# 计算机安全复习提纲

## 计算机安全概述

1. **计算机系统资源包含什么**

**硬件**：计算机系统以及其他数据处理、存储和通信的设备。

**软件**：操作系统、系统实用程序和应用程序。

**数据**：文件和数据库，与安全相关的数据，如口令文件等。

通信设备和网络：局域网和广域网的通信链路、网桥、路由器等。

1. **计算机安全的三个目标及其分别的含义**

**2.1机密性**

数据机密性：确保隐私或机密信息不能由非授权个人利用，或不能披露给非授权个人。

隐私性：确保个人能够控制个人信息的收集和存储，也能够控制这些信息可以由谁披露或向谁披露。

**2.2完整性**

数据完整性：确保信息和程序只能在指定的和授权的方式下才能够被改变。

系统完整性：确保系统在未受损的方式下执行预期的功能，避免对系统进行有意或无意的非授权操作。

**2.3可用性**

确保系统能够迅速地进行工作，并且不能拒绝对授权用户的服务。

可用性缺失：对信息或信息系统的访问和实用的破坏。

## 密码学

1. **密码学术语解释**

密码学是关于如何在敌人存在的环境中通讯。

1. 密码学发展阶段

第一阶段：1949年之前，古典密码，密码学是一门艺术。

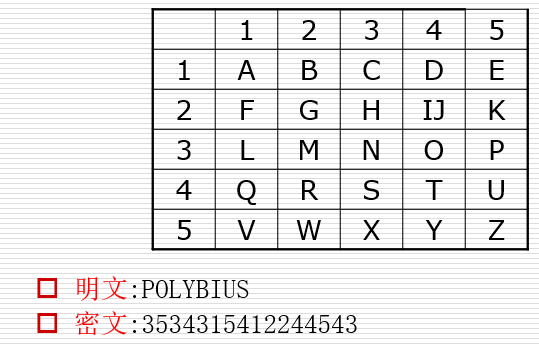
第二阶段：1949年之后，现代密码出现，密码学成为科学。

1976年，公钥密码学。

1. 凯撒密码和棋盘密码的原理；字母频率破译法

凯撒密码：每个字母用它之后的第三个字母代替。

棋盘密码：



字母频率破译法：人类语言是冗余的，字母使用频率不尽相同。

破译原理——频率分析。

1. **加密、解密、密码体制、明文、密文、密钥的概念**

加密：将消息进行编码，以模糊其含义的过程。

解密：是加密的逆过程，将加密过的信息变回其原始形式。

密码体制：用于加密和解密的系统。

明文P：消息的初始形式，原始可理解的信息或数据。

私密的密钥K：用来加密信息的一组秘密的数据。

密文C：加密后的形式，不可直观理解，依赖于明文和密钥。

1. **对称密码概念**

**加密与解密的密钥相同。**

分组密码的一般设计原理：

* + **将明文信息编码后的数字序列划分成长度为n的组，一次处理一个组。**
  + **每组分别在密钥的控制下变换成等长的密文信息。**
  + **典型的分组大小为64bits或128bits。**

现在大部分的密码是分组加密，分组加密是最常用的加密算法之一。加密速度快。

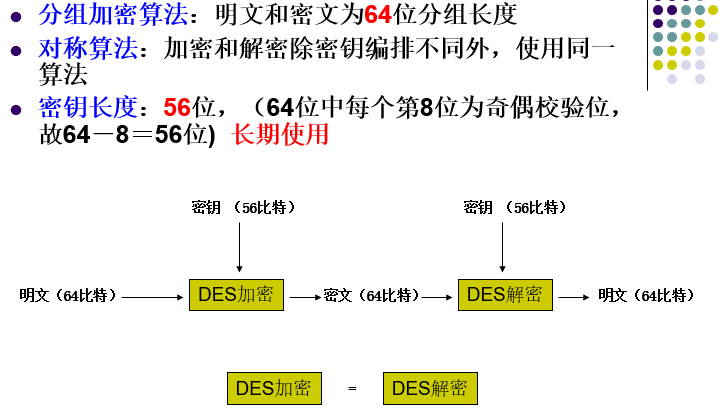
对付统计分析：

混乱：确保密文和明文没有明显的联系，密文尽量随机。替换。

扩散：将明文中一位的影响扩展到密文中的多位。置换。

1. DES、AES分组密码算法

**DES：数据加密标准算法**



**DES抗穷举攻击能力弱，是不安全的。**

**AES：高级加密标准算法**



特点：

有较好的数学基础；

**抵御任何已知的攻击；**

**结构简单，能在许多CPU上高效实现。**

操作都是替换、置换、移位、加、异或运算，故能用32位cpu快速、高效地实现。

能有效抵御目前已知的线性攻击和差分攻击算法。

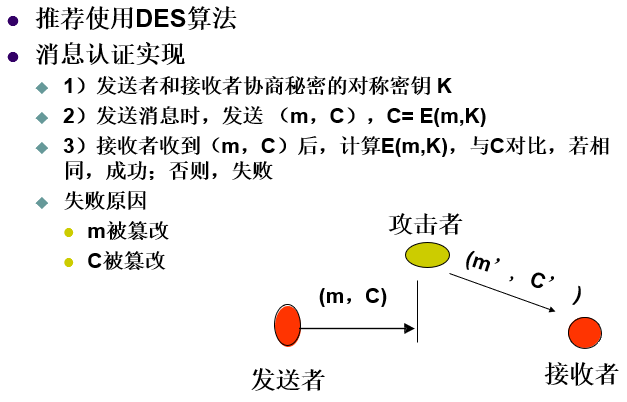
1. **消息认证的目的，如何使用对称密码或哈希函数实现消息认证**

**7.1消息认证的目的：保证信息的完整性。**

第一、信源识别，即验证发信人确实不是冒充的。

第二、检验发送信息的完整性，也就是说，即使信息确实是经过授权的信源发送者发送的，也要验证在传送过程中是否被篡改、重放或延迟。

**7.2消息认证用对称密码实现**



E：Encrypt，加密

**7.3消息认证用哈希函数的实现**

**利用Hash函数生成消息的一个固定长度码字，称为消息认证码（MAC），级联在消息后面发送**

* + **1）发送者和接收者协商秘密的串 K**
  + **2）发送消息时，发送 （m，C），C= H(m,K)**
  + **3）接收者收到（m，C）后，计算H(m,K)，与C对比，若相同，成功；否则，失败**

**倾向于使用Hash函数实现消息认证，而不是对称密码**

* **加密软件比Hash函数软件速度慢**
* **加密硬件成本不容忽视**
* **对称密码要处理消息分组，花费时间多**
* **加密算法可能受专利保护**

1. **哈希函数的定义，要求**

哈希函数是一种典型的消息认证函数，提供消息的完整性保护。哈希函数又称散列函数、杂凑函数、校验和或消息摘要算法等。

**性质：是单向函数**



要求：

* + **对于任意给定的x，计算H(x)较容易，用硬件、软件都可实现**
  + **单向性（抗原象性）：对于任意给定的散列值h，找到满足H(x)=h的x是不可行的**
  + **抗若碰撞性（第二抗原像性）：给定一个x，找到一个y，使得y≠x，且H(y)=H(x)，是计算上不可行的**
  + **抗强碰撞性：找到任何满足H(y)=H(x)的一对(x,y)在计算上不可行**

注意：

哈希函数不使用密钥；

哈希函数是多对一的映射（即不同长度的输入，其输出的位数一样）

1. **公钥加密（或称为非对称加密）概念；公钥加密的密码生成过程**

公钥密码又称为双钥密码、非对称密码，它使用两个密钥：一个公钥、一个私钥；

以数论、近世代数为数学基础；

与对称加密是互相补充的，并不是取代对称加密。

特征：

加密和解密由不同的密钥完成；

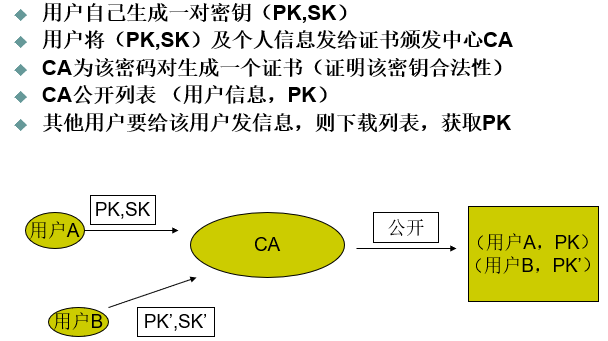
公钥可被任何人知道，可用来加密消息；

私钥只为接收者本人知道，用来解密消息。

**生成过程：**

**PK:Public Key, 公钥**

**SK:Secure Key，私钥**



1. **数字签名的性质，与消息认证区别**

**消息认证用于保护通信双方之间的数据交换不受第三方攻击；但并不能保证通信双方自身的相互攻击、欺骗。**

数字签名：是附加在数据单元上的一些数据，或是对数据单元所作的密码变换。

这种数据或变换允许数据单元的接收者确认。

数字签名的性质：

* **不可伪造：如果P用S(P,M)签署了报文M，其他任何**

**人不可能生成相同的签名S(P,M)**

* **真实性：接收者R可以验证签名S(P,M)是否真的来自声称者P，并且签名严格附属于M**
* **不可变：签名时刻的内容M不可变**
* **不可重用：如果对新的内容M’重用以前的签名S(P,M)，接收者R可以立即察觉**
* **任何人都可以验证签名**

数字签名包括了消息认证的功能。

## 第三四章 用户认证和访问控制

1. **存储口令使用盐值的原理，好处是什么**
   * UNIX操作系统登录，输入ID/口令
     + **口令文件passwd是加密后的文本**，存放在\etc\passwd
     + 使用基于DES的加密函数crypt()，用64bit的盐值，产生13byte的值
   * 使用盐值的好处
     + **防止重复的口令可见**
     + **增加了离线字典攻击的难度**
     + **不能发现在不同系统中使用了相同的口令**
2. **远程用户认证的质询-响应协议，为何防范重放攻击**
3. **访问控制机制中的主体、客体、访问权概念**

主体：能够访问客体的实体。

客体：外界对其访问受到控制的资源。

访问权：描述主体可以访问客体的方式。

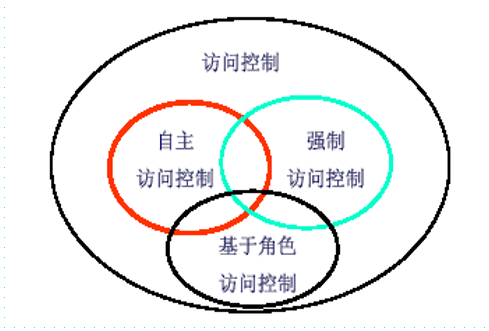
1. **访问控制的目的，实现的安全策略**

目的：**防止未经授权使用资源**，包括防止以非授权方式使用资源，从而使计算机系统在合法范围内使用。

实现的安全策略：

对于每个具体的系统资源，谁或什么可以访问，以及每个实例允许的访问类型。

1. 访问控制机制分类及其分别的含义



自主访问控制：  
**① 每个主体拥有一个用户名并属于一个组或具有一个角色**

**② 每个客体都拥有一个限定主体对其访问权限的访问控制列表（ACL）**

强制访问控制：

* **定义：主体的权限和客体的安全属性都是固定的，由系统决定主体是否可以访问客体。不允许主体干涉访问控制。**

基于角色的访问控制：

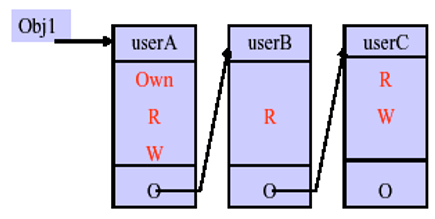
* **基于角色的访问控制是一个复合的规则。一个身份被分配给一个被授权的组。起源于UNIX系统或别的操作系统中组的概念。**

1. **访问控制列表、访问能力表、访问控制矩阵是什么**

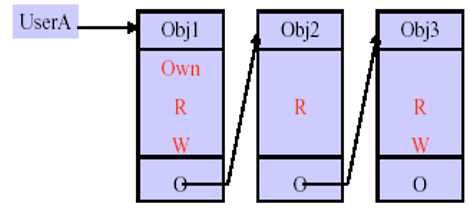
访问控制矩阵：每列看是访问控制表内容，每行看是访问能力表内容。



访问控制列表：以客体为中心，每个客体附加一个可以访问的主体的明细表。



访问能力列表：每个主体都附加一个该主体可以访问的客体的明细表。



1. **计算机系统安全级别 ABCD**

**D级别是最低的安全级别，对系统提供最小的安全防护。（权限最大）**

* + **系统的访问控制没有限制**
  + **无需登陆系统就可以访问数据**
  + **这个级别的系统包括DOS，WINDOWS98等**

C（c1、c2）级别属于自由选择性安全保护。

* + **C1级称为选择性保护级􀂀**
    - **认证、完全访问控制（用户可以访问操作系统的根）**
  + **C2级具有访问控制环境的权力**
    - **比C1的访问控制划分的更为详细（用户权限等级），能够实现受控安全保护、个人帐户管理、审计和资源隔离**
  + **UNIX、LINUX和WindowsNT系统**
  + **安全策略主要是自主访问控制**

B级别——包括B1、B2、B3三个级别，B级别能够提供强制访问控制和自主访问控制。

* + **􀂀所有敏感标识控制下的主体和客体都有标识**
  + **􀂀安全标识对普通用户是不可变更的**
  + **􀂀可以审计**
    - **􀂙任何试图违反可读输出标记的行为**
    - **􀂙授权用户提供的无标识数据的安全级别,以及与之相关的动作**
    - **􀂙信道和I/O设备的安全级别的改变**
    - **􀂙用户身份和与相应的操作**
  + **􀂀维护认证数据和授权信息**
  + **􀂀通过控制独立地址空间来维护进程的隔离。**

**A级别称为验证设计级，是目前最高的安全级别。**

## 第五章 入侵检测

1. **安全入侵、入侵检测定义**

安全入侵：一个安全事件或多个安全**事件的组合**构成一个**安全事故**，在安全事故中入侵者在未经授权的情况下获取或尝试获取一个系统（或系统资源）的访问权。

入侵检测：一种监控并分析系统事件的安全服务，目标是**发现未经授权**而访问系统资源的**尝试活动**，并提供实时或近似实时的报警。

1. **入侵检测系统组件**

**传感器**：负责收集数据；输入类型：网络数据包，日志文件，系统调用痕迹。

**分析器**：从一个或多个传感器或其他分析器接受输入；负责确定是否发生了入侵；提供指导，用于判定什么活动是入侵导致的后果。

用户接口：通过用户接口，用户查看系统输出。

1. **入侵检测的两种方法**

异常检测：依据合法用户的行为规则来判定**用户行为的不合法性**。

特征检测：根据一组规则或攻击模式，来确定给定的**行为是否为入侵者行为**。

1. **掌握入侵检测系统的分类及其各自概念**

**基于主机的入侵检测系统：**

* 从系统运行所在的主机**获取审计数据**（比如系统日志、系统状态信息、运行程序的行为特征、文件变更情况），保护目标是系统所在的主机

**分布式基于主机的入侵检测系统：**

* **主机代理模块**：搜集有关主机安全事件的数据并进行分析，并将可疑行为的报警信息发给中心管理员。
* **局域网监视代理模块**：运作方式和主机相同，但它分析局域网的流量，然后将结果报告给中心管理员。
* **中心管理员模块**：接收上述两个模块送来的报告，对它们进行综合处理，以判断是否存在入侵。

**基于网络的入侵检测系统：**

* 是**附加**在网络上的一台**单独的设备**，从网络传输流中获取网络包，监测特定的网段或设备的流量并分析网络、传输和应用协议，用以识别可疑的活动
* 部署在合理的流量集中点处（能看到所有的数据包），利用的是sniffer技术，采用的是基于攻击特征的检测。

**分布式或混合式入侵检测系统：**

* 每个主机和网络设备都是潜在传感器，提高更高覆盖率
* 入侵检测交换格式

1. **蜜罐的概念和功能**
   * 把攻击者引导到一个经过特殊装备的系统上，这种系统被成为蜜罐。
   * 功能：
     + **转移**攻击者对重要系统的访问
     + 收集有关攻击者活动的信息
     + **引诱**攻击者在系统中逗留足够长的时间，以便于管理员对此攻击做出响

## 第六章 恶意软件

1. **恶意软件的概念、分类**

概念：利用计算机系统挪动来对计算机系统造成威胁的程序。

分类：

* + **按是否依附于宿主程序**
    - 寄生程序：依附于宿主程序的程序片段， 病毒、后门
    - 非寄生程序：独立于宿主程序，可被操作系统调度和执行的独立程序， 蠕虫、bot程序
  + **按是否进行复制**
    - 不进行复制：触发执行的程序或程序片段，后门、bot程序
    - 进行复制：程序或程序片段，执行时生成一个或多个自身的拷贝，在合适的时机在当前系统或其他系统中被激活， 病毒、蠕虫

1. **后门**

进入一个程序的秘密入口，使得知情者不经过通常的安全访问程序而获取访问权限

1. **病毒组成部分、四个经历阶段、病毒的几种分类**

组成部分：

* + 感染机制（感染向量）：病毒传播和使病毒能够自我复制的方法
  + 触发条件：激活或交付病毒有效载荷的事件或条件
  + 有效载荷：病毒除传播之外的活动，包括破坏活动或者无破坏但值得注意的活动

**四个经历阶段：**

* **潜伏阶段**：病毒处于休眠状态
* **传播阶段**：病毒将自身的拷贝插入其他程序或硬盘上某个与系统相关的区域。病毒拷贝时会变异来逃避检测。
* **触发阶段**：病毒被激活以执行预先设定的功能
* **执行阶段**：执行病毒功能

**按照病毒的感染对象分类：**

* **感染引导扇区病毒**：感染主引导记录或引导记录。

感染计算机启动过程中的引导区 （boot sector）

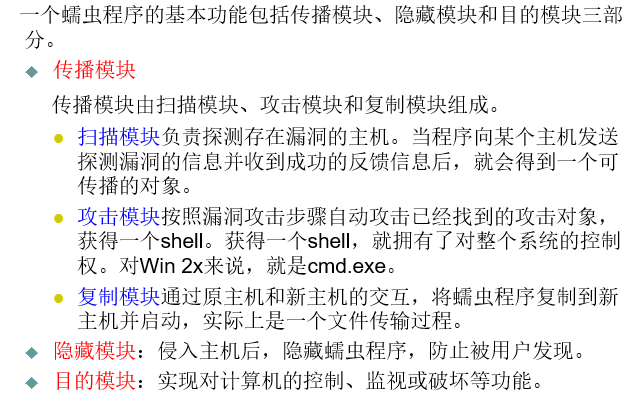
引导区先于其他程序获得对CPU的控制，通过感染引导区上的引导程序，病毒就可先于操作系统截取系统控制权。

* **感染可执行文件病毒**：感染可以在操作系统或shell中执行的文件。
* **宏病毒**：感染包含可执行宏代码的文件。
* **多元复合型病毒**：感染多种文件类型。

1. **蠕虫和病毒的区别、蠕虫构成、每个模块的具体功能、扫描机制、隐藏方式**

**区别：**

* **病毒可通过任何介质进行传播，蠕虫通过网络**
* 病毒的自身拷贝必须**嵌入**到其他程序中来传播，蠕虫的自身拷贝都是以**独立程序**的形式传播



扫描机制：

* 在网段的选择上，可以主要对当前主机所在网段进行扫描，对外网段随机选择几个小的IP地址段进行扫描。
* 对扫描次数进行限制。
* 将扫描分布在不同的时间段进行，不集中在某一时间内。
* 针对不同的漏洞设计不同的探测包，提高扫描效率。

隐藏方式：

* 1）修改蠕虫在系统中的进程号和进程名称，掩盖蠕虫启动的时间记录。
* 2）将蠕虫拷贝到一个目录下，并更换文件名为已经运行的服务名称，使任务管理器不能终止蠕虫运行。
* 3）删除自己

1. 如何构造僵尸网络、扫描方式

**构造僵尸网络：**

* + 攻击者通过扫描或特征码识别找到大量**存在漏洞的主机，获得访问权**，并用bot软件感染它们
  + 被感染的机器上的bot软件继续扫描并感染其他主机，直到组成大型分布式网络

**扫描方式：**

* **随机扫描**：每个受控主机使用一个不同的种子，在IP地址空间中探查随机地址
* **攻击列表**：攻击者先编辑生成一个潜在的易受攻击主机列表，然后逐一感染每台主机。每个被感染的主机拥有列表的一部分继续感染
* **拓扑扫描：利用被感染主机中的信息来找到更多的主机**
* **本地子网扫描**：如果防火墙后的主机被感染，则它通过子网地址结构在本地网络中寻找感染目标。

1. **木马的组成和原理、分类**

关于Trojan（特洛伊木马）程序的定义是：特洛伊木马程序是一种程序，它能提供一些有用的或者令人感兴趣的功能。但是**还具有用户不知道的其他功能**，例如在用户不知晓的情况下拷贝文件或窃取密码。

分类：

远程控制型、信息窃取型

## 第七章 防火墙

1. **防火墙概念、三个设计目标、功能**

**防火墙：一种用来加强网络之间访问控制，防止外部网络用户以非法手段通过外部网络进入内部网络、访问内部网络资源，保护内部网络操作环境的特殊网络互连设备。**

**设计目标：**

* + 所有入站和出站的网络**流量都必须通过防火墙**。
  + 只有**经过授权**的网络流量**才允许通过**防火墙。
  + 防火墙本身不能被渗透，应该运行在有安全操作系统的可信系统上。

**功能：**

* + 对企业内部网实现集中安全管理，强化网络安全策略，比分散的主机管理更经济易行。
  + 作为部署网络地址转换NAT的地点，缓解地址空间短缺，隐藏内部网的结构 （network address translation）
  + 是审计和记录网络的访问和使用的最佳地方。

1. **防火墙分类：包过滤、状态检测、应用代理**
2. **包过滤防火墙工作原理**

在网络层中，对所**接收的每个数据包进行检查**

将数据包的包头信息（如源IP地址、目的IP地址、源端口号、目的端口号、协议类型、方向等）**与事先设定的过滤规则相比较，据此决定转发或者丢弃该包**

1. **按TCP包头信息建立过滤规则**

源端口、目标端口、标志段（SYN、ACK、FIN、RST）等

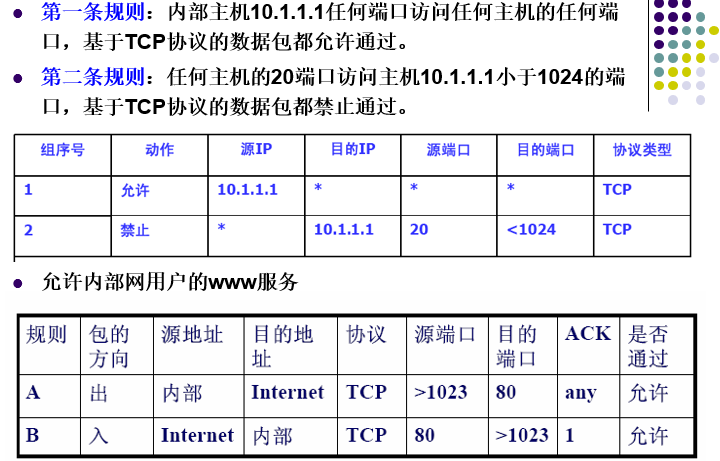
TCP端口号1024以下被用于一些标准的通信服务

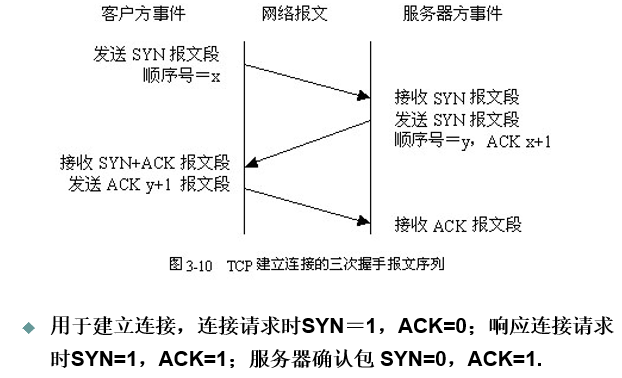
端口21：FTP文件传输

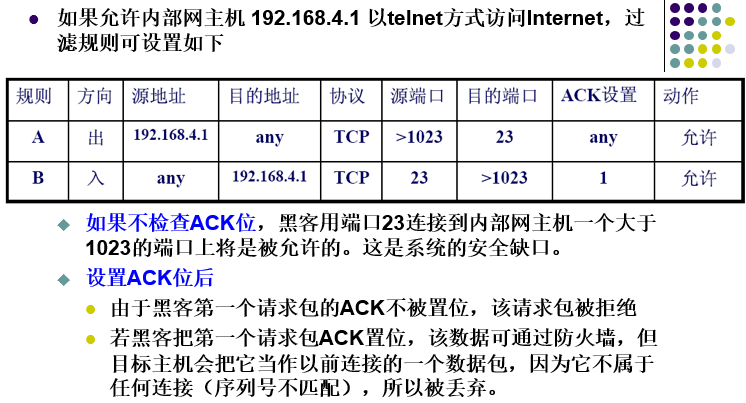
端口23：Telnet远程登录

端口25：SMTP电子邮件

端口80：WWW







1. **状态检测防火墙工作原理**

**动态包过滤，工作在网络层。**

它将属于同一连接的所有包作为一个整体的数据流看待（保证了前后报文的相关性），构成连接状态表

通过规则表与状态表的共同配合，对数据包进行转发或拒绝处理。

流程：

* 它使用了一个在网关上执行网络安全策略的软件模块，称之为监测引擎。
* 对新建的应用连接，检查预先设置的安全规则，允许符合规则的连接通过，并在内存中记录下该连接的相关信息，生成连接记录。
* 对该连接的后续数据包，只要符合状态表，就可以通过，而不需进行规则检查，在一定程度上使性能有较大提高。

1. **代理服务器工作原理，功能、特点**

**工作原理：**

* 应用级网关需要对每一个特定的Internet服务安装相应的**代理服务软件**，如HTTP、 FTP等，其次，用户不能使用未被服务器支持的服务。
* **网络信息的中转站**

**功能：**

（1）**设置用户验证和记账功能**，可按用户进行记账，没有登记的用户无权通过代理服务器访问Internet网。并对用户的访问时间、访问地点、信息流量进行统计。

（2）**对用户进行分级管理**，设置不同用户的访问权限，对外界或内部的Internet地址进行**过滤**，设置不同的访问权限。

（3）连接内网与Internet，**充当防火墙（Firewall）**，节省IP开销：因为所有内部网的用户通过代理服务器访问外界时，只映射为一个IP地址，所以外界不能直接访问到内部网；同时可以设置IP地址过滤，限制内部网对外部的访问权限。

（4）**增加缓冲器（Cache)，提高访问速度**，对经常访问的地址创建缓冲区，大大提高热门站点的访问效率。通常代理服务器都设置一个较大的硬盘缓冲区（可能高达几个GB或更大），当有外界的信息通过时，同时也将其保存到缓冲区中，当其他用户再访问相同的信息时，则直接由缓冲区中取出信息，传给用户，以提高访问速度。

**优点：**

* 代理服务器**理解应用协议**，它针对特定的应用协议使用指定的数据过滤逻辑。根据协议内部可见的内容而不仅仅根据头部数据来控制穿越防火墙的行为；
* **安全性高**，可防止在受信主机与非受信主机间直接建立联系。

**不足：**

* 每个特定的应用（www、FTP、E-mail）都需要一个专门的代理，**扩充性差**，使用时工作量大，效率低，在网络上运行一个代理服务器**可能需要更昂贵的硬件**；
* 首先它会使**访问速度变慢**，因为不允许用户直接访问网络。

1. **软、硬件防火墙概念**

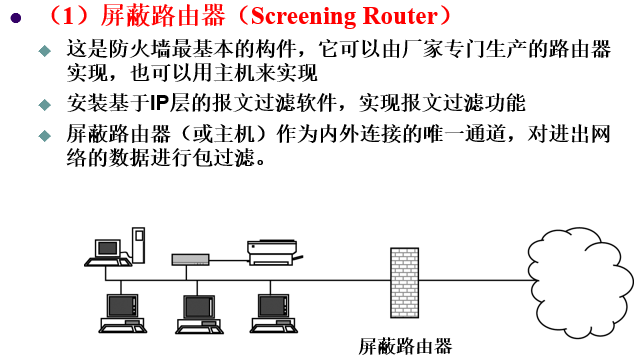
**软件防火墙：**

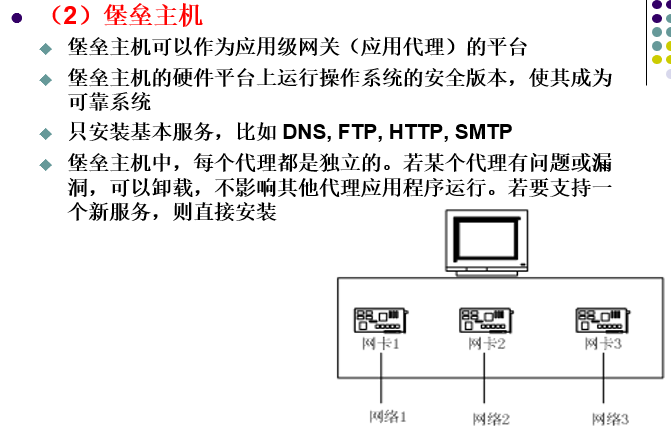
防火墙是运行在通用计算机上的**纯软件**，安装在公共的操作系统上。简单易用，配置灵活。但因底层操作系统是一个通用型的系统，其**数据处理能力、安全性能水平都比较低**。一般应用于个人主机上。

**硬件防火墙：**

* 将防火墙软件**固化在专门设计的硬件平台**上（防火墙程序做到芯片），数据处理能力与安全性能水平都得到了很大的提高。
* 但因来自网络的威胁不断变化，防火墙的安全策略、配置等也需要经常进行调整，**而纯硬件防火墙的调整非常困难**。
* 一般应用于数据处理性能要求高、安全策略比较稳定的情况

1. 防火墙4种部署方式（了解）



用户网络上最容易受侵袭的机器。

* **（3）屏蔽主机结构（ Screened Host ）**
  + **屏蔽主机结构=路由器隔离内部网络和外部网络+代理服务器堡垒主机部署在内部网络上。**
  + **路由器上设置数据包过滤规则，使堡垒主机成为外部网络唯一可以访问的主机，通过路由器的包过滤技术和堡垒主机的代理服务器技术防护内部网络的安全。**
  + **屏蔽主机防火墙实现了网络层和应用层的安全，因而比单独的包过滤或应用网关代理更安全。**
  + **屏蔽主机的防火墙体系结构易于实现，而且比双重宿主主机结构的安全性高，应用比较广泛。**
* **（4）屏蔽子网结构**

**它的实现方法是建立一个被隔离的子网，位于内外网之间，用两台屏蔽路由器将这个子网分别与内部和外部隔开，并利用这两台屏蔽路由器将该子网形成一个禁止穿行区，即内部网和外部网都能访问这个子网，但它们却不能穿过该子网直接通信，这样就形成了屏蔽子网网关。**

## 第八章 数据库安全

1. **数据库访问控制和操作系统访问控制的区别**

**数据库的访问控制更为复杂**，体现在：

控制粒度：

操作系统中控制的粒度是文件

数据库中则需要控制到记录和域一级

关联性：

操作系统中的文件之间没有关联关系

数据库中，不仅库表文件之间有关联，在库表内部记录、域、元素都是相互关联的

**在数据库中可以通过读其他元素的值而推知另一个元素的值，称为推理。**

* + 若要限制推理则意味着要禁止一些访问路径，即限制访问，但也限制了某些用户正常查询。
  + 而操作系统中不要担心推理攻击；

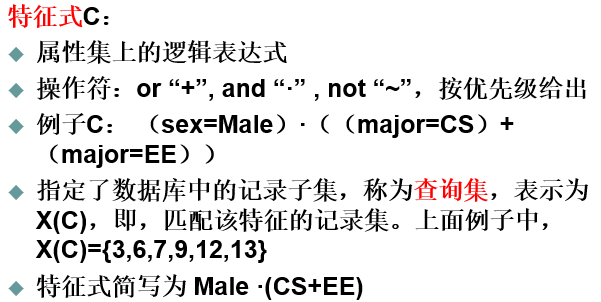
1. **推理攻击、推理信道、元数据定义**

推理攻击：完成授权查询并从得到的合法响应中推导出非法授权信息的过程。

推理信道：获得非授权数据的信息传送路径称为推理通道。

元数据：有关数据项之间相关性或依赖性的知识性。

1. **特征式、查询集定义**



1. **抗击推理攻击的两种方式**

**1）查询限制**：拒绝导致泄密的查询。提供的应答是准确的

**2）扰动技术**

* + 查询限制技术可能**成本很高**，且无法完全阻止推理攻击，尤其是用户有附加知识的情况下
  + 对所有询问提供应答，但**应答是近似的，不准确**的

1. **查询规模限制、查询重叠集控制概念**

（1）.查询规模限制

* + - 针对推理攻击举例： 用户知道Baker是EE的女生，但不确定是不是唯一的一位，于是，用户查询如下统计数据：

count(EE·Female)=1,

sum(EE·Female, GP)=2.5

* + - **对查询集的规模进行限制**，对于规模为N的数据库，要求用户只能对满足如下条件 k≦|X(C)| ≦N-k 的C进行访问

（2）. 查询集重叠控制

* 针对推理攻击举例： 设k=3，则特征式Male ·(CS+EE) 和 Male ·(CS+EE+Bio) 均不受查询规模限制，因为Count(Male ·(CS+EE))=6， Count(Male ·(CS+EE+Bio))=7，

假设用户知道Evans是Bio的一个学生，但不确定是否是唯一的。则可通过询问上述两个计数来确认。然后，用户又可以询问 sum(Male·(CS+EE),SAT) 和 sum(Male ·(CS+EE+Bio), SAT)，获得Evans的SAT值。

* 对查询集重叠进行控制，当特征式C满足

|X(C) ∩X(D)|≦r（r是大于0的固定整数，D是用户查询过的特征式）， 用户才能得到应答。

1. **数据扰动、输出扰动概念**

**数据扰动：修改SDB中的数据**以便不能根据产生的统计数据推理出单个记录的值

**输出扰动**：当进行统计查询时，系统在对原始数据库提供的数据**修改后产生统计数据**，以阻止获得单个记录的信息的企图。

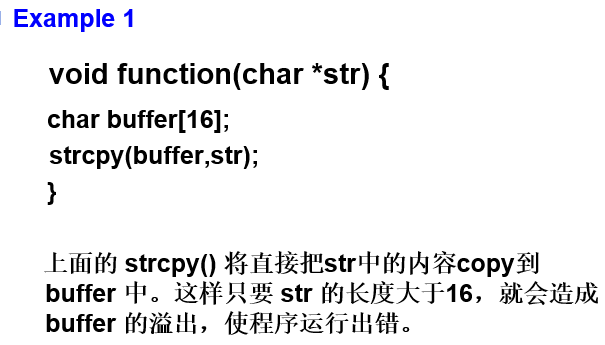
## 第九章 缓冲区溢出

1. **缓冲区定义、缓冲区溢出概念**

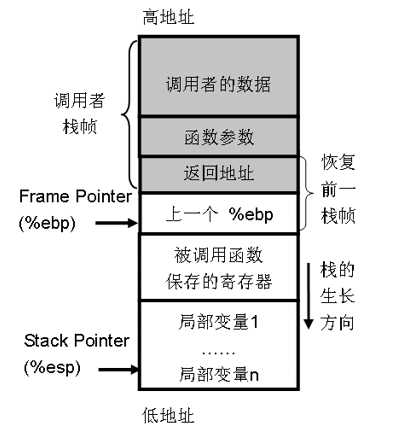
**缓冲区是用户为程序运行时在计算机中申请的一段连续内存**， 存了指定类型的数据。

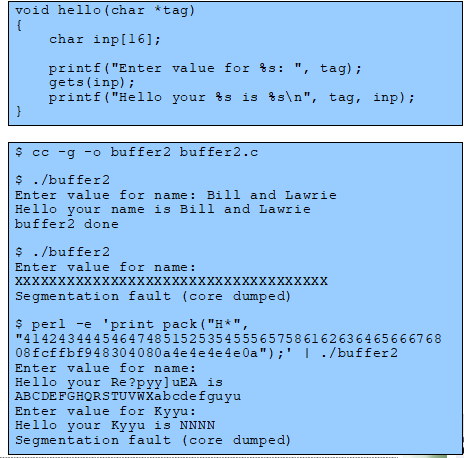
大多时候，在缓冲区内装载的数据大小是用户输入的数据决定的。若程序不对用户输入的数据作长度检查，用户又对程序进行了非法操作或者错误输入，当**输入的数据占满了缓冲区的所有空间，且超越了缓冲区边界**延伸到缓冲区以外的空间的话，缓冲区溢出就产生了。

1. **举例一段存在缓冲区溢出漏洞的程序，并分析原因**



1. **在函数调用中，实现栈缓冲区溢出程序示例。**

**当目标缓冲区被设置在栈区时，所发生的缓冲区溢出，称为栈缓冲区溢出。**



1. **如何利用缓冲区溢出实现攻击、步骤**

缓冲区溢出攻击是指攻击者利用溢出漏洞精心编写的带有某种不良企图可执行代码(shellcode)的程序，**通过在缓冲区写入超过预定长度的数据造成所谓的溢出，破坏了堆栈的缓存数据，**使程序的返回地址发生变化，使它指向溢出程序中shellcode的开始，这样就可以运行攻击者的代码，达到攻击者的目的。

1. **举例2种栈保护机制**

**1）栈卫士（stackguard）：插入了附加的函数入口和出口代码**。函数入口代码，在为局部变量分配的地址空间之前，在旧的帧指针地址之下写入一个canary值；在继续这些常用函数的退出操作（恢复旧的帧指针和转移控制权后退到返回地址）之前，添加的函数出口代码检查canary的值没有变化。

**2）Stackshield和返回地址保护者（RAD）：是用附件的函数入口和出口代码，在函数入口处，添加的代码将返回地址的一个副本写到内存的一个安全区域**（这个区域要想破坏都非常困难）；在函数的出口处，添加的代码检查栈帧里的返回地址与保存的副本，如果发生任何变化就终止程序。