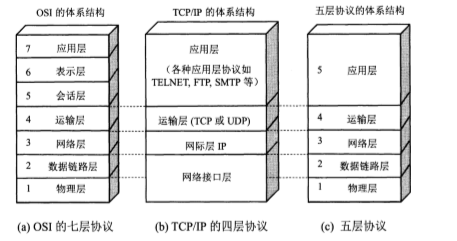
**1.计算机网络体系结构**



应用层：通过应用进程间的交互来完成特定网络应用。应用层协议定义的是应用进程间通信和交互的规则，在互联网中的应用层协议有很多，如域名系统DNS，支持万维网应用的HTTP协议，支持电子邮件的SMTP协议等。应用层交互的数据单元称为报文。

运输层：向两台主机中进程之间的通信提供通用的数据传输服务。运输层主要使用两种协议，分别是传输控制协议TCP和用户数据报协议。

网络层：为分组交换网上的不同主机提供通信服务。

数据链路层（链路层）：将网络层交下来的IP数据报组装成帧，在两个相邻的链路上传送帧。每一帧包括数据和必要的控制信息（如同步信息、地址信息、差错控制等）。

物理层：为设备之间的[数据通信](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E9%80%9A%E4%BF%A1/897073)提供传输媒体及互连设备，为[数据传输](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E4%BC%A0%E8%BE%93/2987565)提供可靠的环境。

**2.网络安全**

2.1主动攻击常见的几种方式

1. 篡改：攻击者故意篡改网络上传送的报文。这里也包括彻底中断传送的报文，甚至是把完全伪造的报文传送接收方。这种攻击方式有时也称为更改报文流。
2. 恶意程序：种类繁多，对网络安全威胁较大的主要有几种，即计算机病毒、计算机蠕虫、特洛伊木马、逻辑炸弹（一种当运行环境满足某种特定条件时执行其他功能的程序）、后门入侵、流氓软件。
3. 拒绝服务Dos：指攻击者向互联网上的某个服务器不停的发送大量分组，使服务器无法提供正常服务，甚至完全瘫痪。

对于主动攻击，可以采取适当措施加以检测。但对于被动攻击，通常确实检测不出来的。根据这些特点，可得出计算机网络通信安全的目标如下：

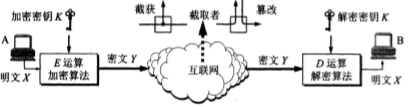
防止析出报文内容和流量分析

防止恶意程序

检测更改报文流和拒绝服务

2.2数据加密模型

一般的数据加密模型



两类密码体制

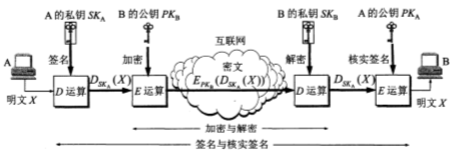
1. 对称密钥密码体制：加密密钥是使用相同的密码体制。
2. 公钥密码体制：使用不同的加密密钥与解密密钥。

公密密钥体制的产生主要有两个方面的原因，一是由于对称密钥密码体制的密钥分配问题，二是对数字签名的需求。

数字签名必须保证能够实现以下三点功能：

1. 接收者能够核实发送者对报文的签名。也就是说，接收者能够确信该报文的确是发送者发送的。其他人无法伪造对报文的签名。
2. 接收者确信所受到的数据和发送者发送的完全一样没有被篡改过。这就叫报文的完整性。
3. 发送者事后不能抵赖对报文的签名。

具有保密性的数字签名的实现

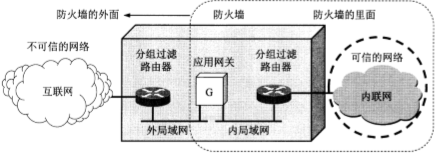


3.系统安全：防火墙与入侵检测

防火墙作为一种访问控制技术，通过严格控制进出网络边界的分组，禁止任何不必要的通信，从而减少潜在入侵的发生，尽可能降低这类安全威胁而带来的安全危险。由于防火墙不可能组织所有的入侵行为，作为系统反顾地第二道放心，入侵检测系统IDS通过对进入网络的分组进行深度分析与检测发现疑似入侵行为的网络活动，并报警以便进一步采取相应措施。

防火墙是一种特殊编程的路由器，安装在一个网点和网络的其余部分之间，目的是实施控制策略。这个访问控制策略是由防火墙的单位自行指定的。

防火墙在互联网中的位置：



3.1防火墙技术一般分为以下两类：

分组过滤路由器：一种具有分组锅炉功能的路由器，它根据过滤规则对进出内部网络分组执行转发或者丢弃（即过滤）。过滤规则是基于分组的网络层或运输层首部的信息，例如：源/目的IP地址、源/目的端口、协议类型（TCP或UDP）等。

应用网关、代理服务器

3.2入侵检测方法一般可以分为基于特征的入侵检测和基于异常的入侵检测

基于特征的IDS维护一个所有已知攻击标志性特征的数据库。每个特征是一种与某种入侵活动相关联的规则集，这些规则可能基于单个的首部字段值或数据中特定比特串，或者与一系列分组有关。当发现有与某种攻击特征匹配的分组或分组序列时，则认为可能检测到某种入侵行为。

基于特征的IDS只能检测已知攻击，对于未知攻击则束手无策。基于异常的IDS通过观察正常运行的网络流量，学习正常流量的统计特性和规律，当检测到网络中流量的某种统计规律不符合正常情况时，则认为可能发生了入侵行为。