

Cyber Security Review

GuLyue

Chapter1 网络安全基本概念

1. Information Security: 保护数据，防止黑客的工具
2. Network Security: 传输过程中保护数据的方法
3. Internet Security: 保护数据在互联网中的传输的方式

CyberSpace:

广泛，无处不在的网络

网络安全问题产生根源：

内因：网络信息系统复杂度：过程复杂，结构复杂，应用复杂

外因：人为和环境：威胁与破坏

网络安全发展阶段历程

通信安全

计算机安全

信息系统安全

信息安全保障

网络空间安全/信息安全保障

网络安全三要素

保密（未经授权使用信息），完整（对信息非法修改和破坏），可用（及时可靠的使用信息）

ISO/OSI

以防护为主的静态安全体系结构

不是能实现的标准，而是如何设计标准的标准

安全攻击

1. 主动攻击

- 伪装：冒名顶替，伴随其他主动攻击
- 重放：先被动的接受认证信息，再把认证信息发送给认证服务器
- 篡改：修改报文的内容，对截获的报文延迟，重新排序（完整性）
- 拒绝服务：组织或占据对通信设施的正常使用或管理，针对特定目标或整个网络（可用性）

2. 被动攻击

- 报文分析：窃听和分析所传输的报文内容
- 流量分析：分析通信主机的位置，通信的频繁程度，报文长度等信息

中断：可用性

窃听：机密性

修改：机密性

伪造：认证，不可否认性

ISO/OSI：

- 安全服务：对象认证服务，访问控制，数据保密性，数据完整性，防抵赖性

服务	机制	加密	数字签名	访问控制	数据完整性	认证交换	防业务流量分析	路由控制	公证
对等实体认证		√	√			√			
数据起源认证		√	√						
访问控制				√					
连接机密性		√						√	
无连接机密性		√						√	
选择字段机密性		√							
流量机密性		√					√	√	
可恢复的连接完整性		√			√				
不可恢复的连接完整性		√			√				
选择字段的连接完整性		√			√				
无连接完整性		√	√		√				
选择字段的无连接完整性		√	√		√				
传递过程的非否认			√		√				√
数据起源的非否认			√		√				√

网络安全模型

Sender-> Security-related transformation -> Information Channel -> Security related transformation->Recipient

网络访问安全模型

Opponent --> Access Channel --> GateKeeper function --> Information System

网络安全基本认识

1. 没有绝对的安全
2. 安全是一个动态构成
3. 人是安全机制中最薄弱环节
4. 安全包括外部和内部的安全
5. 木桶原理

信息安全标准介绍

TCSEC (美国桔皮书) 可信计算机系统评估准则, 美国国防部评估标准

可信网络解释 (TNI) 红皮书

信息技术安全评测标准 (ITSEC) 欧洲白皮书

TESEC

计算机系统安全评估的第一个正式标准

ABCD四类八个等级

A最高, D最低

四个安全等级

无保护级, 自主保护级, 强制保护级, 验证保护级

可信计算基 (TCB)

通信安全:

密码技术解决通信保密, 保证数据的保密性和完整性

主要关注传输过程中的数据保护

计算机安全

预防检测和减少计算机系统用户执行的未授权活动所造成的后果 (TCSEC)

信息系统安全

综合通信安全和计算机安全

信息安全保障

确保信息的保密性，完整性和可用性

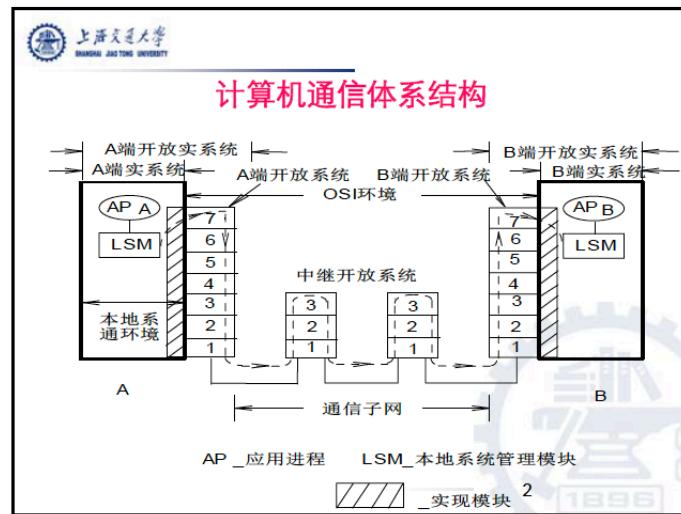
网络空间安全/信息安全保障

CS/IA: Cyber Security/Information Assurance

从传统的信息保障 (IA) , 发展成威慑为主的防御、攻击和情报三位一体的信息保障/网络安全的网空安全

- 网络防御-Defense (运维)
- 网络攻击-Offense (威慑)
- 网络利用-Exploitation (情报)

Chapter2 计算机网路基础



路由系统只有三层，终端系统有7层 (OSI模型)

计算机网的协议单元

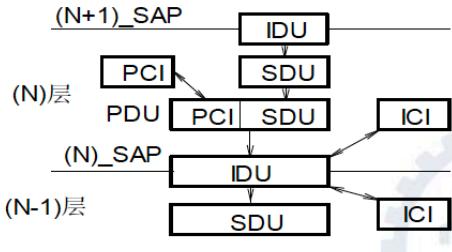


图 2 - 3

3

IDU: interface data unit

SDU: service data unit

PCI: protocol control unit

PDU: protocol data unit (网络层: 包, 链路层: 帧, 传输层: 数据段, 传输层及以上报文)

SAP: service access point

首部

应用层, 传输层, 网络层和链路层都会把上一层的数据当成payload, 之前加上自己的头部

链路层还有尾部

网络互联实现层次

- 转发器

实现于物理层。主要是物理信号的放大和重整, 用于同构网络的扩展。

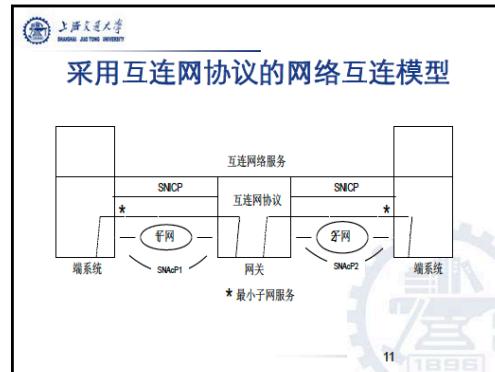
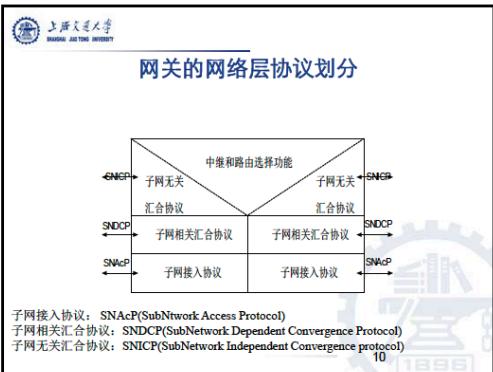
- 桥接器

实现于数据链路层。主要是帧级的存储和转发, 用于同类网络的互连。

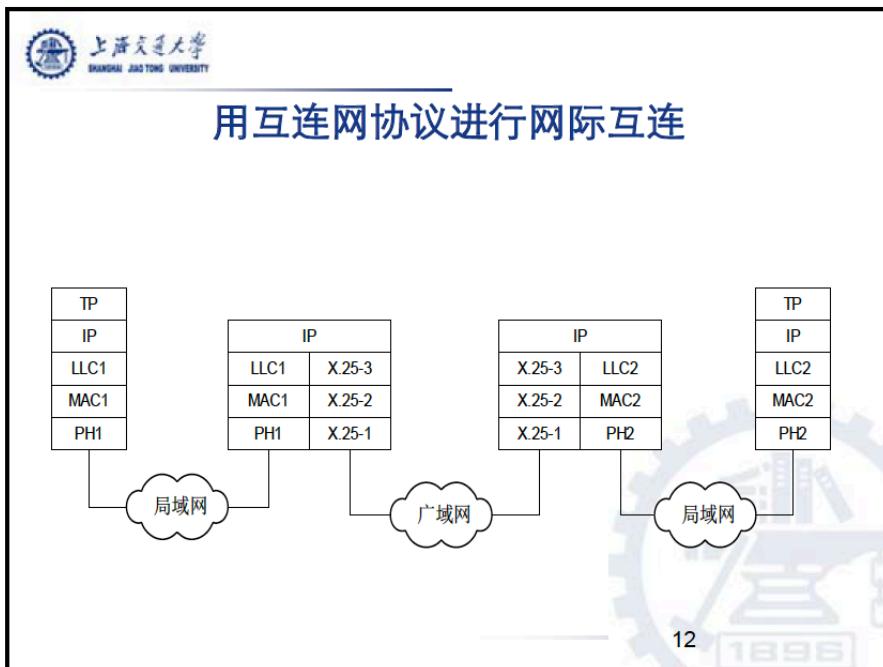
- 多协议路由器

实现于网络层。将重点讨论其原理及实现方法。

- 高层网关实现于网络层之上。将讨论逐跳法的网络互连及其在网络安全中的应用。



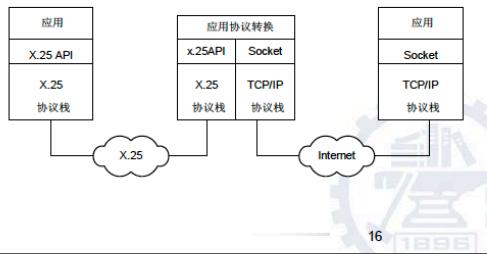
互联网协议网际互联



网络层互联

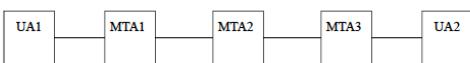
- 虚电路方式
- 无连接方式
- IP路由器

应用网关互连



16

邮件系统互连方式



17

网关协调子网之间的差异

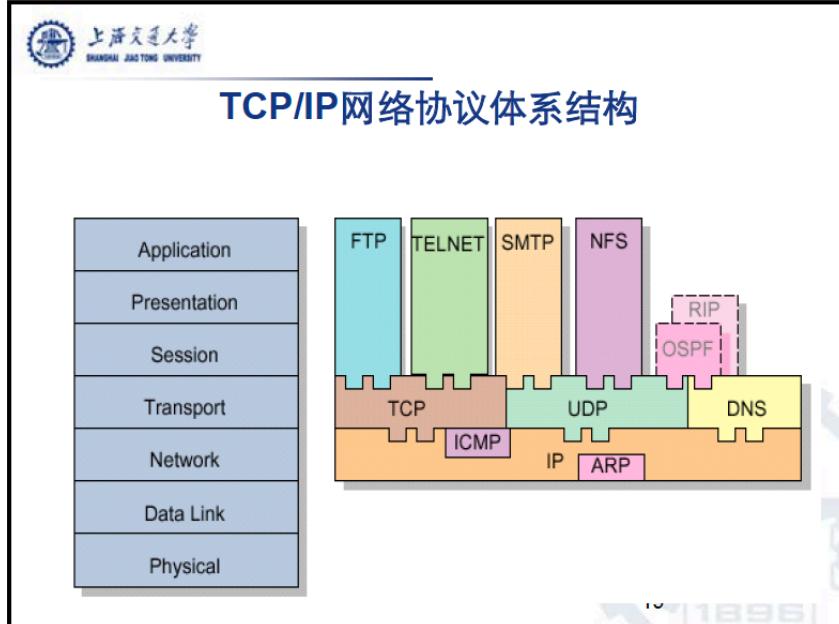
子网间可能出现的差异

项目	可能的差异
服务类型	面向连接或无连接
实子网协议	802.X 或 X.25
子网地址格	48 位以太网址或 X.121
广播	支持或不支持
分组长度	各子网有不同的 MTU
服务质量	提供或不提供保证
流量控制	滑窗式流量控制或不提供
网络参数	各种不同的定时器
计费	依据时间、流量等

18

TCP/IP 网络协议体系 (7层)

TCP/IP网络协议体系结构



TCP/IP概念系统结构

TCP：操作系统内的软件

IP：仅使用IP地址

网络接口以及硬件：仅使用物理地址

TCP/IP协议栈

应用层：TELNET, FTP

传输层：TCP, UDP

网络层：IP

链路层：Ethernet, 802.2, 802.3

物理层：双绞线，同轴线，光纤

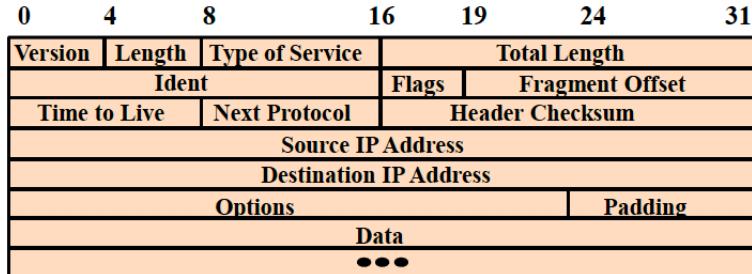
IP协议

- 不可靠，无连接
- IP数据报可能会被投错，没有通知
- 规定了数据格式，分组处理和出错控制

IP包格式



IP 报头格式



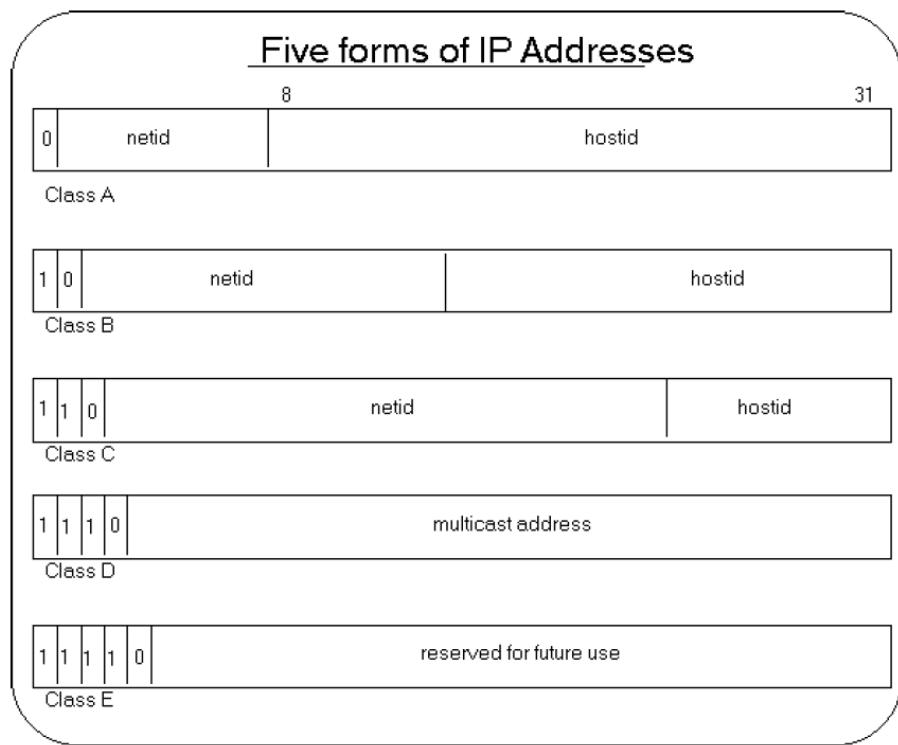
- ④ Version 是 IP 规范所发布的版本号 4 或 快要使用版本 6。
- ④ Length 是 IP报头的长度 (32 比特字长)。
- ④ 总长度 (Total Length)是以八位组计量的 IP 数据报长度，包括报头和数据。

23

IP地址

5类IP地址

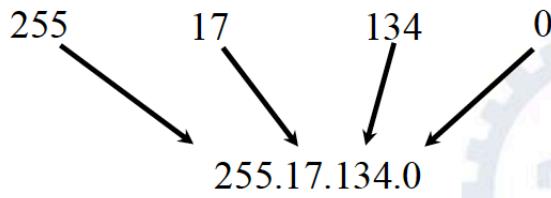
IP地址的类型及其表示



High Order Bits	Octet in Decimal	Address Class
0	1 -126	A
10	128 -191	B
110	192 -223	C

点分十进制表示的IP地址

0	8	16	24
11111111	00010001	10000111	00000000



 上海交通大学
SHANGHAI JIAOTONG UNIVERSITY

IPv4版本TCP/IP的安全缺陷

- 缺乏对用户身份的鉴别
- 缺乏对路由协议的鉴别认证
- TCP/UDP的缺陷
- TCP/IP本身不提供加密传输功能
- 下层的安全缺陷必然导致应用层的安全出现漏洞甚至崩溃
- 由TCP/IP支持的Internet中的各个子网难以实现分级安全的网络结构(如树状结构)，无法实现有效的安全管理。

网络服务安全问题

1. Web服务

操作系统本身安全漏洞，明文或弱口令，Web服务器本身漏洞，脚本程序，Web欺骗

2. FTP服务

匿名登陆，FTP代理服务器，调拌攻击

3. Telnet安全

传输明文，无强力认证，没有完整性检查，传输数据没有加密

4. 电子邮件

软件问题，缓存漏洞，历史记录漏洞，攻击性代码漏洞

5. DNS

域名欺骗，网络信息泄漏，服务器拒绝服务，远程漏洞

6. 路由服务

- 将受控机器的IP地址设置为路由器的IP地址，引起IP地址冲突，破坏路由器的正常运行机制。
- 破坏和干扰路由服务器的域名解析。
- 将受控机器的物理地址随机配置为路由器的物理地址，干扰路由器的运行。
- 构造垃圾网络数据包，发送给路由器，造成拒绝服务攻击。
- 劫持路由器之间的会话连接。
- 破解路由器的弱口令。
- 伪造路由更新消息。

服务	分层							
	物理层	数据链路层	网络层	传输层	会话层	表示层	应用层	
对等实体认证			√	√				√
数据起源认证			√	√				√
访问控制			√	√				√
连接机密性	√	√	√	√		√		√
无连接机密性			√	√		√		√
选择字段机密性						√		√
流量机密性	√		√					√
可恢复的连接完整性				√				√
不可恢复的连接完整性			√	√				√
选择字段的连接完整性								√
无连接完整性			√	√				√
选择字段的无连接完整性								√
传递过程的非否认								√
数据起源的非否认								√

Chapter3 密码技术与用户认证

密码学发展的两个阶段：古典密码以及现代密码

密码学的重要性：机密性，完整性，有效性，可认证性，不可否认性

1. 古典密码学

古典密码体制的安全性在于保证算法本身的保密性

- 不适合大规模生产
- 不适合人员变动较大的组织
- 用户无法了解算法的安全性

种类：

- 替换密码（凯撒密码，有替换表）
- 置换密码（对明文字符按某种规律进行位置的置换）
- 替换密码与置换密码的组合

2. 现代密码学

Shannon: The communication Theory of Secret Systems

Rivest, Shamir & Adleman提出了RSA公钥算法

新特点：数据的安全基于秘钥而不是算法的保密

公钥密码使得发送端和接收端无密钥传输的保密通信成为可能

3. 加密，解密

加密和解密算法的操作都是在一组密钥的控制下进行的，分别称为**加密密钥，解密密钥**

4. 分组密码

分组密码是将明文消息编码后表示的数字（简称明文数字），划分成都为n的组，在密钥的控制下变成等长的输出数字序列

加密前后消息长度不变，但加密的密钥长度不一定

密钥越长越安全

设计原则：

- 针对安全性的原则

置换算法复杂，实现明文和密钥的扩散和混乱

分组长度足够长

- 混乱原则：

明文和密文之间的依赖关系足够复杂（防止根据明文和密文之间的依赖关系进行破译）

- 扩散原则：

密钥和明文的每位数字能够影响密文中的多位数字（防止逐段破译）

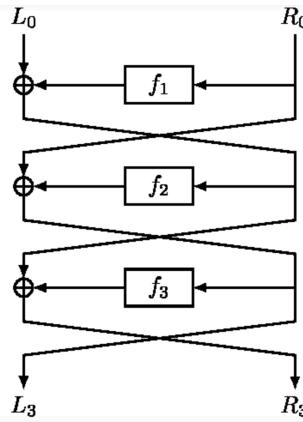
- 针对攻击的原则

必须能抵抗现有的攻击方法，差错传播小，一般无数据扩展

- 针对实现的原则

加解密运算简单，易于软硬件实现

Feistel密码结构



每一轮的秘钥由上一轮的秘钥生成 主要流程如下：先把明文分成左边和右边两部分，首次先对右边进行F变换，之后与左边做异或，最后交换左边和变换后的右边

要素: Block size (64) Key Size (128) # of rounds (16) SubKey Generation Round function

数据加密标准DES

DES: 分组密码，常规密钥密码体制

加密前先对整个密文分组，每个组64bit

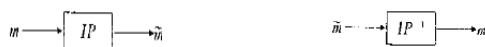
在对每个bit分别做加密，最后串起来

使用的密钥64bit (56bit密钥, 8bit奇偶校验)



1. IP是初始置换, IP^{-1} 是它的逆变化, 满足

$$IP \cdot IP^{-1} = IP^{-1} \cdot IP = I \quad (I \text{为单位阵})$$



设 $m = m_1 m_2 \cdots m_{64}$, $\tilde{m} = \tilde{m}_1 \tilde{m}_2 \cdots \tilde{m}_{64}$
 $\tilde{m} = m_{58} m_{56} m_{42} \cdots m_{23} m_{10} m_7$
即 $\tilde{m}_1 = m_{58}$, $\tilde{m}_2 = m_{56}$, ..., $\tilde{m}_{64} = m_7$

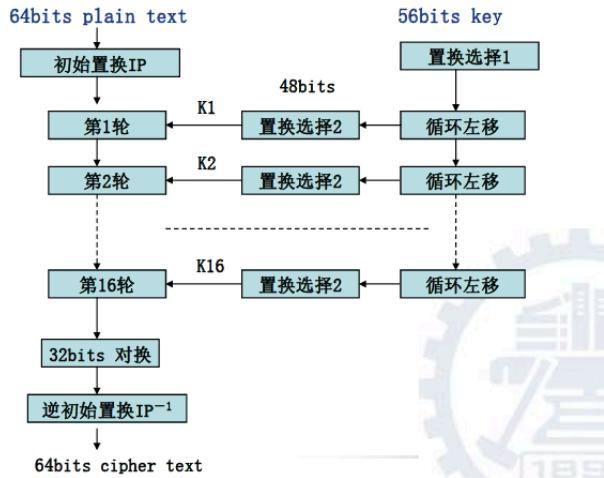
若 $\tilde{m} = \tilde{m}_1 \tilde{m}_2 \cdots \tilde{m}_{64}$

则 $m = \tilde{m}_{40} \tilde{m}_{38} \tilde{m}_{42} \cdots \tilde{m}_{23} \tilde{m}_{10} \tilde{m}_7$

P置换的目的是提供雪崩效应（明文或密钥的一点小的变动都引起密文的较大变化）

2.DES迭代(16轮), 在这里数据和密钥结合

IP置换：把输入的64位数据按位重新组合，并把输出分为L0、R0两部分，每部分各长32位



DES的保密性取决于对密钥的保护，算法是公开的

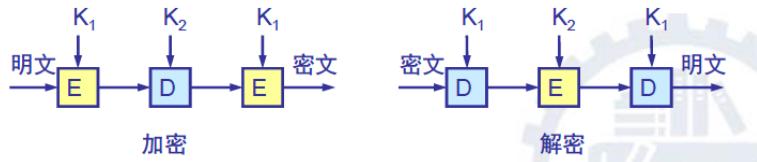
DES是世界上第一个公认的实用密码算法标准

较为严重的问题是DES的密钥长度

现在已经设计出来搜索DES密钥的专用芯片

三重DES

使用两个密钥，进行三次DES算法



对称密码

- 分组密码 (DES,IDEA,RC2,RC5)

在明文分组和密文分组上进行运算，分成固定长度的组，通常为64bits，相同的明文和相同的密钥得到相同的密文，输出也是固定长度

- 序列密码（流密码）(One-time padding,Vigenere,Vernam)

作用在明文和密文的数据序列的1bit或1byte上

安全三要素

- 完整
- 机密
- 可用

消息认证

- 报文鉴别

证实收到的报文或消息来自可信的源点且未被篡改的过程

- 散列函数

一个散列函数以一个变长的报文作为输入并产生一个等长的散列码，有时也称为报文摘要，作为输出

鉴别

防止主动攻击，对开放网络的各种信息系统安全有重要作用

目的：

- 信源识别
- 验证信息完整性，未被篡改，重放或延迟

鉴别函数

- 加密函数：用完整信息的密文作为鉴别码，实现对报文的鉴别
- 散列函数：采用一个公共散列函数，将任意长的报文映射成一个固定长度的散列值作为鉴别符
- 报文鉴别码MAC (Message Authentication Code)：公共函数+密钥产生一个固定长度的值作为鉴别标志

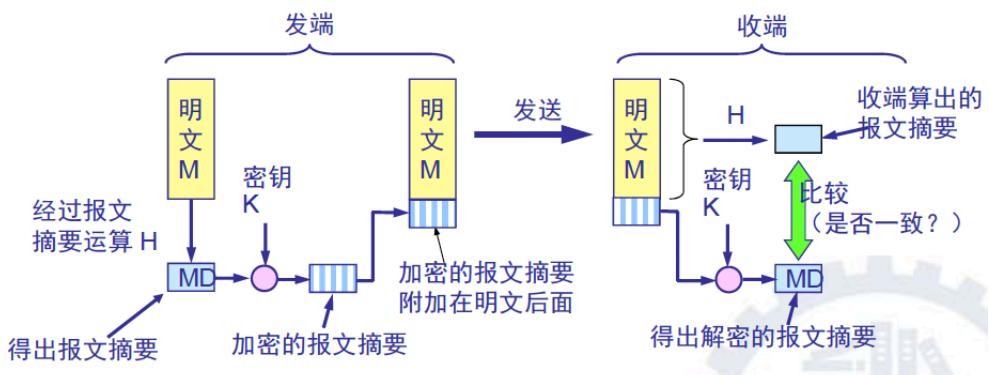
报文摘要

要求：

报文摘要算法必须满足 以下两个条件

- ① 任给一个报文摘要值 x ，若想找到一个报文 y 使得 $H(y) = x$ ，则在计算上是不可行的。
- ② 若想找到任意两个报文 x 和 y ，使得 $H(x) = H(y)$ ，则在计算上是不可行的。

报文摘要的实现



发送端对报文经过报文摘要算法运算，得到固定长度的报文摘要，然后对它进行加密，追加在报文后发送出去

接收端解密还原报文摘要，再将接收到的报文进行报文摘要运算，看看两者是否一样

优点：对报文摘要进行加密比整个长报文进行加密要简单得多

报文和报文摘要合在一起是可检验的和不可伪造的

散列函数

生成消息摘要的函数

生成的散列值可以提供错误检测能力，散列值唯一对应原始报文，消息中的任何一位或多位的变化都将导致散列值的变化

应用：明文认证，数字签名，可以认为是对明文的签名



关于散列函数一些定义

定义1(弱无碰撞)，散列函数 h 称为是弱无碰撞的,是指对给定消息 $x \in X$, 在计算上几乎找不到异于 x 的 $x' \in X$ 使 $h(x)=h(x')$ 。

定义2(强无碰撞)散列函数 h 被称为是强无碰撞的,是指在计算上不可能找到相异的 x, x' 使得 $h(x)=h(x')$ 。

定义3(单向的)称散列函数 h 为单向的，是指计算 h 的逆函数 h^{-1} 在计算上不可行。

定义4 (带秘密密钥的Hash函数)：消息的散列值由只有通信双方知道的秘密密钥 K 来控制。此时，散列值称作MAC。

定义5 (不带秘密密钥的Hash函数)：消息的散列值的产生无需使用密钥。此时，散列值称作MDC。



HASH 函数 $h = H(M)$

满足：

- 1、 H 可以作用于一个任意长度的数据块；
- 2、散列函数 H 必须对任意长度的明文产生固定长度的散列函数值；
- 3、对任意给定的明文 x ,无论是软件还是硬件实现 $H(x)$ ，计算都相对容易。
- 4、对任意给定码 h , 找到 x 满足 $H(x)=h$ 具有计算不可行性；（单向性）
- 5、对任何给定的报文 M , 若要寻找不等于 M 的报文 M_1 使 $H(M_1) = H(M)$ 在计算上是不可行的。
- 6、要找到两个报文 M 和 N 使 $H(M)=H(N)$ 在计算上是不可行。

前三条要求具有**实用性**，第4条是**单向性质**，即给定消息可以产生一个散列码，而给定散列码不可能产生对应的消息。第5条性质是保证一个给定的消息的散列码不能找到与之相同的另外的消息，即**防止伪造**。第6条是对已知的生日攻击方法的**防御能力**。

Hash与MAC之间的区别

与密钥相关的单项散列函数称为MAC

MAC计算速度慢

Hash是一种直接产生鉴别码的方法，不需要密钥，对任意长度的报文直接产生定长的鉴别码

几种常见的HASH算法

- RSA (可以用来签名，效率低，难以实用==>MD算法)
- MD5
- SHA-1(美国政府的安全Hash标准)
- RIPEMD-160
- HMAC

MD5

迭代结构：如果压缩函数能够抵抗碰撞的话，那么合成的迭代函数也有这样的性质

设计碰撞抵抗的压缩函数

攻击MD5方法：

- 直接攻击（穷举，太久了）
- 生日攻击（概率）
- 其他攻击（微分攻击，对MD5的一次循环是有效的，但对全部4次循环无效）

SHA

安全散列函数，美国标准局（NIST）为了配合数字签名算法（DSA）发布的，依据MD4

明文预处理和MD5一样：预处理后的密明文是512位的整数倍，SHA输出为160位，分别存储与5个32位的记录单元

- 安全性：摘要长度比MD5多了32位
- 速度：比MD5慢了25%
- 简易性：每一步操作比MD5简单
- 数据的存储方式：MD5:little-endian, SHA: big-endian

HMAC

传统构造MAC采用分组密码

将散列函数与密钥结合起来产生鉴别码==>基于散列函数的报文鉴别码

优点：

- 无需修改地使用现在的散列函数
- 当出现新的散列函数时能轻易替换
- 不导致算法性能的降低
- 处理和使用密钥简单
- 对鉴别机制的安全强度容易分析，与hash函数有同等的安全性

对称密码和非对称密码

1. 对称密码:

加密密钥和解密密钥相同，或一个易于推出另一个（又称传统算法，秘密密钥算法或单密钥算法）
DES, 3DES, IDEA, AES

2. 非对称密码算法

加密密钥和解密密钥不同，很难从一个退出另一个
又叫公钥密码算法
公钥和私钥
RSA, ECC, ElGamal

公开密钥密码体制

用途：

- 解决常规密钥密码体制的密钥分配问题
- 数字签名

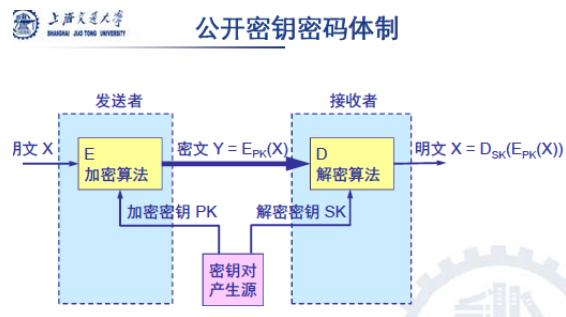
RSA：基于数论中大数分解问题的体制

加密密钥与解密密钥

公钥公开，私钥保密

加解密算法公开

虽然私钥由公钥决定，但不能通过公钥计算出私钥



公开密钥算法的特点

(1) 发送者用加密密钥 PK 对明文 X 加密后，在接收者用解密密钥 SK 解密，即可恢复出明文，或写为：

$$D_{SK}(E_{PK}(X)) = X \quad (9-5)$$

- 解密密钥是接收者专用的秘密密钥，对其他人都保密。
- 此外，加密和解密的运算可以对调，即

$$E_{PK}(D_{SK}(X)) = X$$

特点：

公钥公开，但不能解密

很容易产生公钥和私钥

公钥不可能计算出私钥

公钥算法和私钥算法是公开的

RSA公开密钥密钥体制

原理：根据数论，寻求两个大素数比较简单，而将它们的乘积分解则极其困难。



上海交通大学

RSA 公开密钥密码体制

- ④ 原理：根据数论，寻求两个大素数比较简单，而将它们的乘积分解则极其困难。|
- ⑤ 每个用户有两个密钥：加密密钥 $PK = \{e, n\}$ 和解密密钥 $SK = \{d, n\}$ 。
- ⑥ 用户把加密密钥公开，使得系统中任何其他用户都可使用，而对解密密钥中的 d 则保密。
- ⑦ n 为两个大素数 p 和 q 之积（素数 p 和 q 一般为 100 位以上的十进数）， e 和 d 满足一定的关系。当敌手已知 e 和 n 时并不能求出 d 。

④ 若用整数 X 表示明文，用整数 Y 表示密文（ X 和 Y 均小于 n ），则加密和解密运算是：

加密：
$$Y = X^e \bmod n \quad (9-7)$$

解密：
$$X = Y^d \bmod n \quad (9-8)$$

① 计算 n 。用户秘密地选择两个大素数 p 和 q ，计算出 $n = pq$ 。 n 称为 RSA 算法的模数。明文必须能够用小于 n 的数来表示。实际上 n 是几百比特长的数。

② 计算 $\phi(n)$ 。用户再计算出 n 的欧拉函数

$$\phi(n) = (p - 1)(q - 1) \quad (9-9)$$

$\phi(n)$ 定义为不超过 n 并与 n 互素的数的个数。

③ 选择 e 。用户从 $[0, \phi(n) - 1]$ 中选择一个与 $\phi(n)$ 互素的数 e 作为公开的加密指数。

 上海交通大学 (2) 密钥的产生 (续)

- ④ 计算 d 。用户计算出满足下式的 d

作为解密指数。

- ⑤ 得出所需要的公开密钥和秘密密钥：

公开密钥（即加密密钥） $\text{PK} = \{e, n\}$

秘密密钥（即解密密钥） $\text{SK} = \{d, n\}$

(3) 正确性的例子说明

设选择了两个素数， $p = 7, q = 17$ 。

计算出 $n = p * q = 7 \times 17 = 119$ 。

计算出 $\phi(n) = (p - 1)(q - 1) = 96$ 。

从[0, 95]中选择一个与 96 互素的数 e 。

选 $e = 5$ 。然后根据(9-10)式，

$$5^d \bmod 96 = 1$$

解出 d 。不难得出， $d = 77$ ，因为 $e^d = 5^77 = 385 = 4 \times 96 + 1$ ， $(4 \times 96 + 1) \bmod 96 = 1$ 。

于是，公开密钥 $PK = (e, n) = \{5, 119\}$ ，

秘密密钥 $SK = \{77, 119\}$ 。

(3) 正确性的例子说明 (续)

对明文进行加密。先把明文划分为组，使每个明文分组的二进制值不超过 n ，即不超过 119。

设明文 $X = 19$ 。用公开密钥加密时，先计算

$$X^e = 19^5 = 2476099$$

再除以 119，得出商为 20807，余数为 66。这就是对应于明文 19 的密文 Y 的值。

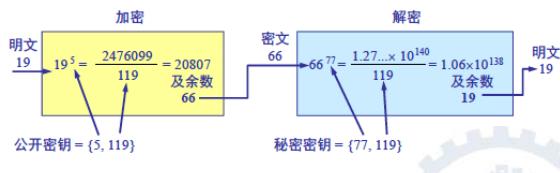
在用秘密密钥 $SK = \{77, 119\}$ 进行解密时，先计算

$$Y^d = 66^{77} = 1.27... \times 10^{140}$$

再除以 119，得出商为 $1.06... \times 10^{138}$ ，余数为 19。

此余数即解密后应得出的明文 X 。

RSA 算法举例



RSA缺点：

产生密钥麻烦，也难做到一次一密

加解密速度很慢

比DES慢1000倍

Diffie-Hellman密钥交换

允许两个用户安全交换信息，用于后续的通讯过程

大量商用产品使用这种密钥交换技术

算法的安全性依赖于计算离散对数的难度

素数 p 的原始根定义：如果 a 是素数 p 的原始根，则数 $a \bmod p, a^2 \bmod p, \dots, a^{p-1} \bmod p$ 是不同的并且包含 1 到 $p-1$ 的所有整数的某种排列。对任意的整数 b ，我们可以找到唯一的幂 i 满足 $b = a^i \bmod p$ $0 <= i <= (p-1)$ 。在离散对数算法中称为对于基数 a 和运算 $\bmod p$ 的离散对数。记为 $ind_{a,p}(b)$

算法：

- 双方选择素数p以及p的一个原根a • 用户A选择一个随机数 $X_a < p$, 计算 $Y_a = a^{X_a} \bmod p$ • 用户B选择一个随机数 $X_b < p$, 计算 $Y_b = a^{X_b} \bmod p$ • 每一方保密X值, 而将Y值交换给对方 • 用户A计算出 $K = Y_b^{X_a} \bmod p$ • 用户B计算出 $K = Y_a^{X_b} \bmod p$ • 双方获得一个共享密钥($a^{X_a X_b} \bmod p$) 素数p以及p的原根a可由一方选择后发给对方

公钥密码基于的数学难题

- 背包问题
- 大整数分解问题 (RSA)
- 有限域的乘法群上的离散对数问题 (ElGamal)
- 椭圆曲线上的离散对数问题 (类比的ElGamal)



密码技术在信息安全中的作用

信息安全要素	所应付的典型威胁	可用的密码技术
机密性 (Confidentiality)	<ul style="list-style-type: none">• 窃听• 非法窃取资料• 敏感信息泄露	对称加密和非对称加密 数字信封
完整性 (Integrity)	<ul style="list-style-type: none">• 篡改• 重放攻击• 破坏	哈希函数和消息认证码 数据加密 数字签名
可鉴别性 (Authentication)	<ul style="list-style-type: none">• 冒名	口令和共享秘密 数字证书和数字签名
不可否认性 (Non-repudiation)	<ul style="list-style-type: none">• 否认已收到资料• 否认已送资料	数字签名 证据存储
授权与访问控制 (Authorization & Access Control)	<ul style="list-style-type: none">• 非法存取资料• 越权访问	属性证书 访问控制

认证实例

Kerberos

X.509鉴别服务

密钥管理

密钥重要性：所有密码技术都依赖于密钥

科克霍夫原则：安全性的关键点

目的：

- 保护密钥不被泄露 • 保护密钥不被非授权使用

密钥生命周期

授权使用该密钥的周期

原因：

- 1 限制密钥使用时间——时间分割 • 2 限制产生密文数量——数量分割 • 3 限制密码分析攻击的有效时间 • 4 降低已泄露密钥所造成的损失

密钥产生

1. 密钥长度
 - 安全性考虑 • 系统成本、计算开销考虑 • 长度的选择与具体的应用有关，如加密数据的重要性、保密期限长短、可能破译者的计算能力等。
2. 密钥产生的方法
 - 集中式 • 分散式

密钥管理的其他阶段

1. 密钥使用 • 注意内存的密钥泄露。私钥不出硬件设备（密码机、USB Key） • 不同用途使用不同的密钥
2. 密钥存储 • 硬盘存储或专用硬件存储，现更多存储在专用硬件中
3. 密钥更新 • 定期或不定期更换密钥。 • 从旧的密钥生成新的密钥 • 重新分配新的密钥

Kerberos

80年代中期是MIT的Athena工程的产物，针对分布式环境的开放式系统开发的认证机制

Kerberos第五版是Windows 2000最基本的安全协议

Linux和Unix类系统都支持Kerberos协议

三种可能的安全方案：

- 依赖服务器强制实施基于用户表示标识的安全策略
- 要求客户端系统向服务器证实自己的身份
- 要求每一个用户对每一个服务证明其标识身份，服务器也要对每一个客户端证明器标识身份

非授权用户无权访问服务或数据，网络环境下的身份认证

- 提供中心认证服务器，集中式认证服务器，提供每个用户到服务器和服务器到用户的认证服务
- 对称加密算法，提供一个可靠的第三方认证服务
- 支持第三种方法

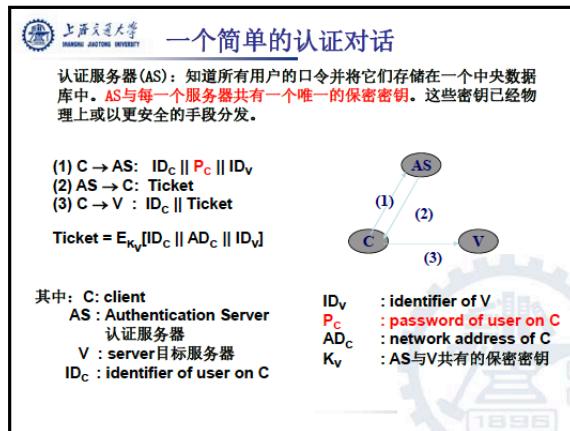
Kerberos系统基本性质

- 安全
- 可靠

- 透明
- 可伸缩

设计思路

- 使用一个或一组独立的认证服务器
- 认证服务器 (AS) : 将用户口令保存在数据库中
- AS与每个服务器共享一个唯一保密密钥 (已被安全分发)



问题:

- 使用者希望输入口令的次数最少 • 口令以明文传送会被窃听, 应该进行加密保护

解决办法

- 票据重用 (ticket reusable) • 引入票据许可服务器 (TGS - ticket-granting server) ,用于向用户分发服务器的访问票据 • 认证服务器AS 并不直接向客户发放访问应用服务器的票据, 而是由TGS 服务器来向客户发放

两种票据

- 服务许可票据
- 票据许可票据 (用户登录申请一次, 多次使用)

X.509

与Kerberos协议相比, X.509鉴别交换协议有个很大的优点:

不需要物理上安全的在线服务器, 因为一个证书包含了一个认证授权机构的签名, 公钥证书可通过一个不可信的目录服务被离线的分配

X.509基于公钥加密和签名, 使用RSA, 没有指定散列算法, X.509双向交换和Kerberos一样依赖时戳, X.509三向交换克服了这一缺陷

应用: S/MIME, IP安全 (IPSEC) , SSL/TLS和SET

证书

- 可信证书权威机构创建 (CA - Certificate Authority)
- 用户或CA把证书存放在目的服务器中
- 证书机构Y颁发给用户X的证书表示为Y<<X>>
- CA<<A>> 表示CA 颁发给用户A 的证书。

CA用私有密钥给证书签名

任何拥有CA 公开密钥的用户都可以从证书中提取被该证书认证的用户的公开密钥 • 除了CA外，任何用户都无法伪造证书或篡改证书的内容； • 由于证书是不可伪造的，可将证书存放数据库（即目录服务）中，而无需进行特殊的保护

证书格式

- X.509版本号
- 证书持有人的公钥
 - 包括证书持有人的公钥、算法(指明密钥属于哪种密码系统)的标识符和其他相关的密钥参数
- 证书的序列号
 - 证书被取消时，实际上是将此证书序列号放入由CA签发的CRL (Certificate Revocation List证书作废表，或证书黑名单表) 中，这也是序列号唯一的原因
- 主题信息：证书持有人唯一的标识符
- 证书的有效期
- 认证机构
- 发布者的数字签名（证书发布者私钥生成的签名）
- 签名算法表示符
 - 用来指定CA签署证书时所使用的签名算法。算法标识符用来指定CA签发证书时所使用的公开密钥算法和HASH算法

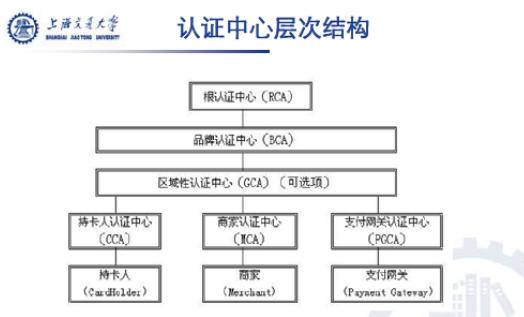
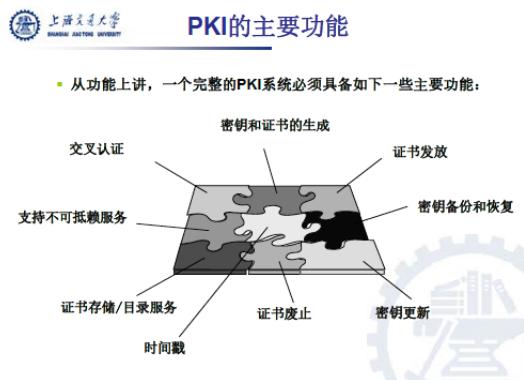
PKI/CA

公钥基础设施PKI (Public Key Infrastructure)

- 提供公钥加密和数字签名服务的系统或平台，目的是管理密钥和证书
- 认证中心CA (Certification Authority)
 - 负责管理PKI结构下的所有用户的证书，把用户的公钥和用户的其他信息捆绑在一起，在网上验证用户的身份

PKI基本组成

- 证书库 • 证书作废处理系统 • 认证机构 (CA Certificate Authority) • 注册机构 (RA Registration Authority) • 密钥备份与恢复系统 • PKI应用接口



Chapter4 访问控制与 计算安全

访问控制

通过某种途径显示地准许或限制访问能力及范围，针对越权使用资源的防御措施，通过限制对关键资源的访问，防止非法用户侵入或因为合法用户的不慎操作而导致的破坏，保证网络资源受控地、合法的使用

基本目标

防止对任何资源进行非授权的访问，允许被授权的主体对某些客体的访问，拒接向非授权的主体提供服务

非授权的访问

- 非法用户进入系统
- 合法用户对系统资源的非法使用

访问控制系统

- 客体（需要保护的资源，又称目标）
- 主体（或称发起者，一个主动的实体，规定可以访问该资源的实体，通常指用户或代表用户执行的程序）
- 授权（准许某个用户为了某种目的可以访问某个目标的权利，即使安全访问策略）

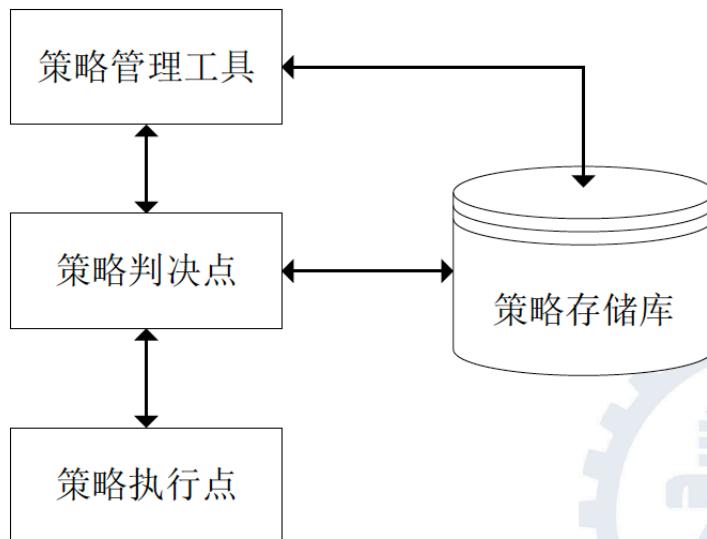
主客体的关系是相对的

访问控制模型



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

基于策略的访问控制模型



如何决定访问权限

- 用户分类
 - 特殊用户（系统管理员，最高权限）
 - 一般用户：最大的一类用户
 - 做审计的用户：负责整个安全系统范围内的安全控制与资源使用情况的审计
 - 作废的用户：被系统拒绝的用户
- 资源
 - 磁盘与磁带卷标
 - 远程终端
 - 信息管理系统的事务处理及其应用
 - 数据库中的数据
 - 应用资源
- 资源及使用

访问控制包：对保护的资源定义一个访问控制包
(资源名及拥有者的标识符，缺省访问权，用户及用户组的特权明细表，允许资源拥有者对其添加新的可用数据的操作，审计数据)
- 访问规则
 - 规则使用与资源配对，指定该用户可在该文件上执行哪些操作，如只读、不许执行或不许访问
 - 由系统管理人员来应用这些规则，由硬件或软件的安全内核部分负责实施

访问控制的一般实现机制

- 基于访问控制属性

- 访问控制表/矩阵

任何访问控制策略最终均可被模型化为访问矩阵形式（行：用户，列：目标，每个矩阵元素规定了访问许可和实施行为）



访问控制矩阵

- 按列看是访问控制表内容
- 按行看是访问能力表内容
- R 读, W 写, Own 管理

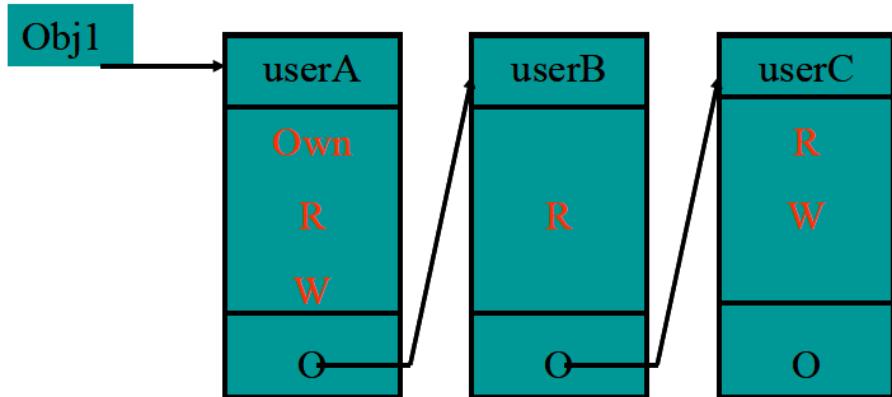
目标 用户	目标x	目标y	目标z
用户a	R、W、Own		R、W、Own
用户b		R、W、Own	
用户c	R	R、W	
用户d	R	R、W	

- 基于用户和资源分级（“安全标志”）
 - 多级访问控制

常用实现方法

- 访问控制表 (ACLs: Access Control Lists)

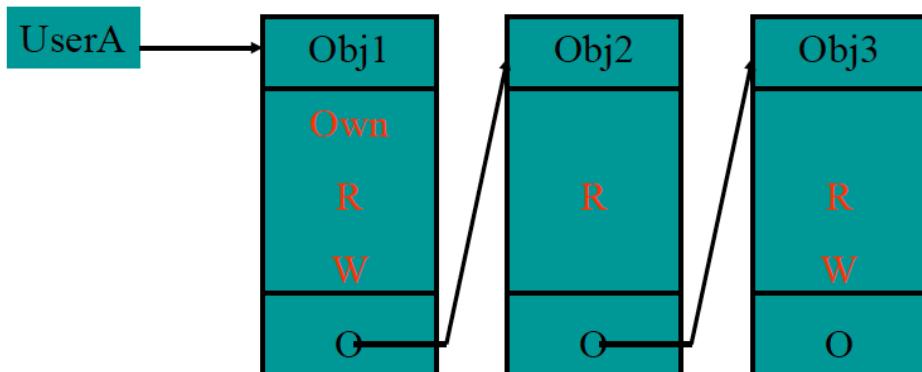
访问控制表(ACL)



每个客体附加一个它可以访问的主体的明细表。ACL对每个资源指定可以访问的用户或用户组及相应的权限，但是当资源很多时候需要设定大量的表项，并且当用户发生变化时候，管理很麻烦；并且ACL不易实现最小权限管理和复杂的安全策略。

- 访问能力表

访问能力表(CL)



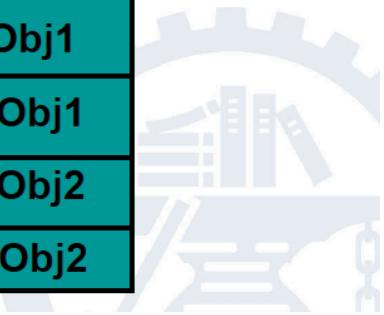
每个主体都附加一个该主体可访问的客体的明细表,着眼于某一主体的访问权限，但是在获得对某一特定客体有特定权限的所有主体就比较困难。

- 授权关系表

授权关系表(Authorization Relations)

- 每一行（一个元组）表示了主体和客体的权限关系，该表类似于关系数据库，可以对客体和主体进行排序，得到需要的结果。

UserA	Own	Obj1
UserA	R	Obj1
UserA	W	Obj1
UserA	W	Obj2
UserA	R	Obj2



访问控制策略

- 自主访问控制 (DAC)：基于身份的控制访问 (IBAC)

1. 基于身份的策略

- 目前实现的最多的访问控制机制
- 基于主体的身份以及他们所属的组的基础对访问进行限定
- 具有某种访问能力的主体能够自主的将访问权的某个子集授予其他主体
- 灵活性高，大量采用 (Windows, Unix)
- 允许某个主体显示地指定其他主体对该主体所拥有的信息资源是否可以访问以及可执行的访问类型
- 缺点：

用户可以把对目标O的访问权限传递给用户B，信息在移动过程中访问权限会被改变

2. 自主访问控制的访问类型

访问许可定义了不改变访问模式的能力或向其他主体传送这种能力的能力

- 等级型
- 有主型
- 自由型

访问模式：主体对客体可进行何种形式的特定访问操作：读、写、运行、无效

- 强制访问控制 (MAC)：基于规则的访问控制 (RBAC)

- 特点：对资源的访问取决于实体的授权而非实体的身份
- 粒度大，缺乏灵活性

- 能阻止特洛伊木马
- 具体细节
 - 将主体和客体分级（绝密级，机密级，秘密级，无密级）
 - 访问控制关系为上读下写（保证数据完整性），下读/上写（保证数据机密性）
 - 通过安全标签实现单向信息流通模式
- 下读：低信任级别的用户不能读高敏感度的信息，上读反之
- 上写：不允许高敏感度的信息写入低敏感度的区域，下写反之
- ④ 强制访问控制(MAC)中，系统包含主体集S和客体集O，每个S中的主体s及客体集中的客体o，都属于一固定的安全类SC，安全类 $SC = \langle L, C \rangle$ 包括两个部分：有层次的安全级别和无层次的安全范畴。构成一偏序关系。

(1) Bell-LaPadula: 保证保密性的数学模型

- 无上读：仅当 $SC(o) \leq SC(s)$ 时，s可以读取o，即是一个给定等级的用户只能读具有相同或比它低的密级的数据。

- 无下写：仅当 $SC(s) \leq SC(o)$ 时，s可以修改o，一个拥有给定等级的用户只能向具有相同或者比它高的密级的目标写数据，防止未授权用户无需授权就删除有密级的数据和防止特洛伊木马攻击。

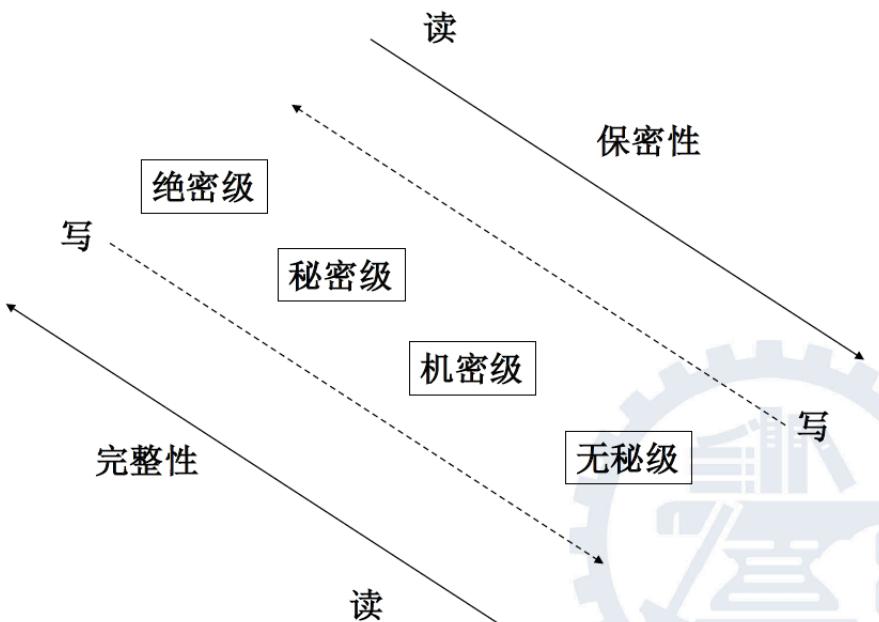
(2) Biba: 保证完整性的数学模型

- 同(1)相反，应用该模型，目标可被分配一个完整性密级和敏感性密级



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

MAC模型



右边：Bell-LaPadula

左边：Biba

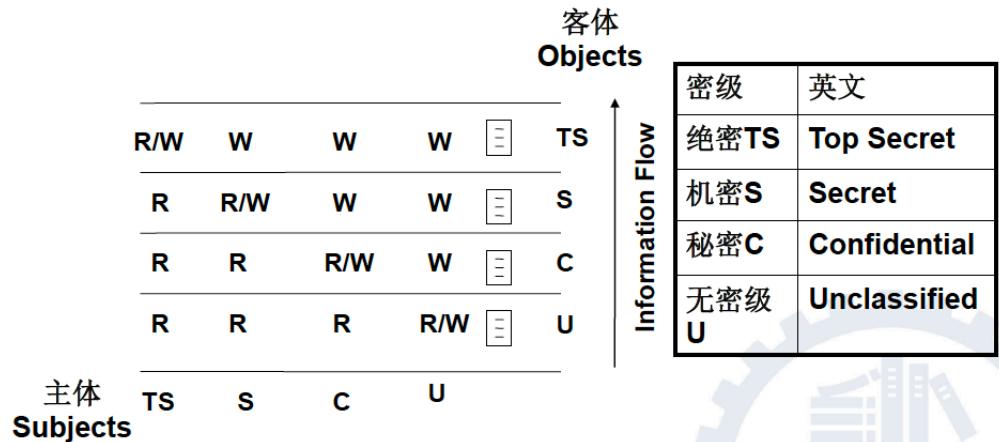
* MAC安全机制--安全标签

限制在目标上的一组安全属性信息项，隶属一个用户，目标，一个访问请求或传输中的一个访问控制信息（支持多级访问控制策略，比较目标和请求的标签，应用策略规则）



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

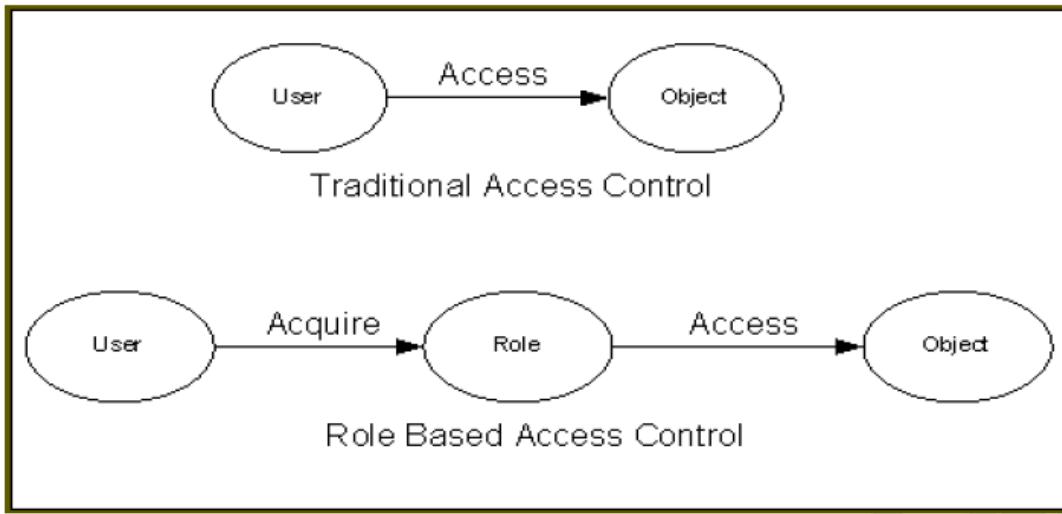
MAC Information Flow信息流



- 基于角色的访问控制 (RBAC)

- 背景：主体客体数量增大，传统模型难以使用，Web上的访问控制称为主流研究课题
- 基本思路：
 - 提出“角色”作为授权中介
 - 角色：一个或一群用户在组织内执行的操作的集合
 - 由系统管理员定义，增减也有系统管理员执行，强加给用户，权限不能自主转让，是非自主型访问控制
 - 角色与组的区别
 - 组：一组用户的集合
 - 角色：一组用户的集合+一组操作权限的集合
 - 定义不同层次访问控制模型
 - 利用RBAC模型实施模型管理
 - 角色控制相对独立，某些角色类似于DAC，某些角色接近于MAC
- RBAC优势：
 - 便于授权管理
 - 便于根据工作分级
 - 便于赋予最小权限
 - 便于职责分离
 - 便于客体分类及文件分级管理

- 增加一层间接性带来了灵活性

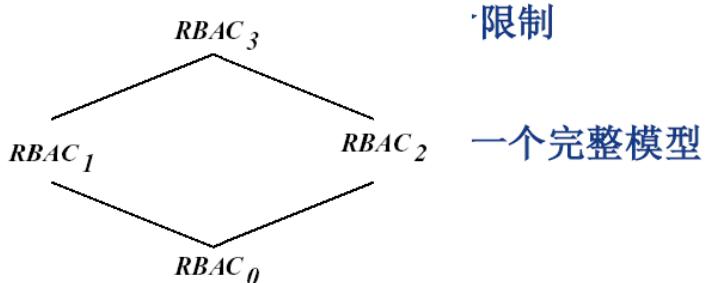


- RBAC基本模型

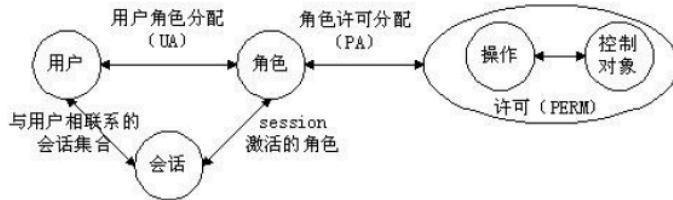
- RBAC96, 分层的RBAC模型

④ 分层的RBAC基本模型

- RBAC₀基本模型:** 含有RBAC核心部分, 定义结构和基本模型
- RBAC₁角色分级模型:** 包含RBAC₀, 另含角色继承关系(RH)
- RBAC₂角色(Constrain)**
- RBAC₃统一**



RBAC0定义了能构成一个RBAC控制系统的最小的元素集合



RBAC0与传统访问控制的差别在于增加一层间接性带来了灵活性，RBAC1、RBAC2、RBAC3都是在RBAC0上的扩展出来的。

- ④ RBAC1引入**角色间的继承关系**，角色间的继承关系可分为
 - ④ 一般继承关系
要求角色继承关系是一个绝对偏序关系，允许角色间的多继承。
 - ④ 受限继承关系。
进一步要求角色继承关系是一个树结构。

RBAC2

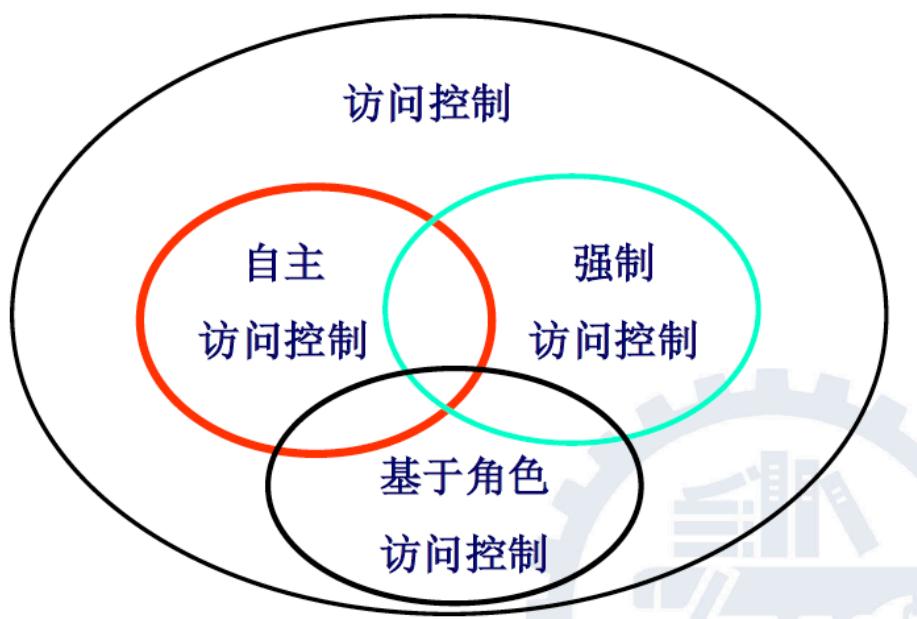
- ④ RBAC2模型中添加了**责任分离关系**。RBAC2的约束规定了权限被赋予角色时,或角色被赋予用户时,以及当用户在某一时刻激活一个角色时所应遵循的强制性规则。
- ④ 静态责任分离
- ④ 动态责任分离。
- ④ 约束与用户-角色-权限关系一起决定了RBAC2模型中用户的访问许可。



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

访问控制的一般策略

- 三种访问控制策略并非绝对排斥，可以相互综合，当产生冲突时候需要管理层来协调。



目标的粒度和策略的结合

相同的信息结构可能需要截然不同的访问策略与机制

多种策略的结合

- 规定策略的优先级
- 否定策略的优先级

网络访问控制组件的分布

输入、输出、插入访问控制（访问控制组件）

对目标：输入访问控制

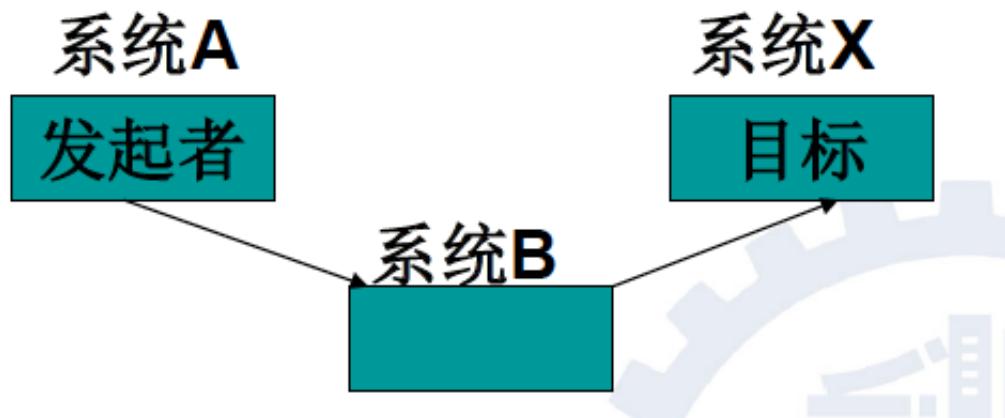
对发起者：输出访问控制

访问请求穿越安全区域边界和区域授权机构，过滤访问请求时：插入访问控制

访问控制转发

发起者A想要系统B去访问在系统X上的目标

A转发他的访问权利给B



云计算发展与应用

1. 云计算的时代：

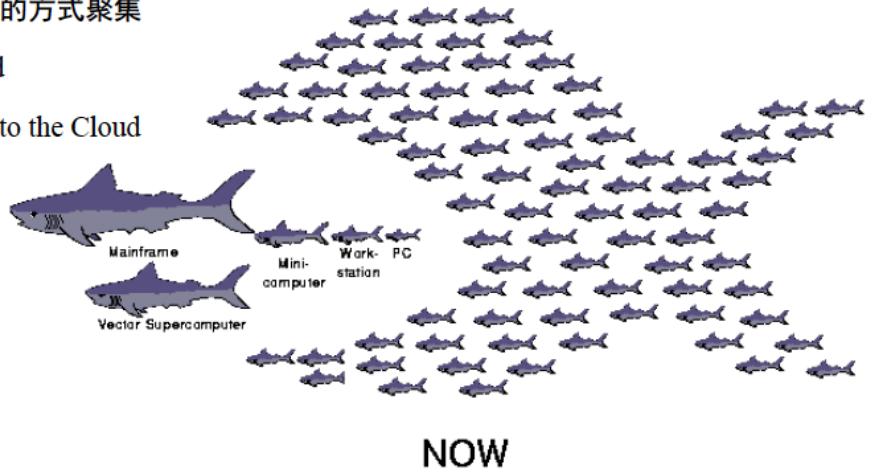
- 云是一种思想 (The Network is the Computer)
- 云是一种方法 (虚拟化)
- 云是一个机会(重新思考，架构你的系统)
- 云是一个方向 (XaaS: everything as a Service)

2. 云计算：

- 公开云，私有云
- 简化的服务接口
- 按量计算的商业模型

	弹性能力	服务	多租户	互联网	IaaS	PaaS	SaaS
•	虚拟化	动态配置	按需付费				

- Mainframes 让路给 Mini-Computers
- Mini-Computers 让路给 Micro-Computers
- Micro-Computers 通过 network 连接在一起
- Networked systems 以 Cluster 的方式聚集
- Cluster 进一步发展为 the Grid
- Micro-Computer Virtualized into the Cloud



3. 云计算的特征

- 超大规模
- 虚拟化
- 高可靠性
- 通用型
- 高可扩展性
- 按需服务

云的三种商业模式

1. SaaS (软件及服务) : 通过网络获取软件服务 (Salesforce online CRM)
2. PaaS (平台及服务) : 把完整的计算机平台作为服务提供给客户 (Google App Engine)
3. IaaS (基础设施即服务) : 企业或个人可以使用云计算技术来远程访问计算资源 (包括计算, 存储以及应用虚拟化技术) (Amazon EC2/S3)



判断是不是云计算的标准

- 用户使用的资源不在客户端而在网络中
- 服务能力具有优于分钟级的可伸缩性
- 五倍以上的性价比提升

云计算的特征

- 单租户到多租户
- 数据和服务外包
- 计算和服务虚拟化
- 大规模数据并行处理

云计算的特点	安全威胁
数据和服务外包	(1) 隐私泄露 (2) 代码被盗
多租户和跨域共享	(1) 信任关系的建立、管理和维护更加困难; (2) 服务授权和访问控制变得更加复杂; (3) 反动、黄色、钓鱼欺诈等不良信息的云缓冲 (4) 恶意SaaS应用
虚拟化	(1) 用户通过租用大量的虚拟服务使得协同攻击变得更加容易，隐蔽性更强； (2) 资源虚拟化支持不同租户的虚拟资源部署在相同的物理资源上，方便了恶意用户借助共享资源实施侧通道攻击。

云计算面临的安全挑战

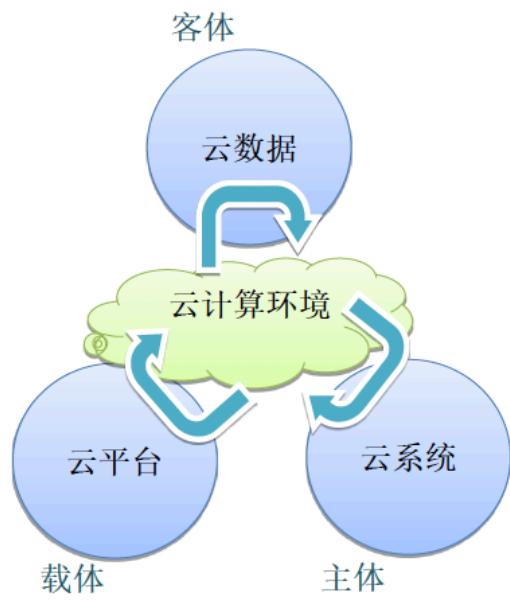
- 云计算环境的隐私安全
- 内容安全

云计算环境的本征和内在机理

云平台：为计算资源的虚拟化和共享提供了底层平台

云系统：采用不同服务模式联系计算资源和用户数据

云数据：云计算应用的核心，存储和发布方式受到云平台影响，也影响着云系统的运行模式



- “云平台”为计算资源的虚拟化和共享提供了底层平台。

- “云系统”采用不同服务模式联系计算资源与用户数据。

- “云数据”是云计算应用的核心，其存储和发布方式受到云平台影响，同时也影响到云系统的运行模式。

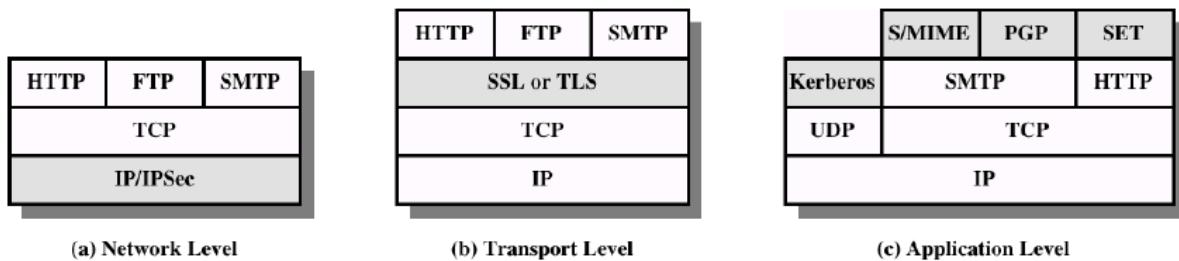
“平台安全-系统安全-数据安全”将构筑云计算安全体系

Chapter5 传输层安全

Web安全方案

- 网络层：IPSec
- 传输层：SSL/TLS
- 应用层：SET/HTTP，主页防篡改

Security facilities in the TCP/IP protocol stack



SSL协议

- 由Netscape提出在Internet上提供秘密通信的安全协议
- 为Client/Server应用提供可靠连接方式下的防窃听、防篡改、防信息伪造的通信
- 采用两种加密技术（非对称加密（交换加密密钥、认证），对称加密：加密传输数据）
- Internet上安全通信与交易的标准，使用通讯双方的证书，建立一条安全的、可信任的通讯通道

SSL基本特征

- 信息保密性
- 信息完整性
- 相互鉴定

SSL基本功能

- Authentication
- Encryption
- Integrity
- Key Exchange

SSL协议栈

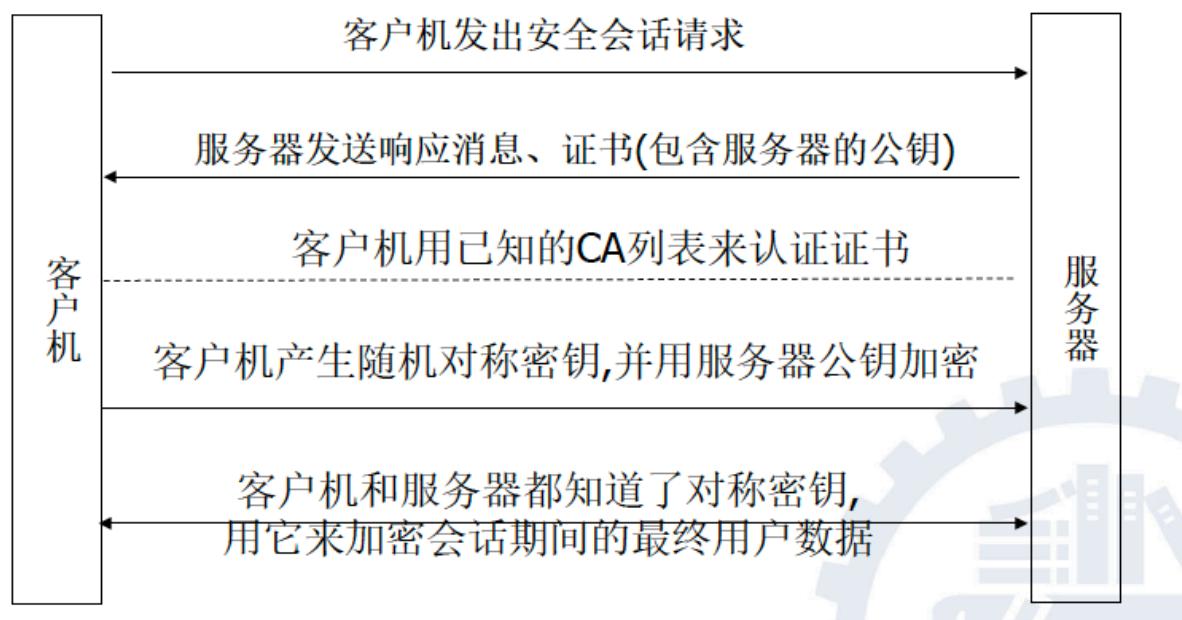
- 不是一个单独的协议，包括两层协议
 - SSL Record Protocol：为不同的上层协议提供基本的安全服务
 - 建立在可靠的传输协议基础上
 - 提供连接安全性
 - 保密性：对称加密算法，定义了一个共享密钥，可用于SSL负载的常规加密
 - 完整性：HMAC算法，定义了一个用于形成消息认证码的共享密钥
 - 用来封装高层的协议

- 三种高层协议：
 - 握手协议
 - 客户和服务器之间相互鉴别（交换SSL管理信息，协商加密算法，生成密钥）
 - 提供连接安全性
 - 身份鉴别
 - 共享密钥安全
 - 协商过程可靠
 - 改变加密规格协议
 - 报警协议
- 主要用于SSL密钥的交换
- SSL独立于各种协议，常用于HTTP协议

SSL两个重要概念

- SSL连接
 - 是一个提供一种合适类型服务的传输
 - SSL连接是点对点的关系
 - 连接是暂时的，每个连接和一个会话关联
- SSL会话
 - 一个SSL会话是在客户与服务器之间的关联
 - 会话由handshake protocol创建，定义了一组可供多个连接共享的加密安全参数
 - 每一个连接提供新的安全参数需要很高的谈判代价

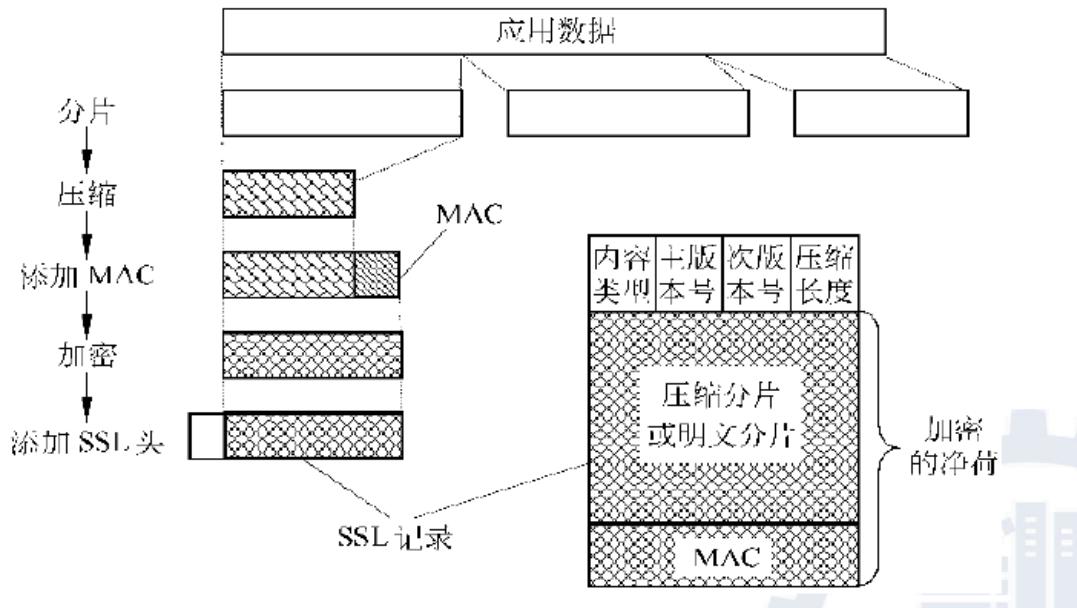
SSL工作过程



混合使用了对称加密和非对称加密

对称加密：不那么安全，效率高

非对称加密：更安全，效率低



SSL/TLS

TLS是SSL的更新版

SSL在TCP协议之上，为两个端实体之间提供安全通道的协议

安全通道透明，独立于应用层

协议目标：

为两个通讯提供保密性和完整性

互操作性，可拓展性，相对效率

SSL功能

- 客户对服务器的身份认证（可选）：利用CA证书（X.509协议）
- 服务器对客户的身份认证：通过公钥技术和证书，也可通过用户名和密码
- 建立服务器与客户之间安全的数据通道：发送的所有数据都被发送端加密、接收端解密（DES, 3DES, IDEA, RC2, RC4），同时还检查数据的完整性(MAC with MD5 or SHA-1)
- 安全优势：
 - 监听和中间人攻击

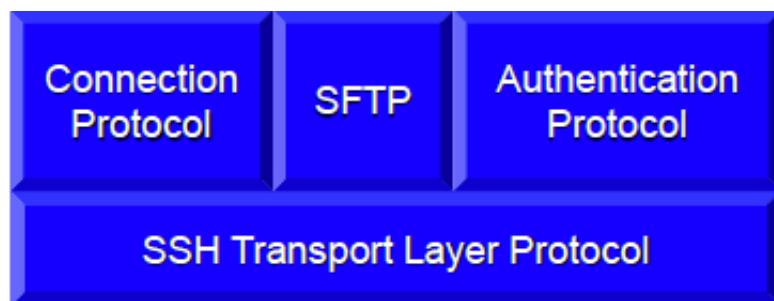
- 流量数据分析攻击（不行）
- 截拼攻击
- 重发攻击
- 可能存在问题：
 - 密钥管理（服务器证书不是由可信的CA颁发）
 - 加密强度
 - 数字签名（没有数字签名，不能抗抵赖）

SSH

提供一条安全的远程登录通道，可以替代telnet, rlogin

主要由以下四部分组成：

- SSH传输层协议：提供服务器主机认证，数据加密，提供数据完整性支持
- SSH认证协议：为服务器提供用户的身份认证
- Secure FTP
- SSH连接协议：将加密的信息隧道复用成若干个逻辑通道，提供给高层的应用协议使用



Chapter6 无线网络安全

移动/无线信道是开放性的，用户漫游，安全性的威胁远远大于固定通信

主要安全威胁：

- 非授权访问
- 对数据完整性的访问
- 拒绝服务攻击
- 主动用户身份捕获攻击
- 否定或抵赖参与的行为
- 使用偷窃的终端和智能卡

移动/无线互联网络应用安全

- NFC安全（near field communication）
- APT（手机恶意软件与APT攻击结合）
- 移动智能终端（身份，位置，手机病毒）
- 后台服务：拒绝服务攻击，信息窃取

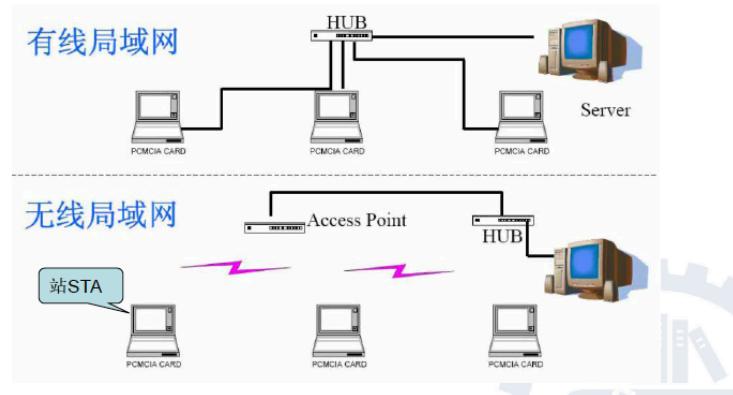
- 内容提供者：不良信息源，存在安全漏洞的业务应用

移动/无线智能终端安全

- 应用安全威胁
- Web安全威胁
- 操作系统安全威胁
- 硬件安全威胁

无线网络安全

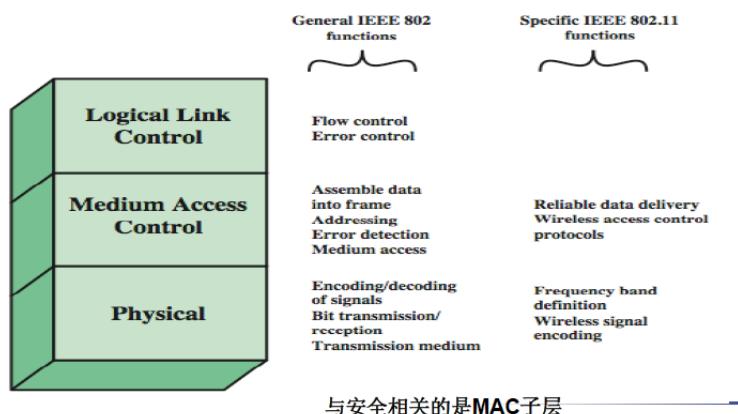
无线局域网结构



802.11基本构件

局域网协议的一部分，IEEE802.11提出的一个体系结构，主要有两个部分：数据链路层的MAC子层和物理层

- 站 (Station, STA) (无限网的端头设备，计算机加一块无线网卡)
- 无线接入点 (Access Point, AP): AP将STA与DS相连，典型的DS是某单位的有线网络，AP也可在不访问DS情况下将多个STA相连



安全协议演变

服务区标识符

每个AP都会设置唯一的网络SSID，是一个数据结构，在逻辑上区分不同的服务区

不提供任何数据机密功能，也不提供终端到无线接入点的认证（使用网络分析工具Sniffer）很容易就可以获得SSID

MAC地址过滤

接入点AP存有一个允许接入STA的MAC地址列表，阻止非列表内的STA访问请求

MAC地址是明文传输，很容易被嗅到

无线网卡允许软件更换MAC地址（Smac, Mac Makeup），攻击者能伪装成有效的MAC地址

802.11网络的安全方案（认证，加密）

认证：对无线终端和设备进行认证，不对用户进行认证

初始化STA和AP建立连接前需要认证

- 开放系统认证（必须）

默认协议，无论谁请求认证都会被对方通过，空认证过程，对确定一个客户是否合法没有提供任何帮助

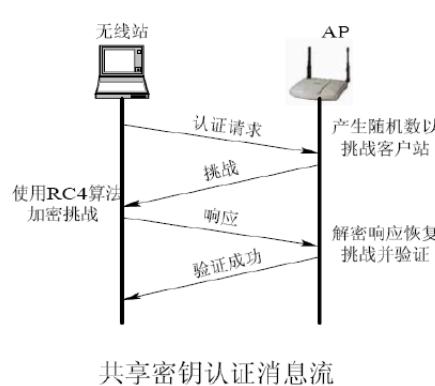
- STA发送认证请求帧给AP，帧内通常包含STA的MAC地址和SSID
- 如果AP的认证方式设为开放系统认证，需要请求者发送认证成功帧

- 共享密钥认证（可选）

- 支持拥有密钥的STA进行身份认证，密钥不会在网络中明文传送，但需要使用有线等效保密协议（WEP），只能在已实现WEP协议的节点运行
- 假设密钥已分配并正确装入MAC层，回避了密钥分配问题



2、共享密钥认证



- ① 请求者向认证者发送认证请求。
- ② 认证者向请求者发送一个明文的随机数。
- ③ 请求者使用WEP密钥加密此随机数，并发送给认证者。
- ④ 认证者使用WEP密钥加密原随机数，并与收到的密文比较，若相同，向请求者发认证成功帧

有限等级保密协议WEP

IEEE802.11标准中采用的信息保密机制

主要用于保障无线局域网中链路层信息数据的保密

- 对称加密
- 支队数据帧实体内容加密
- 只保护客户到访问点之间链路级数据（无连接部分），不是端到端的安全

802.11的巨大安全漏洞

1. 机密性的漏洞分析

WEP中RC4的使用主要有两个缺陷：

- IV重复使用（一般用计数器实现，但24位空间太小，很快就重新使用以前的IV值，会使输出的前几个字节没那么随机，弱密钥）
- 直接密钥攻击

2. 认证的漏洞分析

- AP发送128个字节的随机串，STA用WEP加密后返回，WEP用密钥流与明文异或形成密文

3. 完整性的漏洞分析

- 采用“比特反转”造成攻击

重新制定RSN健壮安全网络

新技术：

- EAP通信协议以及802.1x，强迫使用者必须进行验证以及交互验证
- 使用了MIC（信息完整性编码），检测传送的字节是否有被修改的情况
- 使用了TKIP（临时密钥完整性协议），加密过程：静态=>动态，使攻击者更难以破解
- 支持新的AES标准（Advanced Encryption Standard）

注意点：

RSN重点处理了WEP协议中的缺陷，并对无线链路提供了数据完整性和机密性保护

安全机制只工作在数据链路层，为STA和AP或STA与STA之间的通信提供保护，并不提供端到端的应用层通信保护

RSN只工作在无线网络中

RSN中三种设备

- STA
- AP
- AS（Authentication Server）：为STA提供认证服务

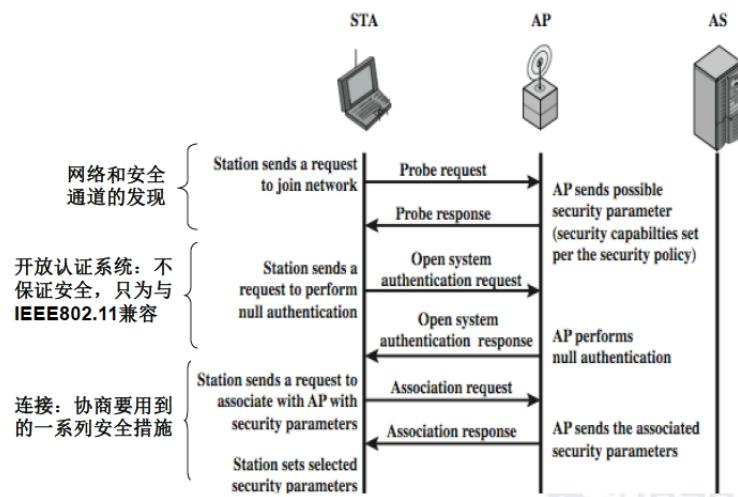
RSN工作4个阶段

● 发现阶段

- STA与AP互相确认身份，协商安全策略，建立连接
- AP使用信标和探测相应信息，确认AP身份
- STA和AP开始保密的通信，包括机密性和数据完整性，所用的算法是在发现阶段协商的



1、发现阶段



● 认证阶段

三个核心协议：

- 802.1x (STA与AS之间提供双向认证，为局域网提供访问控制的另一标准，是基于接口的网络访问控制)



申请者负责相应认证；认证者负责与申请者通信，并将认证信息传递给认证服务器；认证者根据认证结果，决定控制端口处于认证或非认证状态

- EAP
- RADIUS

● 密钥管理阶段

产生一系列的密钥分配到站点

密钥都是分层使用的

- AP和STA之间的单播：成对密钥，成对密钥层次结构
- AP和STA之间的组播：组密钥，组密钥层次结构

创建和交付PMK

成对密钥：层次结构最复杂，从顶端PMK（成对主密钥）开始，其他成对密钥从他这里导出

PMK是认证过程产生的副产物

认证发生在申请者和服务器之间，结果是申请者STA和服务器生成了匹配的PMK，但使用PMK的是STA和AP，需要让服务器把PMK传给AP

计算PTK（成对临时密钥）

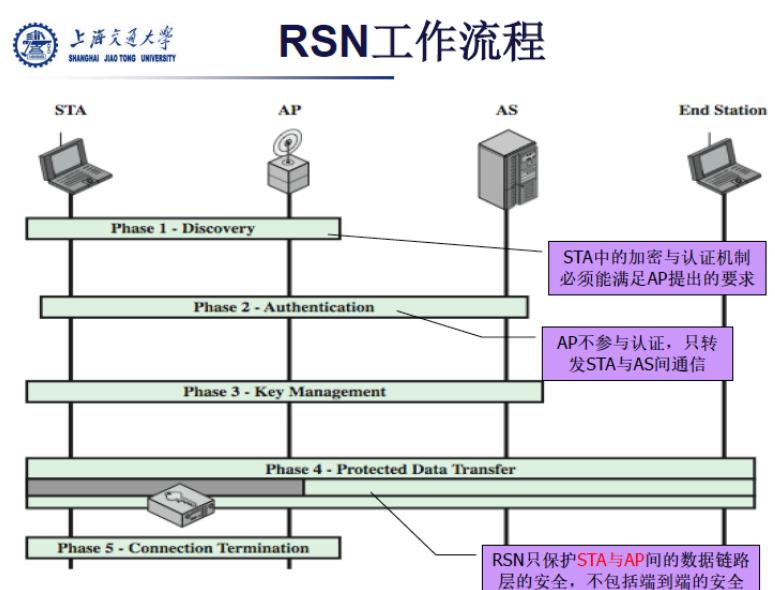
802.11i中密钥的层次结构依据加密方式为TKIP还是AES分成两类

- **数据加密**

在这个阶段，STA和AP已经协商好了安全策略，完成了相互认证，产生分配，确认了会话密钥，控制端口也已经打开

IEEE 802.11i中定义了两种加密和完整性协议：TKIP（临时密钥完整性协议）和CCMP

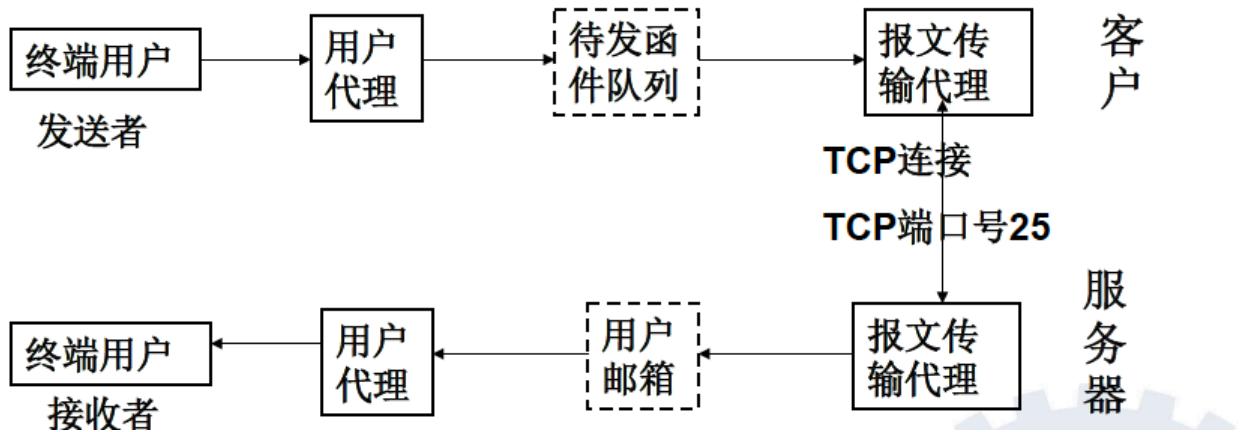
TKIP使用了RC4，不适合高可靠环境，高可靠性环境最好使用CCMP



Chapter 7 电子邮件与IP网络安全

7.1 电子邮件安全

邮件发送流程：

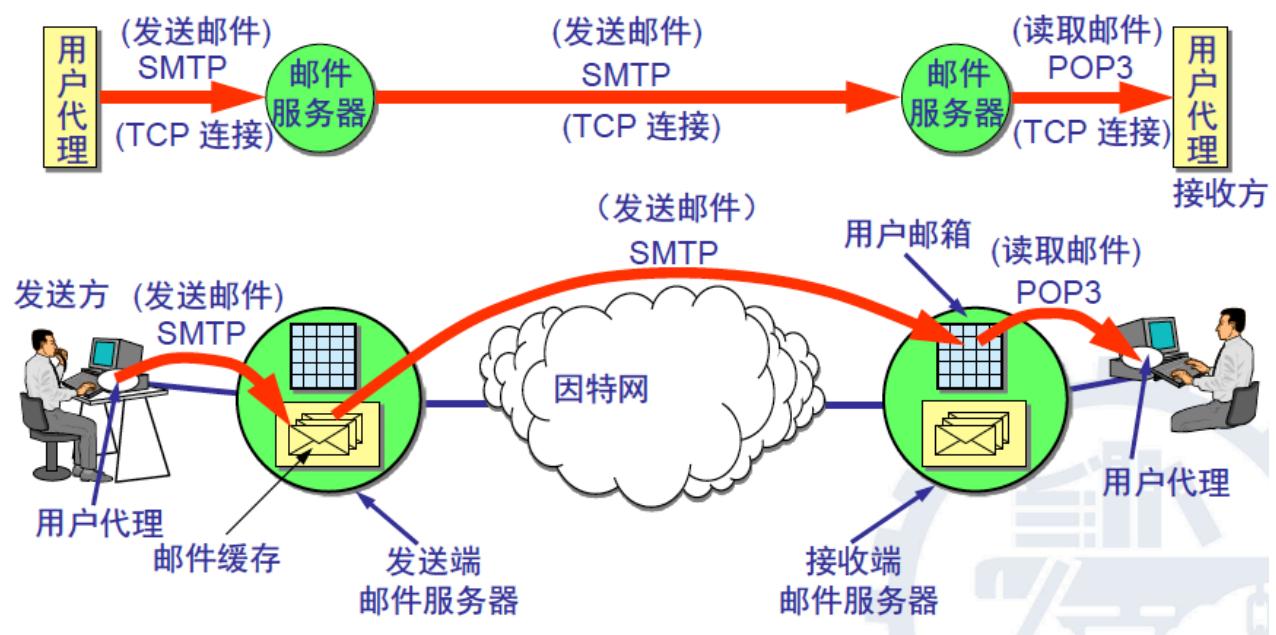


MUA (用户代理) 邮件系统为用户提供可以读写邮件的界面

报文传输代理 (MTA) : Unix sendmail

使用了SMTP协议

电子邮件主要的组成构件



用户代理从邮件服务器读取: POP3

用户代理发送到邮件服务器: SMTP

采用的都是TCP连接

安全问题

- 邮件欺骗 (基本邮件无认证机制, 邮件地址可以假冒)
- 邮件窃听 (邮件的题头和内容是明文, 可能被偷看修改)
- 电子邮件炸弹: 短时间向同一信箱发送大量电子邮件, 让被攻击的计算机系统崩溃
- 电子邮件病毒
- 邮件服务器控制: 修改邮件客户端的账户配置, 直接连到SMTP服务器上发信

- 垃圾邮件

防范方法

- 端到端的安全电子邮件技术 (PGP, S/MIME) (应用层)，使用密码技术对身份进行识别，对信息加密
- 传输层的安全电子邮件：SSL SMTP, SSL POP, VPN, IP通道技术
- 增加邮件服务器的安全与可靠性 (防垃圾邮件)

安全电子邮件

E-mail是Internet是最大的应用，跨平台、跨体系结构的分布式应用

安全性涉及问题：

- 安全算法
- 系统邮件的信息格式
- 如何认证和信任管理
- 邮件服务器的可靠性

实际应用例子：PGP, S/MIME

安全的邮件服务器

WORM病毒，网络入侵和拒绝服务

防范措施

- 防止来自外部的攻击 (拒绝来自特定地址的连接请求，限制单个IP的连接数量)
- 查看完整的电子邮件头部信息 (从源地址到目的地址经过的所有主机)
- 防止来自内部的攻击 (实现用户身份的鉴别)
- 邮件服务器的验证
 - SMTP服务器验证发送者的身份以及发送邮件地址是否和邮件服务器属于相同的域
 - 验证接收方的域名与邮件服务器的域名是否相同
 - 验证发送方的域名是否有效 (反向DNS)

PGP -- Pretty Good Privacy (个体用户使用)

广泛使用，提供可用于电子邮件和文件存储应用的保密与鉴别服务

- 利用单向散列算法对邮件内容进行签名 (邮件不被篡改)，公钥私钥保证邮件内容保密，不可否认
- 链式加密算法 (IDEA加密, RSA加密，保密性好，算法块)
- 多平台：DOS/Windows, Unix, Macintosh

PGP安全服务

- 数字签名 (DSS/SHA) 或者 (RSA/SHA)
- 完整性: RSA, MD5
- 信息加密: CAST-128/IDEA/3DES+Diffie-Hellman/RSA
- 数据压缩 (ZIP)
- 邮件兼容 (Radix 64)
- 数据分段

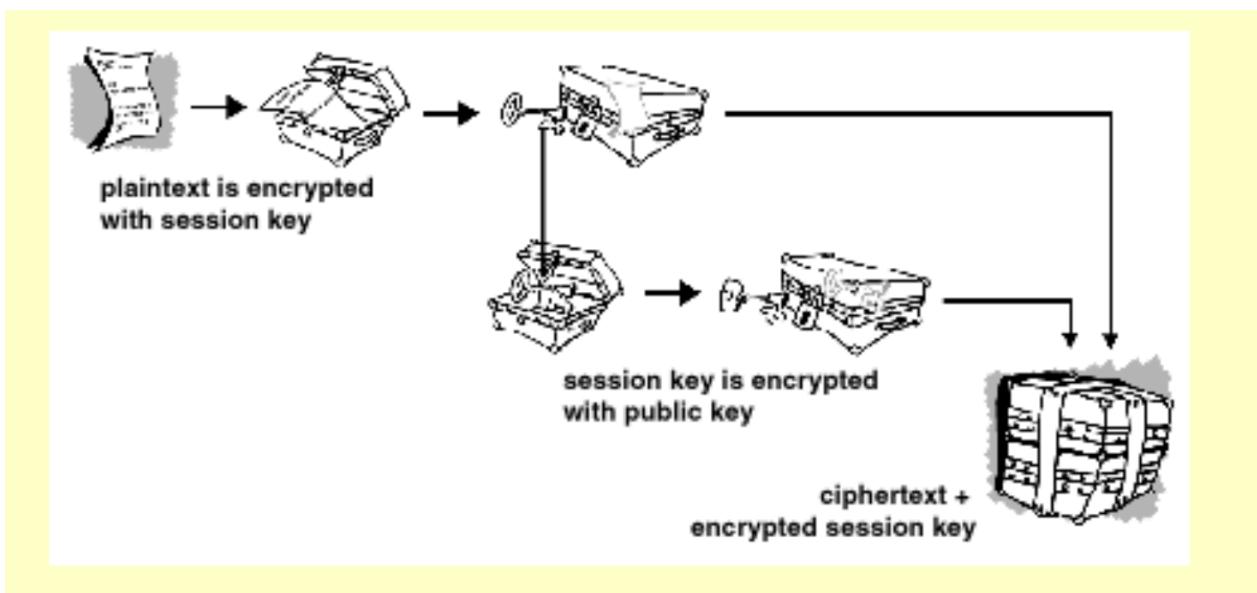
PGP密钥

- 一次性会话常规密钥
- 公钥
- 私钥
- 基于口令短语的常规密钥

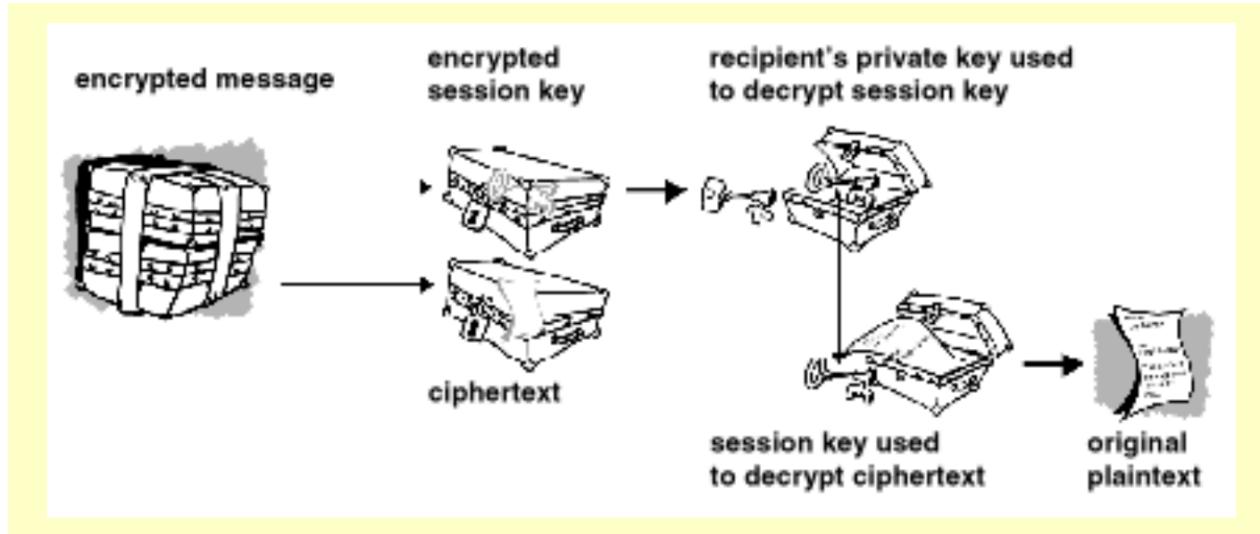
KeyId包括了公钥的低64位，从而去区分识别用户和公钥，两个KeyId包含在任何PGP消息里，提供保密与鉴别

PGP在每个节点提供一堆数据结构

加密



解密



- 存储该节点拥有的公钥和私钥对（私钥环）
- 存储本届点知道的其他用户的公钥（公钥环）

S/MIME (商用或组织使用的工业标准)

由PEM和MIME发展而来，是对MIME电子邮件格式的安全扩展

与PKI (public key Infrastructure) 结合, 使用X.509证书，PKCS (public key cryptography standards) 标准

- 算法协商不在线进行，只用一组规则来保证尽可能达到安全性
- 不严格的信任模式，由客户实现用户决定

垃圾邮件背景

定义：

- 收件人事先没有提出要求，统一的电子邮件
- 收件人无法拒绝的电子邮件
- 隐藏发件人身份、地址、标题等信息的电子邮件
- 含有虚假的信息源、发件人、路由等信息的电子邮件

垃圾邮件分类

- 反动宣传，色情/成人宣传邮件
- 病毒邮件
- 广告邮件

垃圾邮件特点

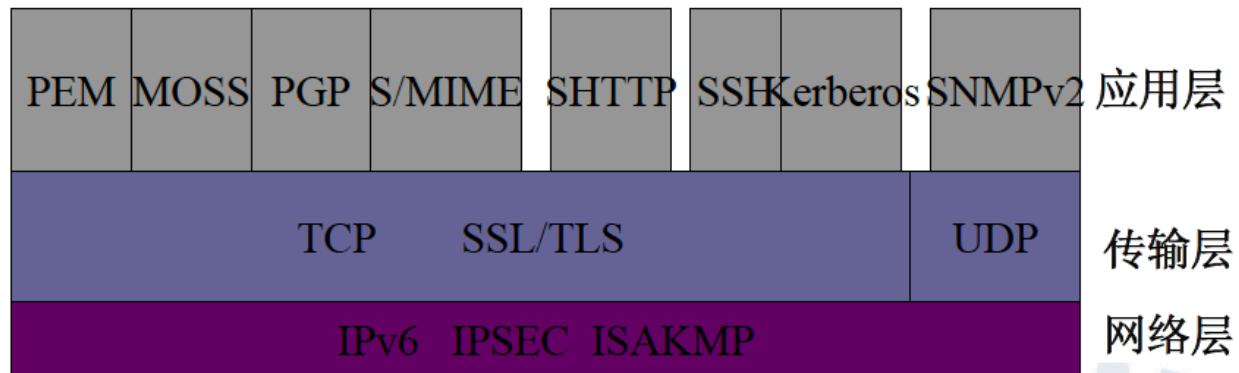
- 发件IP不固定
- 发件人地址不固定

- 收件人地址不固定
- 主体、内容、附件均有相对的随机性和固定性
- 时间不集中

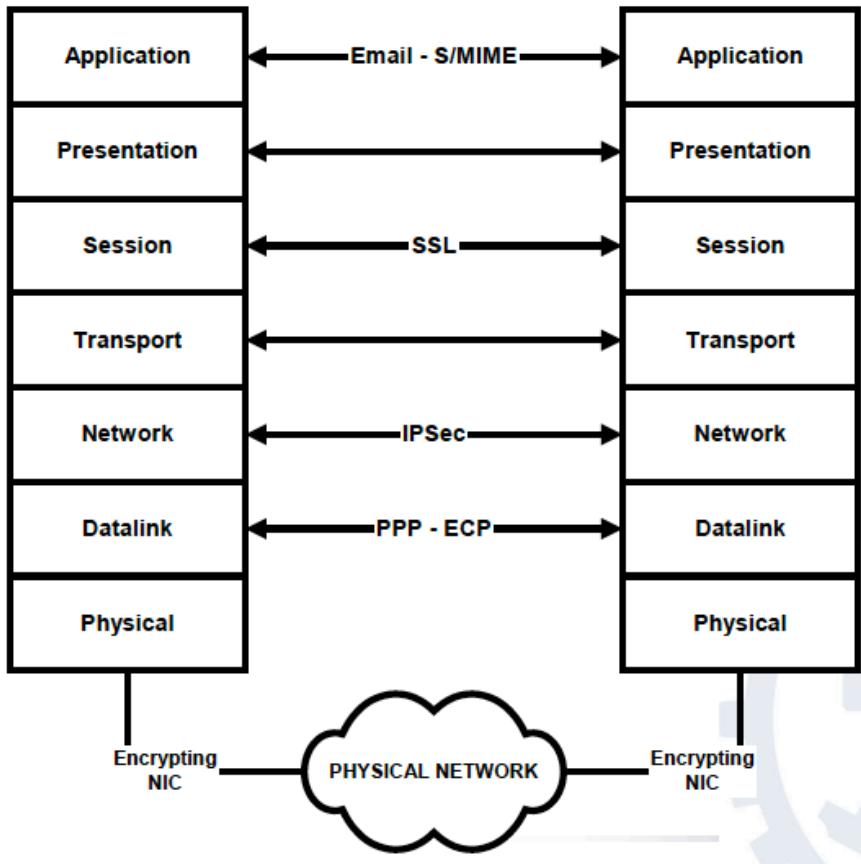
垃圾邮件防护方法

- 邮件地址保护
- 基于IP地址过滤
- 基于内容过滤

IP安全



- ISKAMP Internet安全关联密钥管理协议；
- SSL (secure socket layer) 安全套接层协议用来为使用TCP 提供一个可靠的端到端安全；
- TLS (Transport Layer Security) 传输层安全协议；



IPSec概述

IPSec随着IPv6产生，对IPv6必须，对IPv4可选

三种机制共同保障：

- 认证
- 信息机密性
- 密钥管理

基本目标：

- 保护IP数据包安全
- 为抵御网络攻击提供防护措施

提供服务

- 访问控制
- 无连接完整性
- 数据源鉴别
- 载荷机密性
- 有限流量机密

IPSec应用场景

作用于路由器或防火墙等网络设备，应用了IPSec的网络设备对所有流入或流出的数据流进行解密/解压缩或加密/压缩

IPSec体系结构

1. 两大部分：

- 通信协议 (AH (IP认证头), ESP(IP封装安全载荷))
- 密钥协商及交换协议：IKE

2. 两种操作模式：

- 传输模式（主机与主机的直接通信）

保护的是IP载荷

④ 传输模式

IP head	AH head	ESP head	payload
---------	---------	----------	---------

- 在传输模式中，AH和ESP头标被插在IP头标及其他选项（或扩展头标）之后，但在传输层协议之前。它保护净荷的完整性和机密性。

- 隧道模式（关联到多台主机的网络访问连入设备）

保护的是整个IP包，把一个包封装在另一个新包里面，整个源数据包作为新包的载荷部分，并在前面添加一个新的IP头

⑤ 隧道模式

IP head	AH head	ESP head	IP head	payload
---------	---------	----------	---------	---------

- 在隧道模式下，AH或ESP头标插在IP头标之前，另外生成一个新的IP头放在前面，隧道的起点和终点的网关地址就是新IP头的源/目的IP地址。
- 保护整个IP分组



3. 安全关联SA：通信对等方对某些要素的一种协定
4. 两个重要数据库：SPD安全策略数据库，安全关联数据库SAD
5. 使用鉴别和加密算法

IPSec实施位置---端主机

优点：

- 保证端到端的安全性
- 能够针对单个数据流提供安全保障
- 在建立IPSec的过程中，能够记录用户身份验证的相关数据和情况

实施方案：

- 与操作系统集成
- 作为一个单独的部分在协议堆栈的网络层和数据链路层之间实施

IPSec实施位置---路由器

优点：

- 能对两个子网间通过公共网络传输的数据提供安全保护
- 进行身份验证

实施方案：

- 集成在路由器软件中

- 在直接物理接入路由器的设备中实现，该设备一般不运行路由算法，只用来提供安全功能

SA (IPSec中的安全组合)

为使通信双方的认证/加密算法及参数、密钥的一致，相互间建立的联系被称为安全组合或安全关联

SA是单向的，会话需要两个独立的SA

SA是通过密钥管理协议在通信双方进行协商，协商完毕后，在他们的SAD中存储

由一个三元组唯一标识：安全索引参数SPI，一个用于输出处理的目的IP地址，协议（AH或ESP）

SPI

为了唯一标识SA，32bit证书

包含在AH和ESP头标中

有个SPI，相同源、目的节点的数据流可以建立多个SA

SAD

Chapter12 防火墙

防火墙是一种连接因特网和内部网的互联网关。它对两个或多个网络之间传输的数据分组和连接方式按照一定的安全策略对其进行检查，来决定网络之间的通信是否被允许。它能有效地控制内部网络与外部网络之间的访问及数据传输，从而到达保护内部网络的信息不受外部非授权用户的访问和过滤不良信息的目的。

防火墙的特性

- 位于Internet与Intranet之间的系统，避免内部网络直接暴露在外面
- 防止Internet上非法的破坏、入侵
- 防止内部使用者不当的使用Internet

- 有效的记录及监控企业与互联网活动提供完整的认证与报警

防火墙的安全控制问题

- 服务控制
- 方向控制
- 用户控制
- 行为控制

防火墙技术的发展

1. 包过滤防火墙

由路由器进行分组过滤，通过对IP地址以及TCP/IP端口的甄别进行安全防范

在路由器的实现中经常扩展了正常的选路功能，允许网络管理员进一步对分组的处理

这种机制被称为分组过滤器，它要求网络管理员指明路由器应当如何处理每个分组

基本思想：对每个进来的包决定是转发还是丢弃，过滤可以是双向的

如何过滤：

• 过滤的规则以IP和传输层的头中的域(字段)为基础，包括源和目标IP地址、IP协议域、源和目标口号。
• 过滤器往往建立一组规则，根据IP包是否匹配规则中指定的条件来作出决定。
• 如果匹配到一条规则，则根据此规则决定转发或者丢弃。
• 如果所有规则都不匹配，则根据缺省策略

优点：

分组过滤器直接内置于路由器中，所以它易于实现，并且效率高、速度快

缺点：

• 过滤算法的设计往往存在矛盾关系。规则简单，网络安全性差；规则复杂，则管理困难。在实践中，往往是在实现一个复杂的安全策略时，由于其设置繁琐造成管理员配置不当，使系统出现漏洞。
• 包过滤路由器能够允许或拒绝特定的服务，但是不能理解特定服务的上下文环境/数据。任何直接经过路由器的数据包都有被用做数据驱动式攻击的潜在危险。

应用代理网关