# 信息系统面临的安全威胁

1.物理安全威胁：指对系统所用设备的威胁，如自然灾害、电源故障、数据库故障、设备被盗等造成数据丢失或信息泄漏。

2.通信链路安全威胁：指在传输路线上安装窃听器装置或对通信链路进行干扰。

3.网络安全威胁：指由于因特网的开放性、国际性、无安全管理性，对内部网络形成的严重安全威胁。

4.操作系统安全威胁：指操作系统本身的后门或安全陷阱，如木马等。

5.应用系统安全威胁：指网络服务或用户业务系统安全的威胁，包括应用系统自身漏洞，也受到木马的威胁。

6.管理安全威胁：指人员管理和各自安全管理制度。

# 五大类安全服务和实现方式

1.认证与鉴别服务。鉴别参与通信的对等实体和数据源的合法性，认证服务的基本目的，是为了防止其他实体占用和独立操作被认证实体的身份。

2.访问控制服务。访问控制服务决定开放环境中允许使用哪些资源、在什么地方适合被授权访问的过程。在访问控制实例中，访问可以是对一个系统或对系统内部进行。

3.数据保密性服务，对数据提供保护，防止数据未经授权而被泄漏，防止在系统之间交换数据时被截取。主要通过禁止访问和加密机制两种方式实现。

4.数据完整性服务。防止系统之间交换数据，非法修改数据或丢失数据。常见实现方式包括阻止对数据传输媒介访问的机制和探测对数据非授权修改的机制。

5.抗抵赖服务。阻止通信双方否认发送和接收数据的行为，实现方式主要包括数字签名、用户认证、操作日志等技术。

# 安全属性有什么

1.保密性：指系统中的信息必须按照信息拥有者的要求保证一定的秘密性，不会被未经许可的第三方非法窃取。

2.完整性：指系统中的信息应当安全、准确、有效，要求数据不能被非法改动或删除。

3.真实性：指对信息发送者身份的确认，保证信息可信度。

4.不可抵赖性：指保护信息赖以存储的节点、介质、载体等不被盗用或窃取。

# 认证服务有哪些

1.口令和用户名认证，通过客户端和服务器共知的口令进行验证。

2.令牌认证：进行验证的密钥存放在令牌中，常用令牌有安全证书、智能卡等方式。

3.生物识别认证：根据认证者的图像、指纹、气味和声音作为认证依据。

4.相信可靠的第三方建立的认证。

5.环境，如主机地址等

# 访问控制方式有哪些

1.自主访问控制（DAC)。一个拥有一定权限范围的主体可以直接或者间接地把权限授予其他的主体。

2.访问控制列表(ACL)，从资源角度出发，允许某些主体可访问。与自主访问的区别在于：自主访问是给主体赋予权限，访问控制列表为某个资源赋予哪些主体可访问的列表。

3.强制访问控制（MAC)，强制访问控制是为主体和客体划分等级，而且强制所有主体都必须服从这种访问权限的分配。 MAC 一般用在安全级别层次比较多的军事、安全等特殊应用领域中。

4.基于角色的访问控制(RBAC)。用户通过角色与权限进行关联，将用户和权限解耦，一个用户可有多种角色，一个角色可有若干权限，减少了授权管理的复杂性，是面向企业的系统中一种十分有效的访问控制策略。

5.基于任务的访问控制（TBAC）。参与某个任务的相关人员可拥有相应权限，任务灵活配置。常用于OA系统。

# 基于口令的认证方式VS基于公钥的认证方式

1.基于口令的认证方式实现简单，但是由于口令复杂度及管理方面的原因，容易受到认证攻击；而基于公钥的认证方式，由于其密钥机制的复杂性，同时在认证过程中私钥不在网络上传输，因此可以有效防止认证攻击，与基于口令的认证方式比更加安全。

2.基于口令的认证方式中，用户口令为用户和认证服务器共享，没有用户独有的直接私密信息；而基于公钥的认证方式中，可以基于用户私钥对私有数据加密保护。

# 数据库加密方式

加解密API：数据库管理系统提供在SQL语句中调用加解密API，应用可利用这些API构建自己的基础架构，对数据进行加密保护。----------> 灵活性强，但构建和管理复杂

透明加密：安全管理员为数据库敏感字段选择加密方式及密钥强度，应用访问受保护数据时只需要调用口令打开或关闭密钥表，对数据的加密和解密由数据库管理系统自动完成。----------> 管理简单、应用程序无负担，但灵活性差

# 访问控制-基于角色的访问控制策略和可拓展访问控制标记语言(XACML)

基于角色的访问控制策略，指用户通过角色与权限进行关联，将用户和权限解耦，一个用户可有多种角色，一个角色可有若干权限，减少了授权管理的复杂性，是面向企业的系统中一种十分有效的访问控制策略。

1.XACML提供了统一的访问控制策略描述语言，策略表达能力强，可用来描述各种复杂和细粒度的访问控制需求，适合企业复杂业务。

2.XACML的标准性，便于各子系统的协作交互，各子系统或企业业务部门可分布管理访问控制权限，相比之下，需对访问控制权限集中管理的MAC，并不适用于分布式系统。

# 常用安全手段及实现过程

1、对称加密，加密速度快，但密钥强度不高、密钥分发困难，适用于大内容传输；DES、3DES、AES、RC-5、IDEA

发送者利用对称密钥对要发送的数据进行加密，只有拥有正确相同密钥的接收者才能将数据正确解密。

2、非对称加密 - 接收方公钥加密，接收方私钥解密；RSA、ECC

发送者利用接收者的公钥对要发送的数据进行加密，只有拥有对称私钥的接收者才能将数据正确解密。

3、数字信封 - 对称加密和非对称加密的混合使用，发送方将原文用对称密钥加密，将对称密钥以接收方公钥加密的方式发送。接收方接收到数字信封，用自己的私钥解密，取出对称密钥解密。

4、信息摘要。

发送者根据要发送的数据生成信息摘要，并附到数据发送。接收者根据收到的数据重新生成信息摘要，比较两个摘要是否相同，以验证数据完整性。

常用的信息摘要算法：MD5、SHA等。

1. 数字签名。

数字签名，即发送者才能产生的，别人无法伪造的信息，是对信息的发送者身份真实性的证明。

发送者根据要发送的数据和签名算法生成数字签名，将数字签名附到数据发送。接收者接受数据后，对其中的数字签名进行验证，确认其合法性。

特殊的：

发送者根据要发送的数据生成信息摘要，并用发送方的私钥对信息摘要进行加密后附到数据发送。接收者根据收到的数据后，用发送方公钥解密信息摘要，验证发送者身份。同时重新生成信息摘要，比较两个摘要是否相同，以验证数据完整性。

# 授权侵犯的定义、防止授权侵犯和保留用户痕迹的技术手段

授权侵犯：也称为内部攻击，指被授权以某一目的使用某一资源的某人，将此权限用于其他非授权的目的。

防止授权侵犯和保留用户痕迹的技术是抗抵赖框架。

抗抵赖服务目的：提供有关特定事件或行为的证据。

抗抵赖服务对实体进行的行为进行不可否认性保护，比如发送消息、数据库插入记录、请求远程操作等，事件或行为本身以外的其他实体可请求抗抵赖服务。

抗抵赖框架的内容：证据的生成、验证和记录，以及在解决纠纷时随即进行的证据恢复和再次验证。

具体包括四个阶段：

1.证据的生成：请求者请求证据生成者为事件生成证据。卷入事件的实体称为证据实体，其卷入关系由证据建立。根据抗抵赖服务的性质，证据可由证据实体、可信第三方服务一起生成；或单独由第三方服务生成。

2.证据传输、存储和恢复：证据在实体间传输或从存储器取出来或传到存储器。

3.证据验证：证据在 证据使用者 的请求下被 证据验证者 验证。本阶段的目的，在出现纠纷的事件中，让 证据使用者 确信被提供的证据是充分的，可信第三方也可参与，以提供验证该证据的信息。

4.解决纠纷：由仲裁者解决双方纠纷。

# 如何实现数据交互安全性需求

1、引入https协议或采用加密技术对数据加密后传输

2、采用信息摘要技术对重要信息进行完整性验证

3、防火墙系统

4、安全检测

5、网络扫描

# 什么是SQL注入攻击，常见抵御SQL注入攻击方式。

SQL注入攻击是通过把SQL命令插入到web表单，或者输入请求的查询字符串，最终欺骗服务器执行恶意的SQL命令。

常见抵御SQL注入攻击方式有：

1、使用正则表达式

2、使用参数化的过滤性语句

3、检查用户合法输入

4、用户相关数据加密处理

5、存储过程执行查询（不会暴露表结构，安全）

6、使用专业的漏洞扫描工具

（正则-过滤-加密-工具-存储过程-合法输入）