**第二章：**

1、填空题

（1）数据保密性可以分为连接保密性、无连接保密性 、选择字段保密性 、通信业务流保密性 。

（2）IPSec 的两种工作模式分别为传输模式和 隧道模式。

（3）基于实体的安全体系结构中，安全属性包括：标识属性 、认证属性 、访问控制属性 、保密及完整性属性 。

（4）安全模型用于准确描述系统在 功能 和 结构上的安全特性，

它反映了一定的 安全策略。

2、选择题（单选和多选）

（1） 4.在 7 层 OSI 网络协议中，以下哪一层不能执行数据来源认证（B ）

A.网络层；B.物理层；C.传输层；D.应用层

（2）在 7 层 OSI 网络协议中，以下哪一层能够执行选择字段保密性（E ）

A.物理层；B.数据链路层；C.网络层；D.传输层；E.应用层

（3）基于实体的安全体系结构中，以下不属于其安全属性的是（B ）

A.标识属性；B.资源属性；C.认证属性；E.访问控制属性；

F.保密及完整性属性

（4）以下不属于认证属性的是（ C ）

A.口令；B.对称密钥；C.加密；D.公钥；E.私钥

（5）实施最小特权时，采用的技术有（ABD）

A.模块化编程；B.结构化设计；C.功能模块的耦合性小；

D.面向资源的访问控制.

3、问答题

（1）为什么从系统设计之初就考虑安全性很重要？

如果不在设计初考虑安全性，会导致有关安全的实现无法很好地集成到系统中，

为了获得所必需的安全性，不得不付出巨大的代价。系统设计时，达到要求的方法

多种多样，有的对安全有利，有的对安全不利。在这种情况下，如果没有一个安全

体系结构来指导系统设计的早期决策，就完全有可能选择了有致命安全缺陷的设计

思路，从而只能采取在系统设计完成后，再添加安全功能的补救措施，但此时可能

需要付出比选择其他方案要多很多倍的代价才能获得相应的安全特性和保证。

1. 如何在系统设计时预设安全问题？

1、预设安全问题不能太特殊或太具体；

2、从抽象层次理解安全问题，而不是针对具体的问题；

3、关注安全策略的制定。一旦改变，可能对系统造成灾难性的影响。

1. 入侵检测系统能否芯片化？为什么？

不能

芯片化带来的是速度快但是内部算法和参数固定，但是入侵检测技术需要随着攻击技术的出现和进化改变策略。

（4）信息系统安全体系结构和信息系统体系结构安全之间的区别

虽然两种都是针对信息系统体系架构的论述，但前者是在系统设计之初就考虑了把安全，将安全机制和策略等用于信息系统，重在整体设计，后者是后增或后装的设计，是系统设计完成后，评估其安全性，安全机制和策略等在系统设计之初不一定被考虑

（5）如何预设安全问题

预设安全问题不能太特殊或太具体；

从抽象层次理解安全问题，而不是针对具体的问题；

关注安全策略的制定。一旦改变，可能对系统造成灾难性的影响。