第一章作业

16337341 朱志儒

1.1 OSI 安全框架是什么?

OSI安全框架提供一种系统的方法来定义安全要求并表示满足这些要求的方法，OSI 文档定义了安全攻击，机制和服务，以及它们之间的关系。

1.2 被动和主动安全威胁的区别是什么?

被动攻击的特性是对传输进行窃听和监测，以及流量分析；主动攻击指对数据流进行修改或伪造数据流，可分为四类：伪装、重播、消息修改和拒绝服务。

1.3 列出并简短地定义被动和主动安全攻击的种类。

被动攻击：信息内容泄露、流量分析；主动攻击：伪装、重播、消息修改和拒绝服务。

1.4 列出并简短定义安全服务的种类。

认证：保证通信的实体是它所声称的实体；

访问控制：阻止对资源的非授权使用；

数据保密性：保护数据免于非授权泄露；

数据完整性：保证收到的数据的确是授权实体所发出的数据；

不可否认性：防止整个或部分通信过程中，任一通信实体进行否认的行为。

1.5 列出并简短地定义安全机制的种类。

特定安全机制：可以并入适当的协议层以提供一些 OSI 安全服务，例如，加密、数字签名、访问控制、数据完整性、认证交换、流量填充、路由控制、公证；

普遍的安全机制：不局限于任何特定的 OSI 安全服务或协议层的机制，例如，可信功能、安全标签、事件检测、安全审计跟踪、安全恢复。