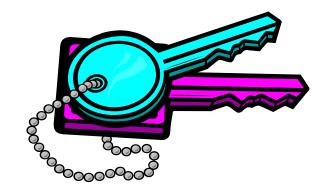
# 第一章基本原理



杨帆 2021春

信息安全概论

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

一The Art of War, Sun Tzu 故用兵之法,无恃其不来,恃吾有以 待之;无恃其不攻,恃吾有所不可攻也。

一《孙子兵法》



### • • • 大纲

1

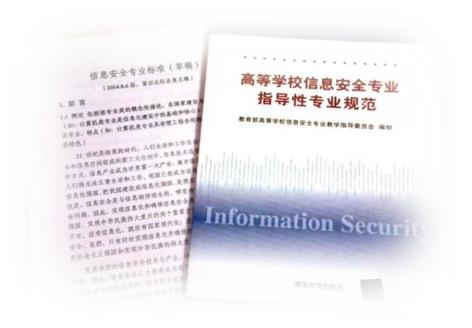
#### 信息安全概念

2 安全攻击、安全机制与安全服务



#### ••• 1 信息安全概念

- o信息安全学科的定义
  - 信息安全学科是研究信息获取、信息 存储、信息传输和信息处理中的信息 安全保障问题的一门新兴学科





#### • • • 违反安全性的实例

- o明文传输
- o篡改
- o伪造
- o延迟
- o否认



## •••2 安全攻击、安全机制与安全服务

# oOSI 安全框架(Open System Interconnection,开放系统互连)

- •安全攻击:任何危及信息系统安全的行为
- •安全机制:用来检测、阻止攻击或者从攻击状态恢复到正常状态的过程
- •安全服务(安全属性):使用一种或者多种安全机制来增强安全、对抗安全攻击的过程



#### ●●● 安全服务(安全属性)

- o 身份认证(鉴别)
  - 确保每个实体都是他们所声称的实体
- o访问控制
  - 防止对资源的未授权使用
- o数据机密性
  - 保护数据免受非授权泄露
- o数据完整性
  - 保护数据免受非授权篡改
- o 不可否认性/真实性
  - 保护通信中针对任何一方的否认攻击
- ◆ 可用性
  - 确保计算机系统资源能在需要时被授权方获得



#### ●●● 安全机制

- o特定安全机制
  - 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

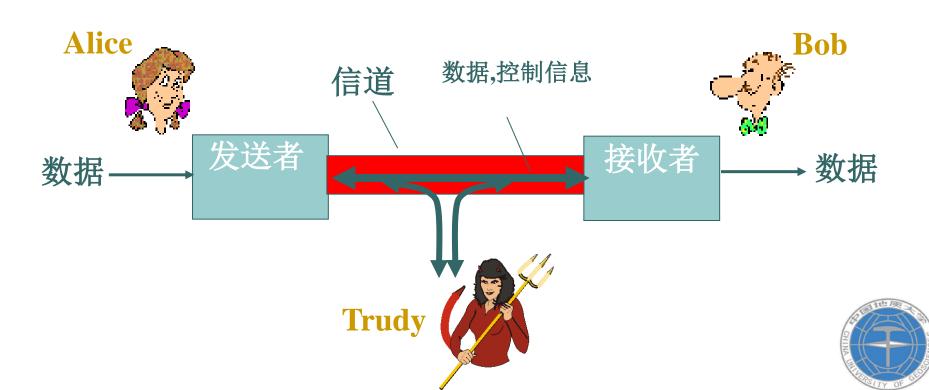
- o普遍安全机制
  - 可信功能
  - 安全标签
  - 事件检测
  - 安全审计跟踪
  - 安全恢复



#### ●●● 安全攻击

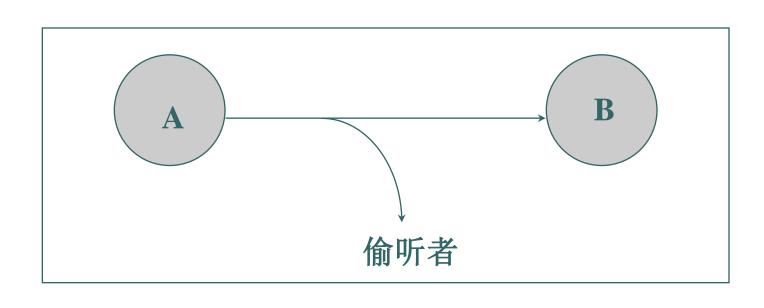
#### 敌手模型: Alice, Bob vs. Trudy

- 网络安全中的经典模型
- · Bob, Alice (朋友)希望安全通信
- · Trudy (入侵者) 可能对原始信息进行拦截,删除, 添加



#### •••偷听,泄露-攻击机密性

- 对传输信息的非授权访问
- 包嗅探和窃听,对文件和程序的非法拷贝
- · 流量分析





#### ●●● 伪造-攻击真实性/不可否认性

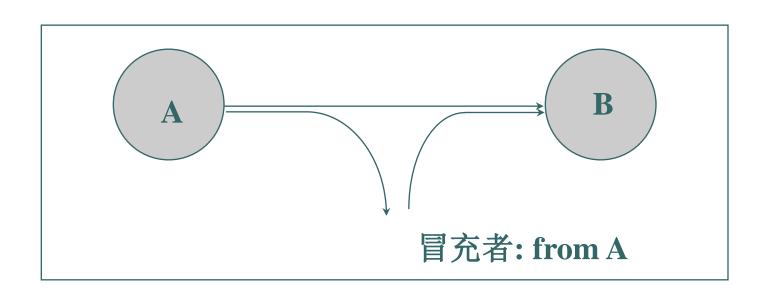
- 非授权冒充他人身份
- 以虚假身份产生和分配信息





#### ●●● 重放-攻击认证和真实性

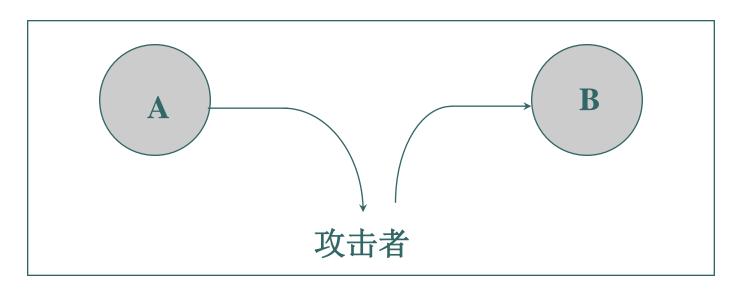
- 偷听认证信息
- 重新发送该认证信息以获得他人的授权身份





#### ●●● 篡改-攻击完整性

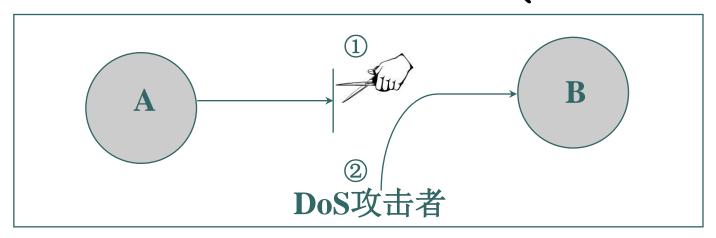
- 阻止信息流
- 延迟并修改信息
- 再次发送信息





#### ●●● 中断-攻击可用性(狭义)

- · 破坏硬件(硬盘失效)或软件(文件管理系统失效),破坏传输的数据包(剪断光缆)
- · 拒绝服务DoS
  - 将服务器攻垮
  - 用海量正常访问淹没服务器(耗尽其资源)





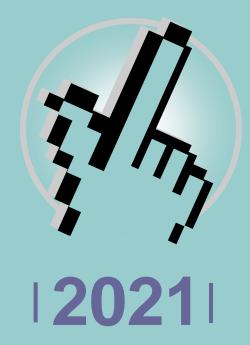
#### ••• 安全攻击分类

- o被动攻击 包括偷听和流量分析,不对数据进行修改
  - 信息内容泄露
    - ✓知晓传输信息的内容
  - 流量分析
    - √监控传输信息的模式,包括信息来源,信息目标,频率 ,长度
    - ✓确定位置和通信主机的身份
- 攻击保密性
- 难以检测
- 可以预防——加密,流量填充



- •
  - o 主动攻击 包括对数据流、系统状态的修改, 创建虚假信息
    - 伪造冒充他人身份(真实性, 不可否认性)
    - 重放旧信息 (认证, 真实性)
      - ✓主动捕获数据,稍后重放以获得非授权效果
    - 修改传输数据 (完整性)
    - 拒绝服务 (可用性)
      - ✓阻止对服务器或通信设备的正常使用和管理
  - 难以预防
  - 可以检测——数字签名, Hash, 入侵检测等





## Thank you...