**1.分析信息系统安全框架三维模型中，3 个维度之间的关系是什么。**

**要点：**

（1）说明三个维度：协议层次、信息系统构成单元和安全服务（安全机制）；（2）三者之间关系：安全服务由哪些安全机制参与，每个协议层可以提供哪些安全服务，每个系统单元可以提供哪些安全服务；（3）3个维度是一个整体，在信息系统安全体系结构设计时同时考虑。

**参考答案：**

三个维度：协议层次、信息系统构成单元和安全服务（安全机制）

（1）安全机制并不直接配置于协议层次，也不直接作用于系统构成单元，而是通过提供安全服务来发挥作用，安全机制看作是安全服务的底层支撑。

（2）协议层以OSI的7层模型为参考，选取了可适宜配置安全服务的五个层次。

（3）系统构成单元的划分与选取的五个层次的协议对应。

**2.详细分析信息系统安全体系结构在信息安全中的作用是什么。**

**要点：**

（1）帮助对信息安全问题的系统思考；（2）便于系统设计人员与组织管理者和用户交流沟通；（3）促进安全系统设计的重用；（4）有益于安全系统间的互连、互通、互操作

**参考答案：**

信息系统安全体系结构是与信息系统的体系结构紧密相连的，它是将信息安全要素加入系统体系结构中，描述的是信息系统满足安全需求时各基本要素之间的关系，即：安全要素如何组织才能满足系统安全的需要。

（1）对信息安全问题进行系统思考。安全体系结构可以非形式化、半形式化或形式化语言表达和表述各种安全性和需求，反映系统开发初期的安全决策，对系统安全的设计质量和后期的使用维护有极大的影响。

（2）安全体系结构在安全需求、安全技术方法与管理技术评估标准、相关法律法规之间架起一座桥梁，使得系统设计人员可以方便地与组织管理者和成员用户交流，并依据标准，根据需求，考虑风险，全局地指导安全系统设计和实现。

（3）安全体系结构能够极大地促进安全系统设计的重用。安全体系结构的通用设计模式、组成部件、文档等很容易被用于新的设计中。

（4）对于复杂的网络化分布式的现代信息系统，以一定的安全体系结构和信息安全标准作指导，有利于保障安全系统间的互连、互通、互操作，以及支持各类安全产品在开发研制过程中的认证和版本升级，使其具有更好的安全性、兼容性和扩展性。

**3.ISO 7498-2 标准 5 大类安全服务和 8 类安全机制分别是什么？安全服务和安全机制的关系是什么？**

**安全服务：**

（1）身份认证（Authentication）服务：提供对通信中对等实体和数据来源的认证。

（2）访问控制（Access Control）服务：对资源提供保护，以对抗其非授权使用和操纵。

（3）数据保密（Data Confidentiality）服务：保护信息不被泄露或暴露给未授权的实体。

（4）数据完整性（Data Integrity）服务：对数据提供保护，以对抗未授权的改变、删除和替换。

（5）不可否认性（Non-reputation）服务：防止参与某次通信、交换信息的任何一方事

后否认本次通信或通信内容。

**安全机制：**

（1）加密机制。加密既能为数据提供保密性，也能为通信业务流提供保密性，并且还能为其他机制提供补充。加密机制可配置在多个协议层次中，选择加密机制的原则是根据应用需求来确定。

（2）数字签名机制。可以完成对数据单元的签名工作，也可实现对已有签名的验证工作。数字签名必须具有不可伪造和不可抵赖的特点。

（3）访问控制机制。按实体所拥有的访问权限对指定资源进行访问，对非授权或非法访问应有报警或审计跟踪方法。

（4）数据完整性机制。针对数据单元，发送方产生一个与数据单元相关的附加码，接收方通过对数据单元与附加码的验证，来保护数据完整性。

（5）鉴别交换机制。使用密码技术，由发送方提供，而由接收方验证来实现鉴别。通过特定的“握手”协议防止鉴别“重放”。

（6）通信业务填充机制。业务分析，特别是基于流量的业务分析是攻击通信系统的主要方法之一。通过通信业务填充来提供各种不同级别的保护。

（7）路由选择控制机制。针对数据单元的安全性要求，可以提供安全的路由选择方法。

（8）公证机制。通过第三方机构，实现对通信数据的完整性、原发性、时间和目的地等内容的公证。一般通过数字签名、加密等机制来满足公证机构提供的公证服务。

**关系：**

安全服务与安全机制存在对应关系，可以是一种或多种安全机制来提供某一种安全服务。可参照表2.3针对OSI参考模型进行说明。

**4.参照表 2.2，如何在 1，2，3，4和 7 层实现连接的机密性？**

**要点：**这里的机密性是指数据的保密性。分析各层是否可以提供相关服务，需要描述数据结构。

第1层，即物理层。可以在通信链路上成对的加入保密设备，如：密码机，达到数据物理层机密性。使用方法是在设备的前端加装保密机。

第2层，即数据链路层。链路层进入物理层（如：网卡）之前，对数据进行加密，从而提供数据保密性服务。

第3层，即网络层。该层提供保密服务，即：将该层的所有数据加密。数据传输时，只能到网关。

第4层，即传输层。提供该层保密服务，即：该层的所有数据加密。可以实现端到端的数据安全传输。

第7层，即应用层。提供该层保密性，即：仅对被传输的数据保密。

**5.参照表 2.2，如何在 3、4 和 7 层实现访问控制？**

**要点**：第1层和第2层不能提供访问控制服务，是因为没有相应的设备。而第5层和第6层不提供访问控制，是因为没有必要

第3层，即网络层。 在主机进行路由时，通过访问控制机制，可以控制主机对终端或子网的访问。

第4层，即传输层。访问控制机制能够在每个运输连接端到端的基础之上而被使用，控制对终端应用的访问。如：防火墙对某一个端口的限制。

第7层，即应用层。 访问控制机制能够提供对应用协议和应用进程得的受控访问。如：防火墙对应用层协议的限制。

**6.详细分析 TCP/IP 协议的安全体系结构。**

**要点：**

（1）基于TCP/IP协议的安全体系结构的基本构成和最终表现形式都是TCP/IP协议族中的协议。

（2）是在TCP/IP各层增加安全协议

（3）举例简要说明：增加的安全协议的作用。

（4）存在的问题：各层的安全协议是分开设计的，针对了不同的应用。因此，在安全体系结构设计过程中，进行协议选择时，要避免冲突或矛盾。

**参考答案：**

基于 TCP/IP 协议的安全体系结构是基于协议安全体系结构的重要组成部分，包括提供基本的主机级安全机制的 IPSec，提供 IPsec 安全机制协商的 ISAKMP，提供对 DNS 机制保护的 DNSSec，提供对 MIME 格式封装内容保护的Security/Multipart、安全机制中证书标准 X.509v3，提供传输层安全机制的 TLS 以及其他安全机制。

IP 层的安全协议 IPSec 由身份认证头（AH，Authentication Header）和封装安全负载（ESP，Encapsulating Security Payload）两个协议组成，这两个协议在通信双方的 IP 层进行加密和认证，保证数据完整性、数据源认证和数据机密性。通常，IPSec 协议的实现需要安全关联（SA，Security Association）的支持，SA是通信双方协商的安全参数，如加密算法与密钥、认证算法与密钥、源地址与目的地址等，它由 ISAKMP/Oakley 协议管理和维护。

传 输 层 安 全 协 议（TLS，Transport Layer Security）是 建 立 在 安 全 套 接 层 协 议SSLP，Secure Socket Layer Protocol）基础之上的一个协议，由 TLS 握手协议和 TLS记录协议组成。TLS 握手协议在客户和服务器双方进行保密通信前确定密钥、加密认证算法等安全参数。TLS 记录协议在可靠的传输层（如 TCP）之上提供加密认证等安全服务。

ISAKMP 协议属于应用层协议，通过认证将密钥管理、SA 的协商双方连接起来，为Internet 上的通信提供所需的安全保障。DNSSec 协议是一种通过软件来验证 DNS 数据在互联网传输过程中未被更改的协议，能够验证数据来源，提供数据完整性和抗抵赖性验证。X.509标准基于公钥定义了数字证书标准。数字证书是一段包含用户身份信息、公钥信息以及身份认证机构（CA）数字签名的数据，作为网上信息交流和商务活动的身份证明，在电子交易的各个环节，解决通信双方相互信任问题。

**7.举例说明如何利用实体的思想设计信息系统安全体系结构。**

**要点：**

（1）说明实体的概念与信息系统中实体的划分。

（2）根据要点（1）中的观点举一个工程中的例子。

**参考答案：**

基于实体的信息系统安全体系结构的基本思想是系统功能的实现是由各种实体（包括应用实体、服务实体、系统实体及管理实体）完成的，为了向系统用户提供安全服务，就需要给各种实体分配相应的安全功能。计算机网络的组成结构模型是安全体系结构的基础，计算机网络系统的组成元素统称为实体（Entity），包括所有的资源、用户、进程等具体或抽象的对象。

以分布式数据库系统为例。

在用户端系统内：用户（人）在应用系统中通过应用实体（DBMS）满足需求,应用实体向下调配资源实体与服务实体（存储引擎、存储介质）。用户在分布式各端的登录方式应当保持一致；各实体需保证实体内部的四种安全属性（标识、认证、访问控制、保密及完整性）。 在分布式的情况下，应用实体代理用户身份，服务实体代理提供服务的组织，这二者共同提供端到端数据的保密与完整性。

安全管理需要维持一种独立于各实体的公共认证与访问控制机制，同时需要管理通信资源与网络公共信息的安全调配。这一过程由各系统中的管理实体共同完成。例如在分布式数据库的数据迁移，需要安全管理来维持数据安全。此外，安全管理需设置管理员与安全政策。