《网络安全技术》作业

第七章作业　传输层安全 TLS

7-1. TLS 在协议栈中处于什么位置？请说明因特网的 TLS 协议提供的安全服务是什么？TLS 由哪些协议组成，这些协议的功能分别是什么。

7-2. 考虑下面的 Web 安全威胁并说明如何通过 SSL 的相应特性来防止每一种威胁？
（1）重放攻击：先前的 SSL 握手消息被重放；
（2）中间人攻击：攻击者在密钥交换过程中，应对服务器时冒充客户端，应对客户端时冒充服务器；
（3）口令窃取：HTTP 数据流或其他应用数据流中传输的口令被窃取；
（4）网站钓鱼：攻击者搭建非法网站冒充合法的 Web 网站欺骗用户访问；
（5）信息篡改：客户端的支付金额等敏感信息在传输过程中被篡改。