第二节 计算机安全服务的主要技术

本节内容

一．网路攻击：主动攻击和被动攻击的概念和区别

二．安全服务

- 数据加密
- 身份认证
- 访问控制
- 入侵检测
- 防火墙

三．Windows7防火墙的基本功能

一、网络攻击

1、网络攻击分为主动攻击和被动攻击。

2、被动攻击

- 是指一切窃密的攻击，它往往没有既定的攻击目标，它主要针对信息的保密性进行攻击，即通过窃听网络上传输的信息并加以分析，从而获得有价值的情报，但它并不修改信息的内容，其目的是获得正在传送的信息

- 典型的攻击方式是网络窃听、流量分析和破译，通过截取数据包或流量分析，从中窃取重要的敏感信息。通过破译，窃取他人机密。被动攻击很难被发现，因此预防很重要，防止被动攻击的主要手段是数据加密传输。

3、主动攻击

- 通常有既定的攻击目标，它攻击信息来源的真实性、信息传输的完整性和系统服务的可用性

- 假冒：是一个实体假装成另一个实体，它通常包括一种其他形式的主动攻击。
- 重放：涉及被动捕获数据单元以及后来的重新发送，以产生未经授权的效果。
- 修改消息：意味着改变了真实消息的部分内容，或将消息延迟或重新排序，导致未授权的操作。
- 拒绝服务：是禁止对通信工具的正常使用或管理，这种攻击拥有特定的目标。另一种拒绝服务的形式是整个网络的中断，这可以通过使网络失效而实现，或通过消息过载使网络性能降低。

二、安全服务

为了保护网络资源免受威胁和攻击，在密码学及安全协议的基础上发展了网络安全体系中的多种安全服务，它们是：密码技术、认证技术、访问控制技术、入侵检测和不可否认技术，防火墙技术和防病毒技术等。

1、密码技术

- 使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性和可用性，防止信息被篡改、伪造或假冒。
- 需要隐藏的消息叫明文；
- 明文被变换成另一种隐藏形式被称为密文；
- 这种变换过程叫做加密；

- 加密的逆过程叫做解密；
- 对明文进行加密所采用的一组规则称为加密算法；
- 对密文解密时采用的有组规则称为解密算法；
- 加密算法和解密算法通常是在一组密钥控制下进行的；
- 加密算法所采用的密钥称为加密密钥；
- 解密算法所使用的密钥叫做解密密钥。

2、认证技术

认证是防止主动攻击的重要技术，是防
过程，它对于开放环境中的各种信息系
身份认证和消息认证。

- 身份识别：我是否知道你是谁？
- 身份验证：你是否是你所声称的你？

（1）身份认证

- 验证信息的发送者是真正的，而不是冒充的，这称为信源识别。同理验证信息的接收者是真正的，而不是冒充的，这称为信宿识别。
- 身份认证的方式有：账户名和口令认证（各类登录系统）、指纹、脸部、虹膜识别等。


淘宝会员
支付宝会员
账户名
手机号/会员名/邮箱
密 码
安全控件登录
登 录
忘记密码?
使用手机号码登录
免费注册
如您曾快速购买过商品，点此登录


MENU
10:51
/01
iFace 302
ZKSoftware

虹 膜

虹膜是盘状的薄膜，位于眼球的前方。

- 虹膜的模式极为复杂且每一个人各不相同，一个人的左眼和右眼或双胞胎的虹膜也不一样；
- 人在两岁后虹膜模式终生保持不变。

掌纹识别

指纹识别的下一阶段很可能是掌纹识别。相比于指纹，掌纹的复杂性更好，可识别范围更大，因此掌纹识别也就更加安全。

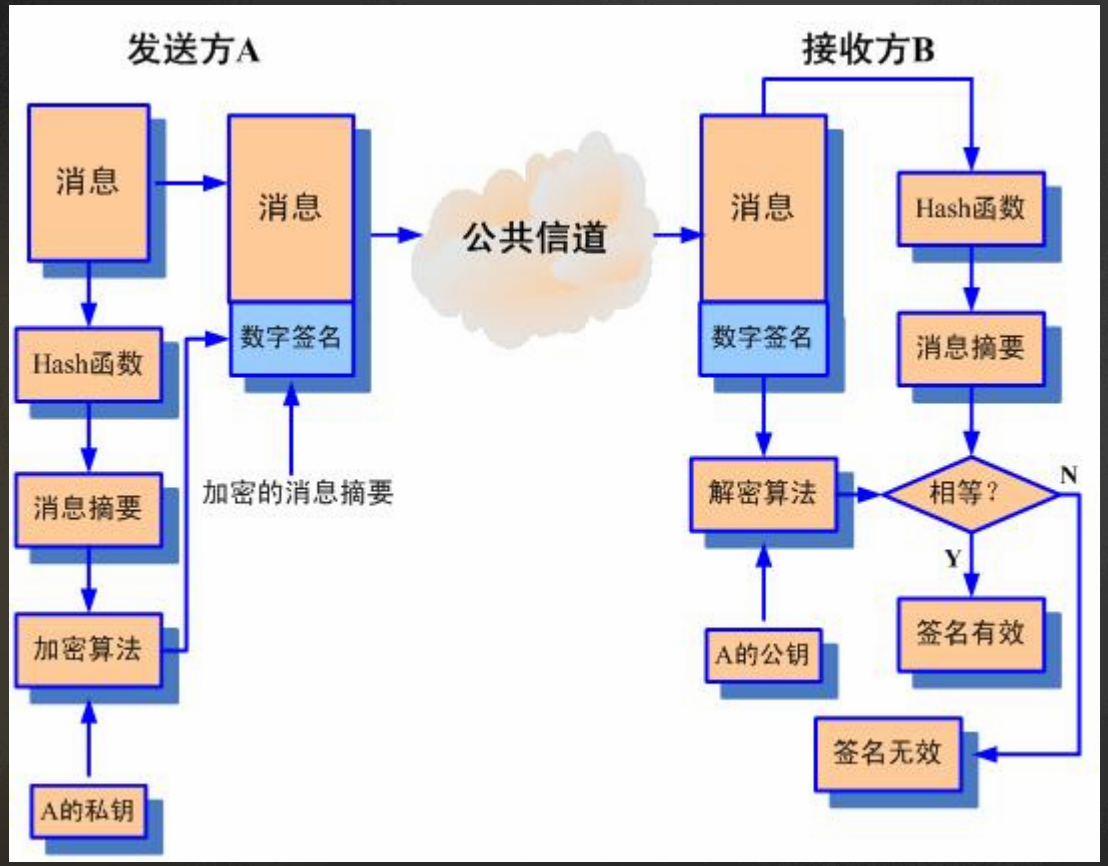
- 数字签名：

数字签名就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用以确认数据单元的来源和数据单元的完整性并保护数据,防止被人(例如接收者)进行伪造。

它是对电子形式的消息进行签名的一种方法,一个签名消息能在一个通信网络中传输

- 数字签名过程说明
  - 发信方用私钥对所发信件加密，收信方用发信方提供的公钥对所接收的信件解密
  - 由于收信方对密文解密是利用发信方提供的公钥，该公钥只能解密对应私钥（也就是发信方写信时的加密密钥）所加密的密文
  - 发信方不能否认发信行为，收信方因无法知道发信方的私钥，所以无法伪造、篡改发信方的信件。
  - 数字签名是个加密的过程，数字签名验证是个解密的过程。

- 数字签名的过程图


发送方A
接收方B
消息
消息
公共信道
消息
Hash函数
Hash函数
数字签名
数字签名
消息摘要
消息摘要
加密的消息摘要
解密算法
相等?
N
Y
加密算法
A的公钥
签名有效
A的私钥
签名无效

2、消息认证

- 消息认证的目的：确认消息内容是否曾今偶然或有意的篡改、消息的序号是否正确以及消息是否在指定的时间内到达
- 它在票据防伪中具有重要应用（如税务的金税系统和银行的支付密码器）
- 消息认证的主要技术是密码技术

- 消息内容认证常用的方法：消息发送者在消息中加入一个鉴别码，即附加校验数据（MAC、MDC等），并经加密后发送给接受者（有时只需加密鉴别码即可）。接受者利用约定的算法对解密后的消息进行鉴别运算，将得到的鉴别码与收到的鉴别码进行比较，若二者相等，则接收，否则拒绝接收。

3、访问控制

- 目的：决定谁能访问系统、能访问系统的何种资源以及访问这些资源所具有的权限。权限是指：读取数据、更改数据、运行程序、发起连接等，从而使计算机资源在合法范围内使用
- 访问控制通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。

- 访问控制的手段包括用户识别代码、口令、登录控制、资源授权、授权核查、日志和审计。访问控制有两个重要过程：

① 通过“鉴别”来检验主体的合法身份；

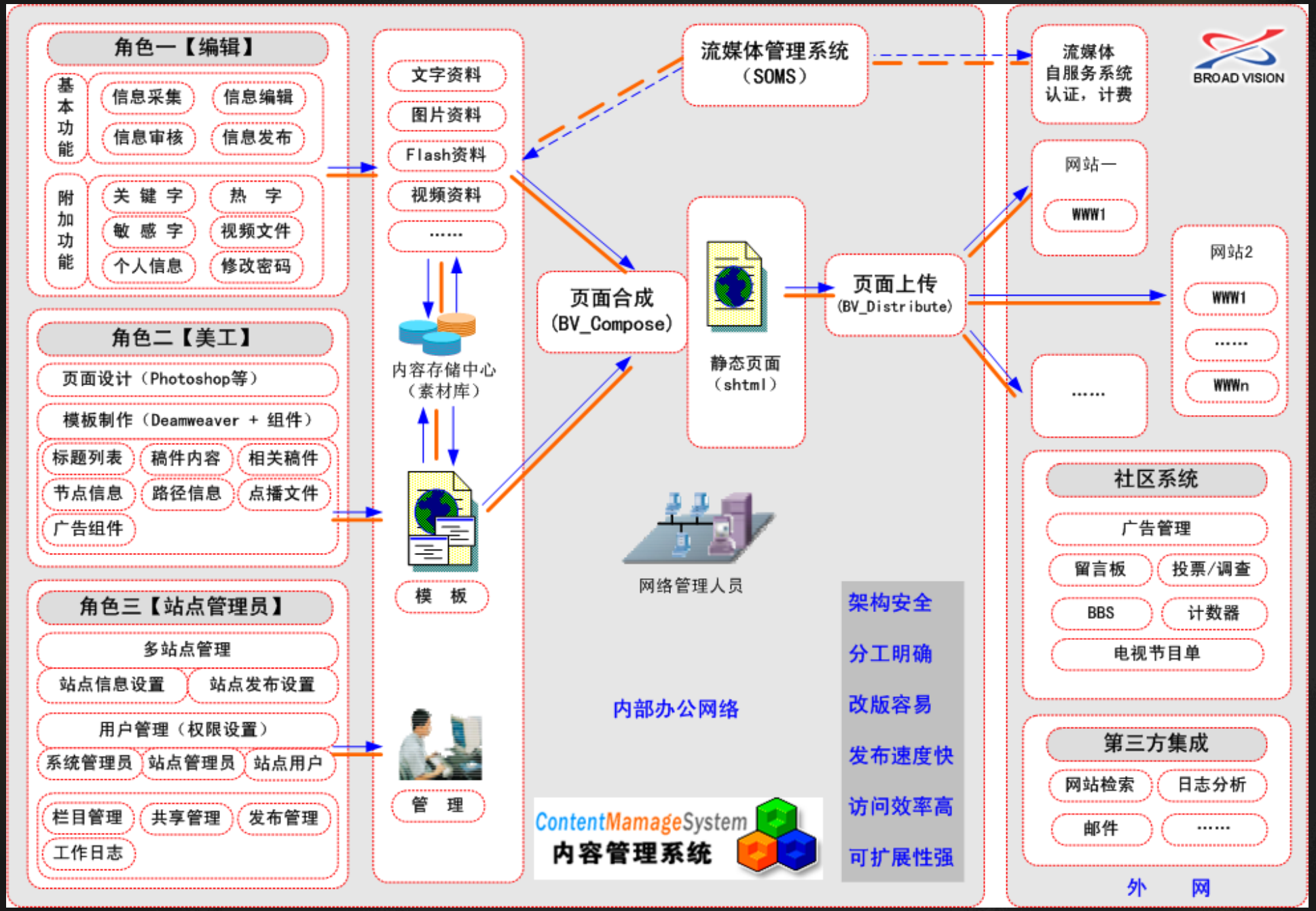
② 通过“授权”来限制用户对资源的访问级别。

- 根据实现的技术不同，访问控制可分为以下三种：

① 强制访问控制；

② 自主访问控制；

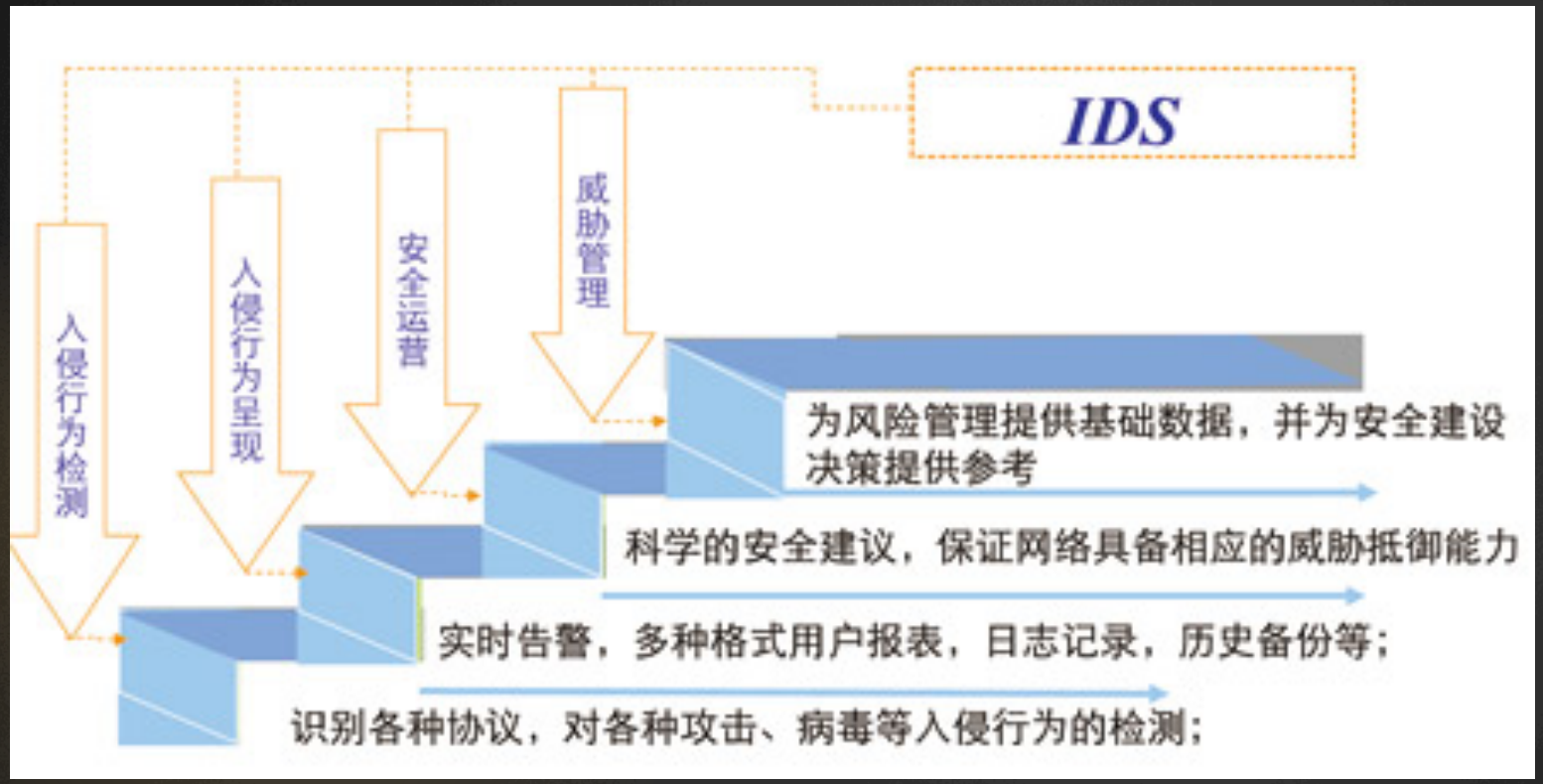
③ 基于角色的访问控制。


角色一【编辑】
基本功能
信息采集
信息编辑
信息审核
信息发布
附加功能
关 键 字
热 字
敏 感 字
视频文件
个人信息
修改密码
角色二【美工】
页面设计（Photoshop等）
模板制作（Deamweaver + 组件）
标题列表
稿件内容
相关稿件
节点信息
路径信息
点播文件
广告组件
角色三【站点管理员】
多站点管理
站点信息设置
站点发布设置
用户管理（权限设置）
系统管理员
站点管理员
站点用户
栏目管理
共享管理
发布管理
工作日志
文字资料
图片资料
Flash资料
视频资料
……
内容存储中心
（素材库）
模 板
管 理
流媒体管理系统
（SOMS）
页面合成
(BV_Compose)
静态页面
（shtml）
页面上传
(BV_Distribute)
网络管理人员
内部办公网络
架构安全
分工明确
改版容易
发布速度快
访问效率高
可扩展性强
ContentMamageSystem
内容管理系统
流媒体
自服务系统
认证，计费
BROAD VISION
网站一
WWW1
网站2
WWW1
……
WWWn
……
社区系统
广告管理
留言板
投票/调查
BBS
计数器
电视节目单
第三方集成
网站检索
日志分析
邮件
……
外 网

4、入侵检测

- 就是对入侵行为的发觉。他通过对计算机网络或计算机系统中若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。
- 入侵检测作为一种积极主动地安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。因此被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测

IDS: “Intrusion Detection Systems”



5、防火墙

（1）防火墙的概念

防火墙是一个或一组在两个不同安全等级的网络之间执行访问控制策略的系统，它由硬件和软件共同组成，通常处于企业的局域网和Internet之间，目的是保护局域网不被Internet上的非法用户访问，同时也可管理内部用户访问Internet的权限。

- 本质上，它遵从的是一种允许或阻止业务来往的网络通信安全机制，也就是提供可控的过滤网络通信，只允许授权的通信。
- 其目的如同一个安全门，既为门内的内网用户访问外网提供安全，也对门外的外网用户访问内网进行控制。
- 防火墙可根据是否需要专门的硬件支持分为硬件防火墙和软件防火墙。

（2）防火墙的功能

① 所有进出网络的通信流都应该通过防火墙；

② 所有穿过防火墙的通信流都必须有安全策略的确认与授权。

6、Windows7软件防火墙（实操部分讲解）

- Windows7防火墙的启动
- 网络的选择
- 个性化设置
- 使用高级设置配置文件

7、日志（实操部分讲解）

- 日志是一种特殊的文件，其特殊性是在于：一是它通常由系统管理，并加以保护，一般情况下，普通用户不能随意更改；二是：不是文本类型的文件
- 日志包括：系统日志、安全日志、程序日志等