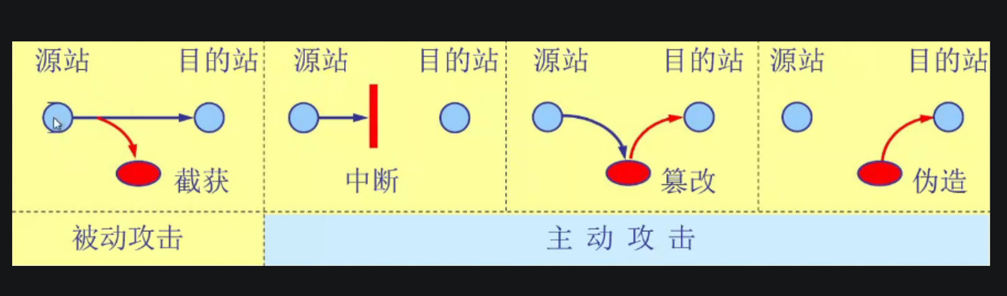
第一章计算机网络安全概述

- 网络安全的重要性
  - 当前网络存在的主要问题P2
    - 机房安全（设备问题）
      - **物理安全**：火灾、雷击、盗贼等（**防火防盗防静电**）
      - 电气安全：停电、负载不均等
    - 病毒的侵入和黑客的攻击（外部问题）
    - 管理不健全造成的安全漏洞（内部问题）
- 网络脆弱性的原因
  - 网络安全问题的原因P3
    - 外在的威胁（外因）
    - 内在的脆弱性 —— 计算机网络本身的脆弱性是根本原因
  - 脆弱性p3 —— 指一个系统的可被非预期利用的方面
  - 从技术角度，脆弱性包括p4
    - 对象
    - 环境
    - 对象所受到的影响
    - 影响对象的方式
    - 外部输入
  - 脆弱的类型p5
    - (计算机原因，瞬时) 逻辑错误
      - 环境错误
      - 编程错误
      - 配置错误
    - 系统弱点 (计算机原因一段时间)
      - 通过隐晦手段获得相对安全
      - 加密技术缺陷
      - 易被破解的弱口令和静态口令
      - 老化的硬、软件
    - 社会工程（人的原因，瞬时）
    - 管理策略失误 (人的原因，一段时间)
  - 从使用角度，脆弱性包括
    - **操作系统的脆弱性**
      - 操作系统结构体制本身的缺陷。
      - 在网络上传输文件，加载与安装程序，包括可执行的文件。
      - 在创建进程，甚至可以在网络的节点上进行远程的创建和激活
      - 操作系统中有一些守护进程，实际上是一些系统进程，它们总是在等待一些条件的出现。
      - 操作系统都提供远程过程调用(RPC)服务，而提供的安全验证功能却很有限。
      - 操作系统提供网络文件系统(NFS)服务，NFS系统是一个基于RPC的网络文件系统。
      - 操作系统的debug。
      - 操作系统安排的无口令入口，是为系统开发人员提供的边界入口，但这些入口也可能被黑客利用。
      - 操作系统还有隐蔽的信道，存在着潜在的危险
      - 尽管操作系统的缺陷可以通过版本的不断升级来克服，但系统的某一个安全漏洞就会使系统的所有安全控制毫无价值。
    - **网络的脆弱性** —— 使用TCP/IP协议的网络所提供的FTP、EMail、RPC和NFS都包含许多不安全的因素存在着许多漏洞。
网络的普及，使信息共享达到了一个新的层次，信息被暴露的机会大大增多。特别是Internet网络就是个不设防的开放大系统。
数据处理的可访问性和资源共享的目的性之间是一对矛盾。它造成了计算机系统保密性难。
    - **数据库管理系统的脆弱性** —— 数据库系统在安全方面的考虑却很少。
数据库管理系统安全必须与操作系统的安全相配套。
    - **防火墙的局限性** —— 尽管利用防火墙可以保护安全网免受外部黑客的攻击，但它只是能够提高网络的安全性，不可能保证网络绝对安全。事实上仍然存在着一些防火墙不能防范的安全威胁，如防火墙不能防范不经过防火墙的攻击。另外，防火墙很难防范来自于网络内部的攻击以及病毒的威胁。
    - **其他方面的原因** —— 计算机领域中重大技术进步都对安全性构成新的威胁。
安全性的地位总是列在计算机网络系统
总体设计规划的最后面，勿略了网络系统的安全
易受环境和灾害的影响。
电子技术基础薄弱，抵抗外部环境较弱。
电磁泄漏的不可避免。
- 网络安全的定义
  - 定义
    - 网络安全是指网络系统的硬、软件及其系统中的数据受到保护，不会由于偶然或恶意的原因而遭到破坏、更改、泄露等。
    - 狭义的定义——指信息内容的安全性：
      - 即保护信息的秘密性、真实性和完整性
      - 保护网络系统的硬、软件及其系统中的数据，不会由于偶然或恶意的原因而遭到破坏、更改、泄露等，保护合法用户的利益和隐私。
    - 广义的网络安全定义：凡是涉及到网络上信息的安全性，完整性，可用性，真实性和可控性的相关理论和技术都是网络信息安全所要研究的领域
  - 组成
    - 操作安全
    - 人员安全
    - 计算机安全
    - 工业安全
    - 物理安全
    - 通信安全
    - 操作安全
  - 从技术角度，网络安全内容包括
    - 网络实体安全（物理安全）
    - 网络数据安全（逻辑安全）
    - 软件系统安全（操作系统安全）
    - 网络管理安全（联网安全）
- 网络安全的基本要素
  - 安全性/可控性（最基本特性）
    - 内部安全
    - 外部安全
  - 完整性 —— 不被篡改
  - 保密性 —— 授权才可用，口令密码
  - 可用性 —— 随时可用
  - 不可抵赖性/不可否认性
- 信息安全发展历程
  - 面向信息的安全保障（通信保密阶段）
  - 面向业务的安全保障（信息安全阶段）
  - 面向服务的安全保障（信息保障阶段）
- 网络安全防护体系
  - 网络安全的威胁
    - 定义：安全威胁是指某个人、物、事件或者概念，对某一资源的机密性、完整性、可用性或合法性所造成的危害
    - 分类
      - 偶然性威胁
      - 故意性威胁
        - 被动攻击:截获信息的攻击
        - 主动攻击:更改信息和拒绝用户使用资源的攻击
    - 计算机网络上通信面临的四种威胁
      - 

      - 截获—从网络上窃听他人的通信内容。
中断—有意中断他人在网络上的通信。
篡改—故意篡改网络上传送的报文。
伪造—伪造信息在网络上传送。
  - 网络安全威胁因素
    - 软件漏洞：任何的操作系统或软件都不是完美、无缺陷、无漏洞的，这些缺陷和漏洞就有可能成为威胁。（内部）
    - 配置不当：安全配置不当造成威胁，如防火墙配置错误，未起到应有作用。（内部）
    - 安全意识不强：用户选择口令简单、随意将账号和口令泄露等。（内部）
    - 病毒：目前网络安全最大的隐患是病毒，计算机病毒是病毒编制者书写的一段程序，能够破坏计算机硬件、软件或者数据，并且能够自我复制等特点。（外部）
    - 黑客：黑客利用网络或计算机系统中的漏洞非法进入未授权的计算机、网络或数据库系统，如果黑客具有恶意倾向，那么造成的危害是十分严重的。（外部）
  - 几种常见的网络安全技术p14
    - 防火墙技术
    - 数据加密技术
    - 系统容灾技术
    - 漏洞扫描技术
    - 物理安全保障技术
  - 网络安全策略
    - 安全策略的分类p16
      - 物理安全策略
      - 访问控制策略
      - 信息加密策略
      - 网络安全管理策略
    - 网络安全基本原则
      - **最小特权**
        - 完成某种操作时赋予每个主体（用户或进程）必不可少的特权
        - 最基本的保安原则
        - 只给每个主体需要履行某些特定任务的那些特权而不给更多
      - **纵深防御**
        - （不能只依赖单一安全机制，建立多重安全机制，相互支撑）
        - 基本的保安原则
        - 没有绝对安全的保护措施，不要绝对相信任何技术
        - 例如：路由器—防火墙一入侵检测一主机保护一密码安全一人员安全数据备份
      - **阻塞点**
        - （设置一个窄道，在那里可对攻击者进行监视和控制。）
        - 例如：网络安全中的防火墙
      - **最薄弱链接**
        - （木桶原理）安全系统的强度取决于其最薄弱环节的强度
        - 安全系统的配置过程中尽量消除或者严密保护薄弱点
      - 失效保护状态
        - (设备损坏) 当系统失效时，拒绝攻击者的访问
        - 安全保护的两种思路
          - 默认拒绝：没有明确允许就是禁止的
          - 默认许可：没有明确禁止的就是许可的
      - 普遍参与 —— （安全需要全体人员的努力）
      - 防御多样化
        - （使用不同种的安全手段）
        - 避免不同系统被同一个人配置）
      - 简单化 —— （让事情简单使他们易于理解，复杂化可能出现问题）
    - 安全保护措施
      - 身份认证
      - 信息保密
      - 数字签名
      - 访问控制
      - 不可否认性
    - 安全策略的实现涉及方面
      - 证书管理
      - 密钥管理
      - 安全策略
      - 安全算法实现
      - 安全策略数据库
  - 数据安全
    - 数据安全因素
      - 内部因素
        - 由于非法入侵以及病毒所导致的数据安全问题
        - 由TCP/IP网络体系结构本身导致的数据安全性问题；
      - 外部因素
        - 管理人员对系统的非法操作
        - 非法用户对网管系统的操作
    - 数据边界安全策略
      - 被动防御技术：防火墙
      - 主动防御技术：入侵检测系统
    - 数据传输安全策略
      - 数据发送/接收端 —— 窃取数据 → 身份验证
      - 数据传输通道 → 加密通道
        - 截获数据
        - 窃听数据
    - 数字加密技术
      - 对称密码体制
        - DES
        - IDEA
      - 非对称密码体制 —— RSA
    - 数据存储安全策略
  - 网络监控软件
    - 防止并追查重要资料，文件外泄目的主机：
    - 监督、审查、限制和规范网络使用行为；
    - 限制消耗网络资源的聊天、下载、游戏等；
    - 备份重要网络资源文件；
    - 监视聊天软件内容；
    - 流量限制以及网站方位统计。
    - sniffer
      - 一种基于被动侦听原理的网络分析方式
      - 当网络接口设置为监听模式时，可以截获网上传输的信息
      - 黑客们常用它来截获用户的口令
      - 分为软件和硬件两种
  - 病毒
    - 系统病毒：感染Windows操作系统的.exe和.dll文件。
    - 蠕虫病毒：通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性。
    - 木马病毒：通过一段特定的木马程序来控制另外一台或多台计算机。
    - 脚本病毒：使用脚本语言编写，通过网页进行的传播的病毒
    - 宏病毒：让计算机感染传统型的病毒。删除硬盘上的文件或文档
    - 后门病毒：后门就是辅助木马进一步入侵的小程序，通常会开启若干端口或服务。