

# 网安概论 2

519021910025 钟睿哲

## 1. 什么是 OSI 安全体系结构？

OSI 是一种开放系统互连参考模型的信息安全体系结构，充分体现信息安全层次性和结构性的特点，是一个以防护为主的静态的安全体系结构。

OSI 安全体系结构主要包含三部分内容，安全服务、安全机制、安全攻击。

ISO 对 OSI 规定了五个方面的安全服务：认证、数据保密性、数据完整性、访问控制、非否认服务。

## 2. 被动攻击和主动攻击之间有什么不同？

被动攻击通过截取数据，对保密内容进行泄密与流量分析，主要影响保密性。

主动攻击通过中断、修改、伪造，主要影响可用性、完整性、认证。

## 3. 列出并简要定义被动攻击和主动攻击的分类。

被动攻击的分类：消息内容的泄露、通信量分析。

被动攻击的定义：对信息进行的截取和窃听。

主动攻击的分类：伪装、重放、更改消息内容、拒绝服务。

主动攻击的定义：对数据以及信息的篡改以及伪造。

## 4. 列出并简要定义安全服务和安全机制的分类。

安全服务的定义：一种用来增强数据处理系统安全性和信息传递安全性的措施或服务。

安全服务的分类：认证服务、访问控制服务、数据机密性服务、数据完整性服务、非否认服务。

安全机制的定义：用来检测、防范安全攻击并从中恢复系统的措施。

安全机制的分类：加密机制、数字签名机制、访问控制机制、数据完整性机制、通信业务流填充机制、路由控制机制、认证交换机制、公正机制。

## 5. 网络信息安全的基本要素有哪些？

C.I.A.三要素：

机密性、完整性、可用性。