（Vulnerability），即缺陷。
2. 控制（control），一些动作、装置、程序或技术，消除或减少脆弱点。

三者关系：通过控制脆弱点来阻止威胁。

控制：保护CIA；消除威胁或者关闭脆弱点；风险：预防、阻止、转移、检测、恢复。

1. **信息安全模型**
2. PDR系列模型：

P2DR：策略：（Policy），保护（Protection），检测（Detection），响应（Response）

PDR2 ：保护（Protect），检测（Detect），反应（React）和恢复（Restore）

1. 信息安全系统综合模型

攻击者能做的事：攻击地点、数据截获、消息收发、利用漏洞和疏忽、分析和计算

攻击者有困难的事：数字猜测、破解密码、推知私钥、越权访问、截获安全信道

信息安全技术的主要目标归纳：在不影响正常业务和通信的情况下，利用攻击者有困难的事去制约攻击者，使攻击者能够做到的事情不能构成信息安全威胁。

1. **密码技术**
2. **密码分析/攻击种类及含义**
3. 唯密文攻击：分析者有一个或更多的用同一个密钥加密的密文；
4. 已知明文攻击：除了待破解的密文，分析者还有一些明文和用同一密钥加密的对应密文。
5. 选择明文攻击：即分析者可得到所需要的任何明文对应的密文，这些密文和待破解的密文是用同一密钥加密的。
6. 选择密文攻击：分析者可得到所需要的这些密文对应的明文，这些密文和待破解的密文是用同一密钥加密的，获得密钥是分析者的主要目的。
7. **代换密码**

凯撒密码、移位密码、仿射密码（密钥311种）、Vigenére 密码（26的m次方）、轮转密码机、弗纳姆密码

置换密码：将报文中的字母重新排序，产生混淆，也称为排列（permutation）。

破译方法：置换更安全；计算字母出现频率: 判断是否列置换；分割成列：找出密文中相邻的列，以及各列的结尾位置；滑动比较；扩大比较（其他列）。

1. **香农提出的“优质”密码特征**

1.加密、解密的工作量应该由所要求的安全程度来决定

2.密钥集合和加密算法不应该过于复杂

3.执行过程应该尽量简单

4.密码中的差错不应该具有传播性，也不应该影响报文中的其他信息

5.加密后的文本大小不应该比原始报文更大

**四、混淆和扩散**

混淆性：明文中的字符变化时，截取者不能预知密文会有何变化

扩散性：把明文信息扩散到整个密文中去；截获者需要获得很多密文才能去推测算法。

1. **对称和非对称加密体制**
2. 对称加密体制：1.加密解密采用同一密钥；2.解密算法和加密算法密切相关；3.可用于鉴别；4.典型算法：DES、AES、IDEA、RC5；5.带来的问题：密钥分配——n个用户两两通话需要n\*(n-1)/2个密钥；6.密钥数量按用户数的平方增长；7.需要密钥分配手段。
3. 非对称加密体制：1.公钥、私钥；2.私钥需要保密3.典型算法：DH、RSA、椭圆曲线…

DES:明文分组：64比特；密文分组：64比特；密钥：64比特，8位校验位，有效位56比特；轮数：16；轮密钥：48比特。

RSA:两个密钥：d, e； 分别用于加密和解密可以互换P=E（D（P）=D（E（P））；加密Pemod n对Pe对因式分解还原明文困难；解密（Pe）d mod n =p。

1. **数字签名**

性质：不可伪造、必须真实、不可改变、不可重用。

1. **标识与认证技术**

**一、实体、主体与客体**

实体：抽象地指代一个程序、设备、系统或用户等；

主体：业务操作发起者；客体：业务操作对象。

1. **系统实体标识**

文件、数据库、程序、主机标识、网络资源标识、连接标识

口令猜测：规律性较强，长度较短，预设口令（易被猜测）

规律性较强，长度较短，预设口令（对策）

猜测方法：尝试所有可能的口令（穷举法）；尝试许多很可能的口令；尝试一个用户可能的口令；查找系统的口令表；问用户。

**三、挑战-响应技术**

线路窃听

威胁：在网络和通信线路上截获口令；对策：口令不在网上直接传输（加密连接）

重放攻击

威胁：截获合法用户通信用户全部数据，冒用重放；对策：使用非重复值（NRV）

对验证方攻击

威胁：入侵验证方获取口令信息；对策：妥善保管、Windows SAM加密保存

**四、Kerberos认证系统**

KERBEROS利用票据进行安全协议所需的通信。在声称者C和验证者V开始通信前，C和认证服务器S先执行一个协议，随后V才能验证C。三个步骤：认证服务器交换、票据颁发服务交换、客户/服务器交换。

1. **基于公钥密码技术的认证**

不需要在线服务器，只要离线服务器

X.509：第一次通信：A到B，第二次通信：B到A（第三次通信：A到C）

1. **生物认证**

指纹：可欺骗；视网膜：不舒服，非独一无二，可克服更易接受；手型：非独有；声音：重放，模仿；相貌：有难度；实施因素：代价、用户接受程度；隐私考虑

1. **PKI技术（公钥基础设施）**

基本元素：数字证书

一种定义：以公钥加密为基础，创建、管理、存储、分发和撤销证书所需要的一组硬件、软件、人、策略和过程

PKI组成：

认证和注册机构、证书管理、密钥管理、非否认服务、系统间认证、客户端软件。

1. **授权和访问控制策略的概念**
2. **自主访问控制**

每个客体有且只有一个属主；客体属主决定该客体的保护策略；系统决定某主体能否以某种方式访问某客体的依据是：是否存在相应属主的授权。

1. HRU模型

1.Harrison，Ruzzo，Ullman提出

2.基于访问控制矩阵，基本的自主访问控制模型。当前授权状态Q=（S，Q，M）

3.每个主体同时也是对象。

4.基于命令(command)，其中每条命令含有条件(condition)和原语操作(primitive operation)。

结论：

(1) 在模型化系统中，当每个命令都被限制为一个单独的操作时，我们就可能判断出一个给定的主体是否能够获得对一个对象的特殊权限。

(2)如果不把每条命令限制为单一操作，就不总能判定是否能够将给定的权限授予一个给定的保护系统。

（二）取予模型

矩阵模型没有自然表达权限传递关系；有些模型采用图结构： take-grant，Action-Entity

Jones提出取予模型；系统状态采用(S,O,G)表示；四种权限：读写取予；操作原语：取，予，实体创建，取消权限。

1. **强制访问控制**
2. 、BLP模型

主体可信度（Clearance）安全属性：

1. 反映主体的最高级别2.主体级别可以改变，不会高于可信度级别

存取权限：只读、添加、执行、读/写

操作：

Get/Release、Give/Resind、Create/Delete、改变主/客体安全级别

策略：简单安全（下读）星策略（上写）自主安全

1. 、BIBA模型

“完整性”模型

完整性级别（Integrity Level）

L（C，S）

Critical>Very Important>Important

操作

Modify、Invoke、Observe、Execute

非自主策略：上读下写

自主安全策略：ACL和环

1. **基于角色的访问控制**
2. 核心RBAC模型（CORE RBAC）

五个集合：用户集对象级操作级权限级角色集会话集

四类操作：用户分配、特权分配、用户会话、激活/去活角色

1. 有角色继承的RBAC模型（Hierarchical RBAC）

建立在Core RBAC基础上、增加角色继承（RH）操作、受限继承、多重继承

1. 有约束的RBAC模型（Constraint RBAC）

通过提供职责分离机制进一步扩展了Hierarchical RBAC、静态与动态职责分离

1. **PMI技术**

支持授权服务的安全基础设施

由属性证书、属性权威机构、属性证书库等部件构成

实现权限和证书的产生、管理、存储、分发和撤销

属性证书、属性权威机构、PMI模型（通用模型控制模型传递模型角色模型）

1. **信息隐藏技术**

**一、含义、基本原理**

含义：起源于古代就出现的隐写术，密码学隐藏保密的内容，隐写隐藏保密的事实，是相互补充的关系。

基本原理：1.在可以公开的数字内容中嵌入并提取要隐藏的信息；

1. 只要能够嵌入能够代表0和1的信息编码，即可以隐藏信息；
2. 多媒体数据的特点之一：人眼对部分变化不敏感。
3. **信息隐藏**

位平面替换：

最简单的信息隐藏方法，也是使用最为广泛的替换技术。

黑白图像通常用8个比特来表示每一个像素(Pixel)的明亮程度，即灰阶值(Gray-value)。

彩色图像则用3个字节来分别记录RGB三种颜色的亮度。

将信息嵌入至最低比特，对宿主图像(Cover-image)的图像品质影响最小，其嵌入容量最多为图像文件大小的八分之一。

量化索引调制（基本原理）：QIM的信息隐藏能够消除载体信号对提取算法的干扰，在载体信号尺寸一定的情况下能嵌入较多的数据，信息隐藏的嵌入码率较高，也是较多使用的一类信息隐藏方法，主要适用于水印和隐写。

1. 数字水印
2. 鲁棒：面向数字内容版权保护的信息隐藏技术

需求：感知透明性、鲁棒性、安全性、盲性、嵌入码率

分类：时空域和变换域。按嵌入方法分类

1. 脆弱：保护数据完整性和真实性的技术

主要性能：篡改敏感性、可定位性、感知透明性、半脆弱性、盲性

分类：基于密码、基于信号处理

1. 隐蔽通道

将一些信息传送给不该接受这些信息的人，传送信息的通道方式是隐蔽的——隐蔽通道。

1. **网络与系统攻击技术**
2. **一般黑客攻击的三部曲**：攻击前奏（踩点扫描查点）、实施攻击、巩固控制（日志清理、安装后门、安装内核套件）。
3. **网络扫描**

种类：端口扫描及服务探测、后门探测、拒绝服务漏洞探测、本地权限提升漏洞探测、远程漏洞探测、火墙漏洞探测、敏感信息漏洞探测。

工具：一些扫描软件系统

口令截收和欺骗——网络窃听；非技术手段——社会工程学

1. **拒绝服务攻击**

四类：利用系统漏洞、利用网络协议、利用合理服务请求、分布式拒绝服务攻击

原理：发送大量的（精心构造的）服务或操作请求，这是手段，目的则为使对方无法正常提供服务。

1. **分布式拒绝服务攻击**

原理：使用多台计算机（肉鸡、傀儡、僵尸网络）结构：控制端、代理端

1. **缓冲区溢出攻击**

原理：利用堆栈结构，通过在以上缓冲区写入超过预定长度的数据造成所谓的溢出。可以针对数据段和堆栈段

1. **网络与系统安全防护与应急相应技术**
2. **防火墙**

功能：过滤不安全的服务和通信；禁止未授权用户访问内部网络；控制对内网的访问方式；记录相关的访问事件，提供信息统计、预警和审计功能。

种类：包过滤防火墙、代理网关、包检查型防火墙、混合型防火墙

**二、入侵检测技术**

（一）功能：监视用户和系统活动、审计系统配置中存在的弱点和错误配置、评估关键系统和数据文件的完整性、识别系统活动中存在的已攻击模式、通过统计分析识别不正常活动、

管理审计跟踪，当用户违反策略或正常活动时，给与警告、纠正系统配置错误、安装、运行陷阱以记录入侵者的相关信息。

1. 基于主机和基于网络
2. 滥用检测和异常检测
3. **蜜罐技术**

概念：一类对攻击、攻击者信息的收集技术

分类：应用型和研究型、低交互型和高交互型、真实型和虚拟型、蜜罐网络

原理：伪装和引入、信息控制、数据捕获和分析

雾计算

1. **安全审计与责任认定技术**
2. **安全审计的概念和作用**

日志：日志记录可以由任何系统或应用产生，记录了这些系统或应用的事件和统计信息，反映了它们的使用情况和性能情况。审计系统一般是专门的系统或子系统，输入可以是日志也可以是相应事件的直接报告，一边生成审计记录一边记录所定义的审计事件的发生情况，比普通日志文件更安全更结构化，格式更统一。

事件记录：当审计事件发生时，由审计系统用审计日志记录相关的信息。

记录分析：对审计记录的分析有助于向用户提供更精简、更合理的信息，也有助于用户发现信息系统存在的攻击事件和安全问题。

1. **事件分析与追踪**

检查进程、检查通信连接、检查登录用户、分析日志、文件系统分析、地址追踪（基于主机的追踪、基于网络的追踪）、假冒地址追踪（逆向洪水、入口调试、其他方法）

1. **电子证据的特性**

电子证据是自计算机技术出现及发展以后产生的一种新型证据类型，是指以存储的电子化信息资料来证明案件真实情况的电子物品或电子记录，具有高技术性、多样性、客观实时性、易破坏性。

1. **电子取证过程与技术**

取证准备、取证、证据保管

1. **主机系统安全技术**
2. **操作系统安全技术**
3. 内存和进程分离：物理、时间、逻辑、密码分离，内存管理中划分为操作系统空间和用户程序空间，需要CPU分时调度。

上下文转换：操作系统在用户间转移控制时的准备工作：地址改变

基址/范围寄存器：存放下界限制

分段式:将程序分为几块，每一块是一个逻辑单元，表现为一组有关联的代码或数据

分页式：用户程序的地址空间被划分成若干大小相等的区域---页；内存空间也分成与页相同大小的存储块。

段页式：两者结合

1. 特权管理（setuid、特权分离）

特权操作：对系统安全较为重要的操作

最小特权原则和特权分离原则

1. 内核安全技术：在内核设置安全模块来实施基本安全操作。安全内核负责在硬件、操作系统、计算系统的其他部分之间提供安全接口，安全内核一般包含在操作系统内核中。

**二、数据库安全技术**

推理：一种通过非敏感数据推断或推导敏感数据的方法。

事务定义：DBMS一般通过SQL向用户提供事务的定义方法，用户可以将一个操作系列定义为一个事务，由DBMS负责执行。

事务执行和提交：DBMS不是简单地使事务进入执行状态，而一般采用所谓两阶段提交地方法，第一阶段事务中包含的操作在缓存中被预先执行，在这一阶段任何操作结果都不会真正影响数据库，但有可能此时DBMS不允许其他操作修改相关数据库表；仅仅在第一阶段操作全部成功的情况下，DBMS才通过提交事务的操作永久更新数据库。

事务回滚：当第一阶段的操作失败后，或者事务提交本身失败，DBMS需要使整个数据库回滚到事务执行前的状态。

1. **可信计算技术：**通过设置TPM/TCM并实现TSS/TSM与TNC，保证了系统操作和网络连接的可信性。
2. **网络系统安全技术**
3. **OSI安全体系结构**
4. 五类安全服务：鉴别服务、访问控制、数据完整、数据保密、不可抵赖
5. 八种特定安全机制：公证、路由控制、业务流填充、数据完整性、访问控制、数字签名、鉴别交换、加密
6. 四类不同层次安全性

应用级安全：OSI安全组件通过各类信息安全技术保护应用层数据安全实现的安全性被称为应用级安全。如安全电子邮件

端系统级安全：应用层以下网络层以上，如电子购物系统

网络级安全：OSI安全体系结构中在网络层提供安全功能能够实现网络到网络之间的安全通信获得网络级安全。如VPN

链路级安全：在链路层保护通信帧的内容。如大型网络通信中心。

1. **SSL**

功能：TLS记录协议用于对传输、接收的数据或消息进行处理

基本原理（过程）：①上层数据分块，(块也被称为目录)；

② 压缩分块数据；

③ 计算分块的杂凑值或MAC值，附在分块后；

④ 加密数据分块和MAC值；

⑤ 添加TLS协议头

1. **VPN和IPSEC**

功能：不同区域子网通过公用网进行连接的一种技术，

子网之间用所谓的隧道 (Tunneling)技术通信，全部子网在逻辑上是一个网络，可以进行更方便的管理；VPN隧道通信需要提供相应的安全性，由于连接相对固定，更加适合在网络层提供这类安全。

组成部分：IPSEC在IP层中引入数据认证机制、加密机制和相关的密钥管理，实现了比较全面的网络层安全，包括网络之间的相互验证、加密链路的建立及保密通信等

应用模式：涉及数据保护范围的基本概念、传输模式和隧道模式

1. **SET协议**

解决问题：信息安全问题：买家的账户和购买信息是需要保护、买卖双方需要相互确认对方的身份、卖家和负责支付的电子金融机构之间也存在交互的安全问题

特点：商家不知道用于支付的银行账号、银行不知道客户购买的商品、但两者之间建立了联系。

**第十一章 恶意代码检测与防范技术**

一、**计算机病毒、蠕虫、特洛伊木马各自特性，区别**

计算机病毒：计算机病毒是一种特殊的计算机程序，能够寻找宿主对象，并且依附于宿主，是一类具有传染、隐蔽、破坏等能力的恶意代码。传染性、依附性。

蠕虫：通过网络繁殖，不依附于其他程序，是独立程序。可能只在内存中维持一个活动副本，甚至根本不向硬盘中写入任何信息。一般利用系统漏洞传播。

特洛伊木马：表面上有用的程序或命令过程，但其中包含了一段隐藏的、激活时将执行某种有害功能的代码，可以控制用户计算机系统的程序，并可能造成用户的系统被破坏甚至瘫痪。

位于受害者系统中的恶意程序或攻击的代理。伪装成正常运行的程序。一般不复制。

1. **恶意代码分析检测方法**

分析方法：动态分析静态分析

检测方法：特征代码法、校验和法、行为监测法、软件模拟法、比较法、感染实验法

1. **恶意代码清除方法：**

清除工具

干净地重启(工具盘)-使用清除工具

手动清除

杀进程改注册表或相关配置-删本体-补丁-重启-干净地重启(工具盘)-改注册表或相关配置-删本体-补丁

1. **内容安全技术**
2. **内容和信息的区别**

在信息科技中，“信息”和“内容”的概念是等价的

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。

信息和内容的概念也在一些特别的场合略有区别

内容更具“轮廓性”和“主观性”，即在细节上有些不同的信息可以被认为是相同的内容，不同的人对相同信息的感知也可能不同。

因此一般认为信息更具“细节性”和“客观性”，信息具有自信息、熵、互信息等概念，可以用比特、奈特或哈特等单位衡量它们数量的多少。

在细节并不重要的场合下，内容往往更能反映信息的含义，也可以认为内容是人们可感知的信息或较高层次的信息。

多个信息可以对应一个内容，但信息论研究的信息是客观的，即它一般不认为一个信息可以在主观感知下对应多个含义。

1. **内容安全的概念**

内容安全就是指内容的复制、传播和流动得到人们预期的控制。

1. **文本过滤方法——**基于特征向量匹配（思路，步骤）

对等待过滤文本进行分词并计算词条的权值后，根据特征数据库中的特征向量，可以得到由等待过滤文本在相应特征词上的权值所组成的特征向量(W1’,…,WN’)。

1. **信息安全测评技术**
2. **信息安全测试技术**

测试环境的构造与仿真:传统测试方法依靠构建实际运行环境进行测试，随着运行环境的复杂化，代价越来越高，测试环境仿真技术应运而生，由各类测试仪来实现。例IPSEC测试

有效性测试:用测试的方法检查信息安全产品、系统与他们模块、子系统是否完成了所设计的功能，包括通过测试相应的指标量衡量完成的程度与效果。测试方法包括典型的应用实例或输入数据，包含典型输入数据与边界值的测试用数据为测试序列。

负荷与性能测试:通过输入、下载不同带宽、速率的数据或建立不同数量的通信连接，得到被测产品或系统的数据处理能力指标值及他们之间可能的相互影响情况。如得到最大带宽、吞吐量、最大处理速率等。

攻击测试:利用网络攻击或密码分析手段，检测网络安全设备或密码模块的安全性质（如网络扫描技术），用于测试防火墙、IDS与服务器安全特性。

故障测试:通过测试了解信息安全产品或系统出现故障的可能性、故障环境及故障类型，故障测试结果课反映被测对象的运行稳健性，如错误数据输入。

一致性与兼容性测试:对于信息安全产品、系统或其模块、子系统，检测他们在接口、协议等方面与其他配套产品、系统或模块、子系统的互操作情况，确定他们是否都符合相关的接口、协议设计与规范。

1. **信息安全评估准则**
2. TCSEC（安全等级）：评估计算机系统对敏感信息保护——1983美国国防部和国家标准局（彩虹系列，橙皮书）

七个安全级别：D1、C1、C2、B1、B2、B3、A1

D1 : 无安全性

C1 :开始有安全，基于分离的操作系统安全技术，自主访问控制

C2：处理敏感信息的最低安全级别

B2：开始可信计算基（TCB)

A1: 形式化安全验证

1. 信息技术安全评估准则（ITSEC)——英法德意制定，1991年欧共体标准化委员会发布；适用更多产品、应用和环境；“功能”和“保证”10级功能7级保证
2. 信息安全技术通用评估准则（CC）

TOE、ST、PP；11类安全功能；10类安全保证；7个EAL。

1. **信息安全管理技术**
2. **信息安全计划：**较高层次上确定一个组织涉及信息安全的活动，应明确安全策略、安全需求、计划采用的安全措施、安全责任和规划执行时间表
3. **安全策略：**信息安全规划的核心组成部分，表达了组织的信息安全目的和意图。应明确安全目标、访问主体、访问客体、访问方式。
4. **信息安全风险评估**

风险评估的形式：组织内部自我评估、委托专业机构、上级机关执行检查性评估

风险评估的方法：定性方法、定量方法、定性定量结合

步骤：资产识别与估价、威胁与脆弱性识别、安全防护措施确认、确定风险大小与等级、安全措施建议。

威胁与脆弱性识别：对每一项信息资产进行分析，识别出可能的威胁

估计威胁发生可能性PT：资产吸引力、资产转化为报酬的难易程度、产生威胁的技术含量、利用脆弱点的难易程度。

识别脆弱性，估计被利用的可能性PV——与具体信息系统、组织结构、管理体系、基础平台相关。

1. **《信息安全等级保护管理办法》：**自主保护级、指导保护级、监督保护级、强制保护级、

专控保护级。