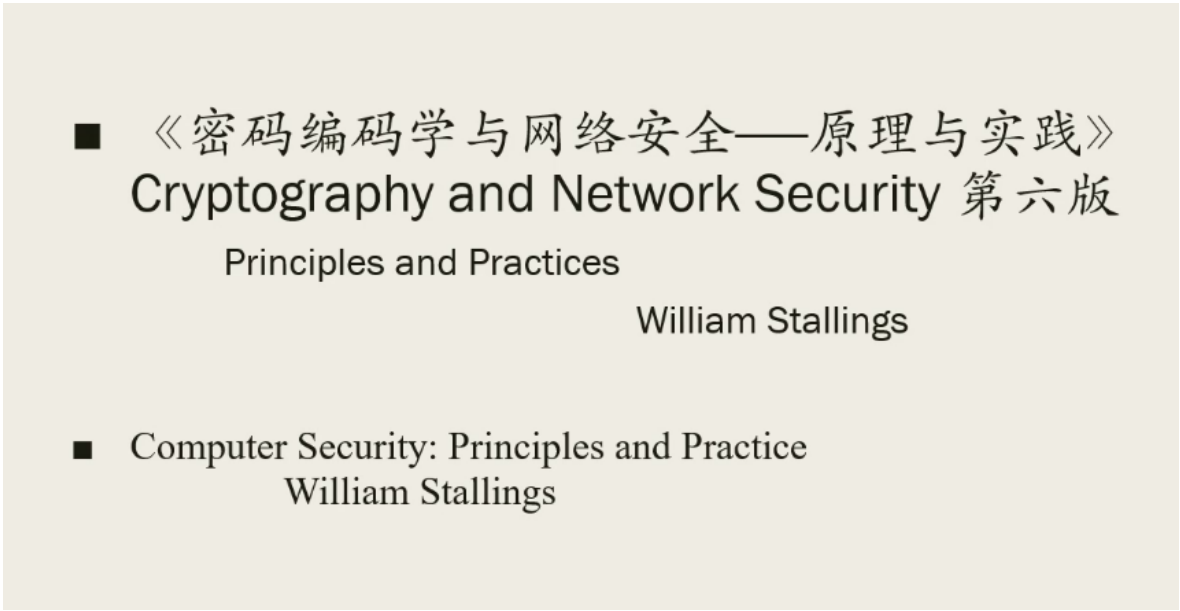
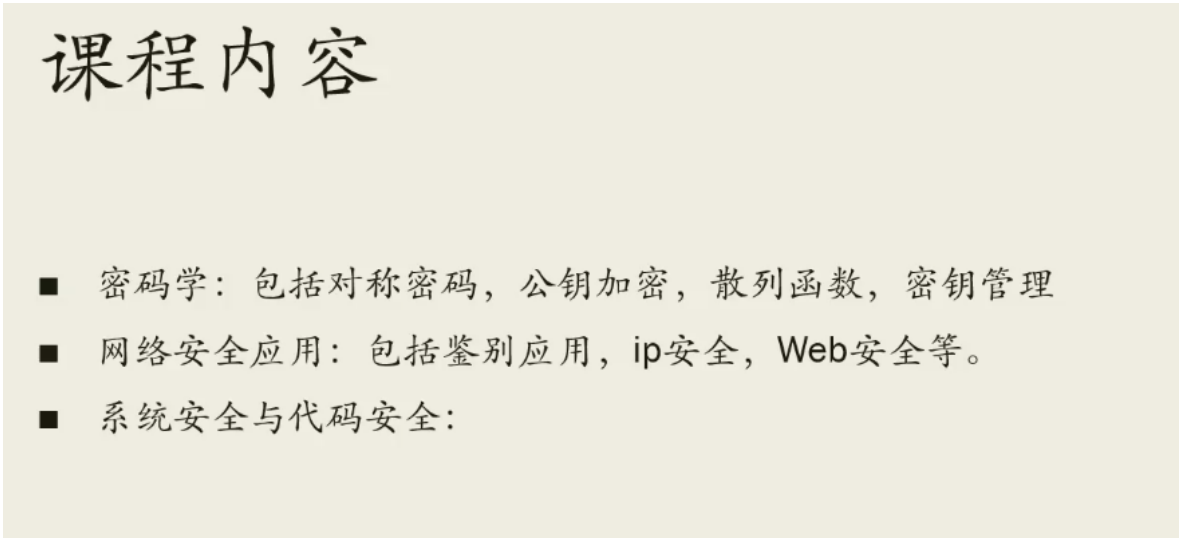
考勤作业





选择15道：30分　填空20分 判断20分

简答25-30分

第一章 网络安全概述

安全威胁

23456——56分

3-CIA

5-五种安全威胁

关键性的安全需求：CIA triad——**考点（选择/判断/填空）**

1 **C：机密性**。对信息资源访问，，开放的限制比如访问控制，加密等

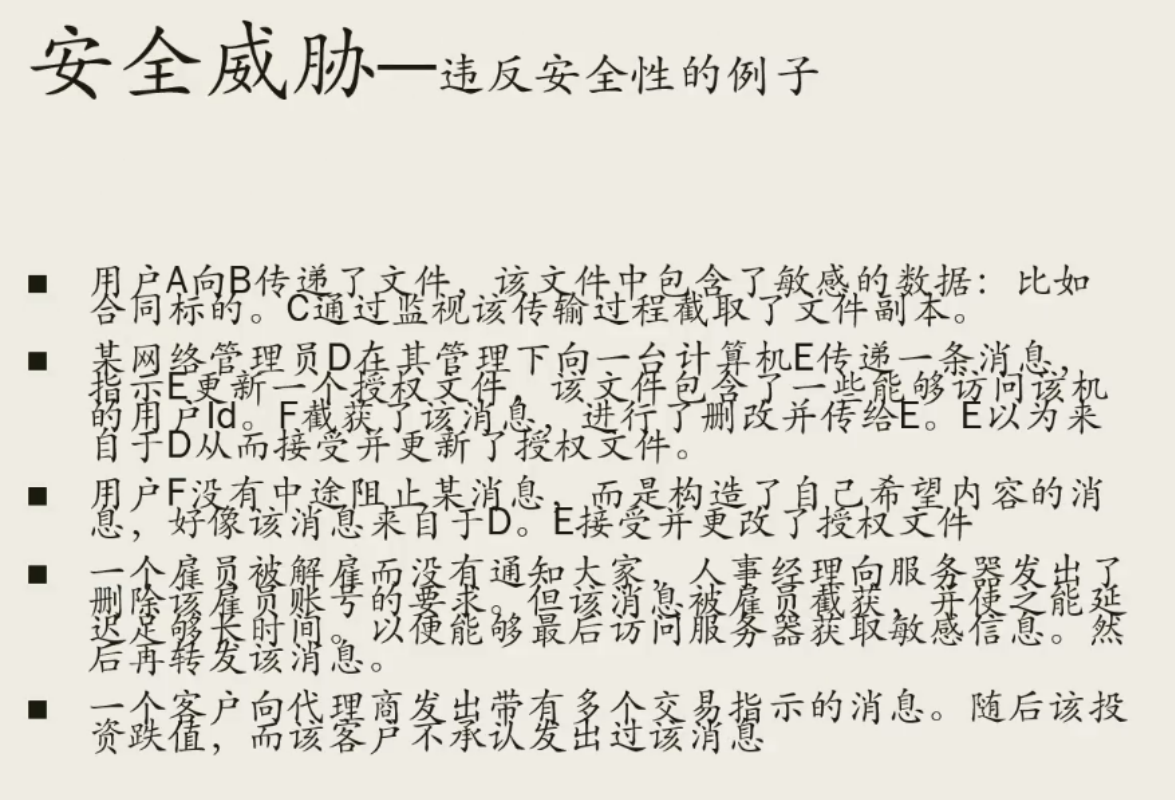
2 **I：完整性**。保证

3 **A：可用性**。合法的访问能够及时有效地得到实施

4 **Authenticity (Authentication)：真实性**。鉴别（认证)还有翻译成可控。指特性(身份)等可验证，可信

5 **Accountability：可审计性/可追溯性**。可说明性指实体行为前唯一性的追踪我们书上的描述是不可否认性(non-repudication)

> 安全威胁：一个客户向代理商发出带有多个交易指示的消息，随后该投资跌值. 而客户不承认发送过该消息

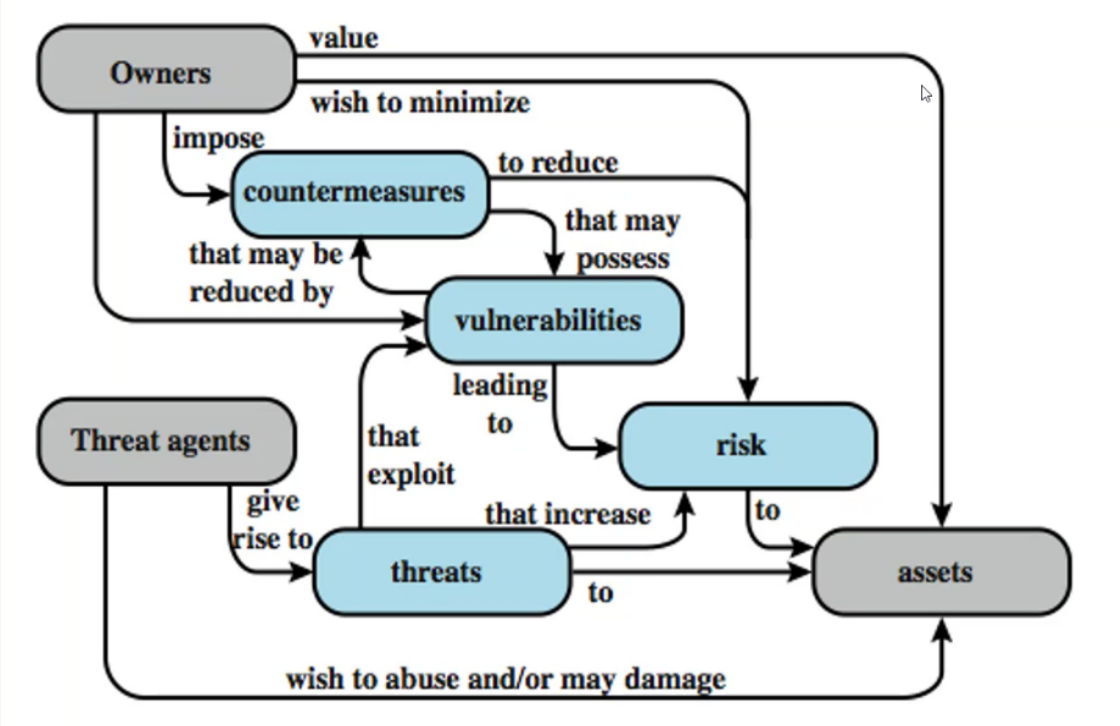


计算机与网终安全问题的挑战

- 安全问题从提出上并不太难，其需求也很明确，描述起来可能只是简单的：机密性，鉴别，完整性等。然而在真正实施的过程中满足这些要求的机制可能相当复杂与困难。
- 开发某种安全机制或协议时，需考虑对这些安全特征的潜在攻击但攻击往往以不同的方式观察问题。
- 由上，对提供特定服务的程序通常是违反直觉的。需要充分考虑各种不同的威胁
- 对于已经设计的安全机制，需要决定其适用的场合
- 安全机制通常包含不止一种算法或协议。牵扯大量的创建分发，存储等问题
- 攻击与防守的不对称性
- 在安全保障失效前，用户与管理者很少能看到安全投入的好处
- 安全要求定期甚至持续监视，注重实效，高负荷运转的系统难以做到
- 安全性经常是作为事后加入的考虑
- 有人认为会影响信息系统的高效性与用户操作的友好性

OS安全体系结构

为了有效评估一个机构的安全需要以及评价和选择各种安全产品和策略，负责安全需求的管理员需要采用某些系统方法来定义安全性需求和表征满足这些需求的方法。事实上，OS安全体系结构已经对此给出了相关的概念：

> **安全攻击**：危及由某个机构拥有的信息安全的任何行为
>
> **安全机制**：设计用于检测、防止或从安全攻击中恢复的一种机制
>
> **安全服务**：加强一个组织的数据处理系统和信息传送安全性的一种服务。该服务的**目标是对抗安全攻击**，它们利用**一种或多种安全机制**来提供该服务
>
> 
>
>
> owner：拥有者
>
> vulnerability：脆弱点
>
> threat agent：攻击者
>
> asset：资产
>
> countermeasure：对策

密码学算法与协议的研究方向——考点4

> 对称加密
>
> 非对称加密
>
> 数据完整性算法
>
> 认证协议

安全攻击——考点2

1 **被动攻击**：被动攻击从本质上是在传输中的偷听或监视，其目的是从传输中获得信息。可分为以下两种：

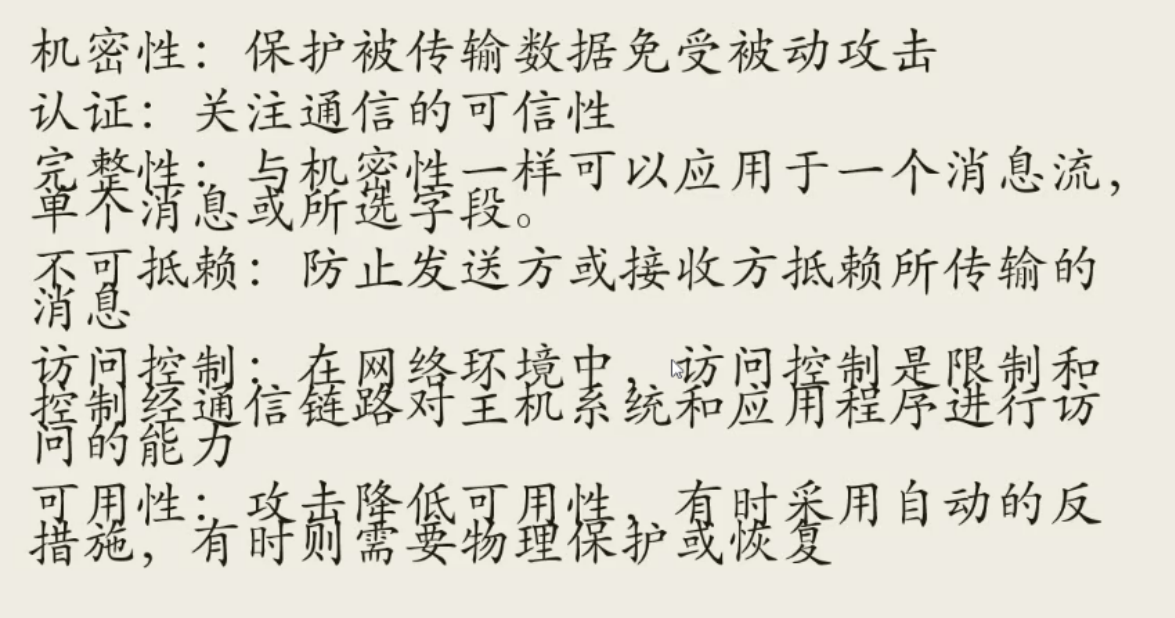
> **析出消息release of message contens**
>
> **通信量分析traffic analysis**：如果消息被屏蔽（比如加密）则即使被析出也不影响。但这时也许对手仍能够观测这些消息的模式。该对手能够测定通信主机的位置和标识，能够观察被交换消息的频率和长度。这对于猜测通信性知识有帮助的。**该方法比较难检测，应对方法是防止而不是检测。——通信量填充来解决**

2 **主动攻击**：主动攻击涉及某些数据流的篡改或一个虚假流的产生可进一步划分为：**伪装，重放，篡改消息和拒绝服务**

> **伪装**就是一个实体假装为另一个实体
>
> **重放**涉及一个数据单元被动获取及后继的重传，以产生一个未授权的效果
>
> **消息篡改**意味着、一个合法消息的部分被改变，或消息被延迟或改变次序，以产生一个未授权的效果
>
> **拒绝服务**防止或禁止通信设施的正常使用或管理

6种安全服务ISO 7498-2——考点

> 机密性：保护被传输数据免受被动攻击
>
> 认证：关注通信的可信性
>
> 完整性
>
> 不可抵赖
>
> 访问控制
>
> 可用性



应用层提供安全服务的特点——记住

只能在通信两端的主机系统上实施。

优点：

> 安全策略和措施通常是基于用户制定的，对用户想要保护的数据具有完整的访问权，因而能很方
> 便地提供一些服务，
>
> 不必依赖操作系统来提供这些服务，
>
> 对数据的实际含义有着充分的理解。

缺点：

> 效率太低
>
> 对现有系统的兼容性太差
>
> 改动的程序太多，出现错误的概率大增，为系统带来更多的安全漏洞。

传输层提供安全服务的特点

只能在通信两端的主机系统上实施。

优点：

> 与应用层安全相比，在传输层提供安全服务的好处是能为其上的各种应用提供安全服务，提供了更加细化的基于进程对进程的安全服务，这样现有的和未来的应用可以很方便地得到安全服务，而且在传输层的安全服务内容有变化时，只要接口不变，应用程序就不必改动。

缺点：

> 由于传输层很难获取关于每个用户的背景数据，实施时通常假定只有一个用户使用系统，所以很难满足针对每个用户的安全需求。

网络层提供安全服务的特点

在端系统和路由器上都可以实现

优点：

> 主要优，点是透明性，能提供主机对主机的安全服务，不要求传输层和应用层做改动，也不必为每个应用设计自己的安全机制，其次是网络层支持以子网为基础的安全，子网可采用物理分段或逻辑分段，因而可很容易实现VPN和内联网，防止对网络资源的非法访问，第三个方面是由于多种传送协议和应用程序可共享由网络层提供的密钥管理架构，密钥协商的开销大大降低。

缺点：

> 无法实现针对用户和用户数据语义上的安全控制。

链路层提供安全服务的特点

越往上定制性越好，越往下透明性越好——判断题

不需要背

安全机制——考点2

设计用来检测，阻止，恢复攻击行为

没有单一的安全机制能应对所有的安全需求

然而有一个元素是作为许多安全机制的基础：**密码学**

特定的安全机制：加密，签名，完整性检验，认证，流量填充等

> 针对特定攻击方式

被动的安全机制：信任机制，安全级别，事件检测，安全追踪，安全恢复

> 不针对某个特定的威胁

基本安全设计原则

> 经济机制原则
>
> 安全缺省设置原则
>
> 绝对中介原则
>
> 开放式设计原则
>
> 特权分离原则
>
> 最小特权原则