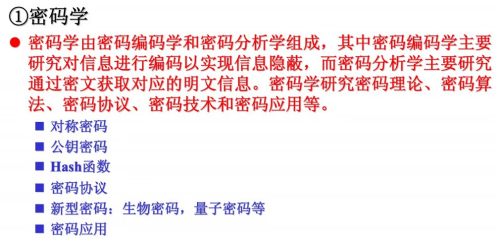
网安导论2021-2022题目（学长回忆版）

### 网络空间的三个基本要素

### descript

### 密码学的具体研究内容（不确定是填空还是简答）

密钥管理？

### 物理安全分为哪些/物理安全的概念

物 理 安 全 又 叫 实 体 安 全 （ Physical Security），是保护计算机设备、设施

（网络及通信线路）免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污

染等）破坏的措施和过程。

物理安全主要包括：环境安全、设备安全 和介质安全。

### sm4是什么算法

2017 年 安 华 金 和 发 布 国 内 首 款 支 持 MySQL 数 据 库 的 透 明 加 密 产 品

（DBCoffer-MySQL TDE）采用国产SM4加密算法，相较传统AES等算法更

安全可靠、合规，最大程度保证数据安全

### 关于网络入侵检测系统，HIDS和NIDS的区分

网络数据传输（NIDS），主机系统行为（HIDS），

### 解释系统安全

确保以电磁信号为主要形式的、在计算机网络化系统进行自动通信、处理和利用的信息内容，在各个物理位置、逻辑区域、存贮和传输介质中，处于动态和静态过程中的机密性、完整性、可用性、可审查性和抗抵赖性的，与人、网络、环境有关的技术安全、结构安全和管理安全的总和。

系统安全包括：

物理安全：计算机与网络的设备硬件自身的安全，就是信息系统硬件的稳定 性运行状态。

运行安全：运行过程中的系统安全，就是信息系统软件的稳定性运行状态。

信息安全（数据安全）：信息自身的安全问题，包括对信息系统中所加工、存储和网络中所传递数据的泄露、仿冒、篡改以及抵赖过程所涉及的安全问题。

### 简述什么是安全的操作系统

安全操作系统是指对所管理的数据与资源提供适当的保护级，有效地控制硬件与软件功能的操作系统。安全操作系统在开发完成后，在正式投入使用之前,一般都要求通过相应的安全评 测。

指操作系统无错误配置、 无漏洞、无后门、无特洛伊木马等，能防止非法用户对计算机资源的非法存取，一般用来表达对操作系统的安全需求。

### 解释一下可信计算这个概念

可信就是可靠加安全

➢首先建立一个信任根。

信任根的可信性由物理安全和管理安全确保。

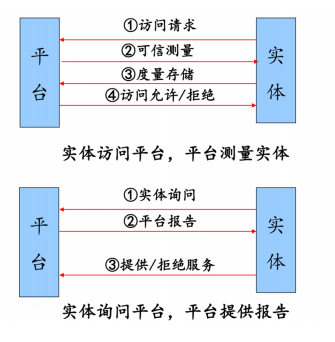
➢再建立一条信任链。

从信任根开始到硬件平台、到操作系统、再到应用，一级认证一级，

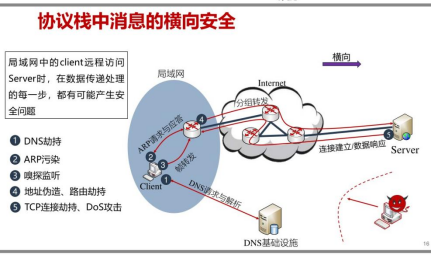
一级信任一级。从而把这种信任扩展到整个计算机系统。

➢可信计算的思想源于社会

### 怎么进行可信计算/可信计算流程、思想



### 协议栈中信息的横向安全

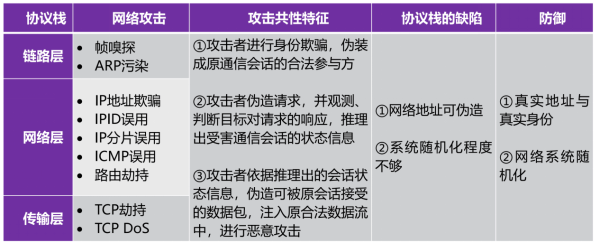


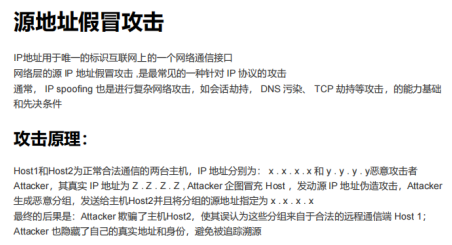
### ARP欺骗5步过程可能遇到哪些攻击



### 网络每一层上面会出现什么样的攻击

协议栈中消息传递的安全，大说说不同层可能发生的网络攻击和安全问题

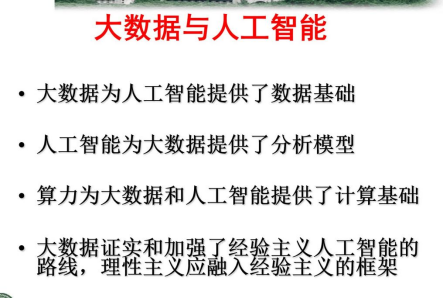




### 数据的几个V特点



### 大数据与人工智能的关系



### 大数据和AI安全的联系（这个不太确定有没有）

数据安全性

-- 指人工智能算法所依赖的数据的安全性

### 路由

路由（routing）是通过互联的网络，把信息从源地址传输到目的地址的活动。

路由安全包括域间路由安全和域内路由安全

### 冗余和容错

➢容错技术是指在一定程度上容忍故障的技术，也称为故障掩盖技术

（Fault Masking）。采用容错技术的系统称为容错系统。

➢容错主要依靠冗余设计来实现，它以增加资源的办法换取可靠性。

➢冗余技术可分为：硬件冗余、软件冗余、信息冗余和时间冗余。

### 密码学研究方向

对称密码；公钥密码；哈希函数；密码协议；新型密码：生物密码、量子密码、混沌密码；密码管理；密码应用。

### 网络安全研究方向

网络安全威胁；通信安全；协议安全；网络防护；入侵检测与态势感知；应急响应与灾难恢复；可信网络；网络安全管理。

### 系统安全研究方向

系统的安全威胁；系统的设备安全；系统的硬件子系统安全；系统的软件子系统安全；访问控制；可信计算；系统安全等级保护；系统安全测评认证；应用信息系统安全。

### 内容安全研究方向

内容安全的威胁；内容的获取；内容的分析与识别；内容安全管理；信息隐藏；隐私保护；内容安全的法律保障。

### 信息对抗研究方向

通信对抗；雷达对抗；光电对抗；计算机网络对抗。

### 简单列举我国网络空间安全的有关法律法规

《中华人民共和国国家安全法》《中华人民共和国密码法》《中华人民共和国电子签名法》《中华人民共和国数据安全法》

《中华人民共和国计算机信息系统安全保护条例》《关键信息基础设施安全保护条例》

《计算机信息网络国际联网安全保护管理办法》

网络安全等级保护制度2.0系列标准

《公安机关互联网安全监督检查规定》

### 网络空间安全对应的四个层面

设备、系统、数据、应用

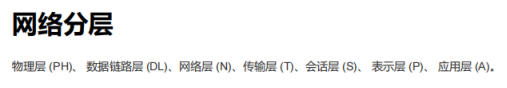
### 应对网络空间安全的手段

法律、管理、技术、自律

### 密码算法的作用

加密、认证

### 计算机的各层极其功能





### 分片攻击分为哪三种

 拒绝服务攻击

 污染攻击

 安全策略逃逸

### IPsec协议：

即Internet协议安全性，是一种开放标准的框架结构，通过对IP协议的分组进行加密和认证，来保护基于IP协议的网络传输

### IPSec的两种安全机制

认证AH、加密ESP

### 工作模式

传输模式、隧道模式

### IDS技术路径

基于特征匹配的ids

基于异常检测的ids

### 常见DOS攻击

计算机网络带宽攻击和连通性攻击

### TLS安全功能：

加密、身份验证、完整性

ARP欺骗与污染

源地址假冒攻击

IP分片攻击原理和分类

网络入侵检测系统

路由安全

拒绝服务攻击

TCP劫持攻击

(开放题)怎样设置密码让黑客不容易猜到/怎样设计密码使得足够安全，而且说明安全的密码有什么特征/比较安全的密码要注意什么

崔老师上课讲得一个生动的例子，大概是设置这样一个密码有什么用

考通信监听问题，如何加密使其更安全

有个开放题，是网络安全在当下的应用（可能和俄乌战争有关系，但我不确定是题目考了这个还是我拿这个举例子