数据安全

第3章 关键基础技术

计算机与大数据学院 刘延华

福州大学
FUZHOU UNIVERSITY

第3章 关键基础技术

福州大学
FUZHOU UNIVERSITY

3.1 加密技术

□ 术语：加密 encryption

通过一种密码算法产生密文的（可逆的）数据转换，即隐藏数据的信息内容。[ISO/IEC 10116:2017，定义3.6]

□ 术语：解密 decryption

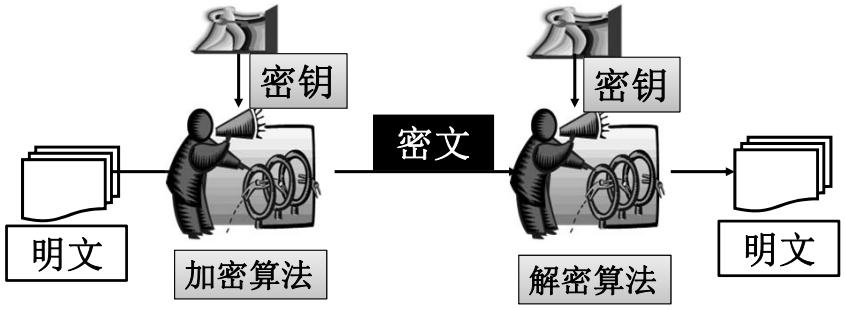
与加密对应的逆过程。[ISO/IEC 10116:2017，定义3.5]

□ 术语：密钥 key

控制密码变换（如加密、解密、密码校验函数计算、签名生成或签名验证）运算的符号序列。[ISO/IEC 11770-1:2010，定义2.12]

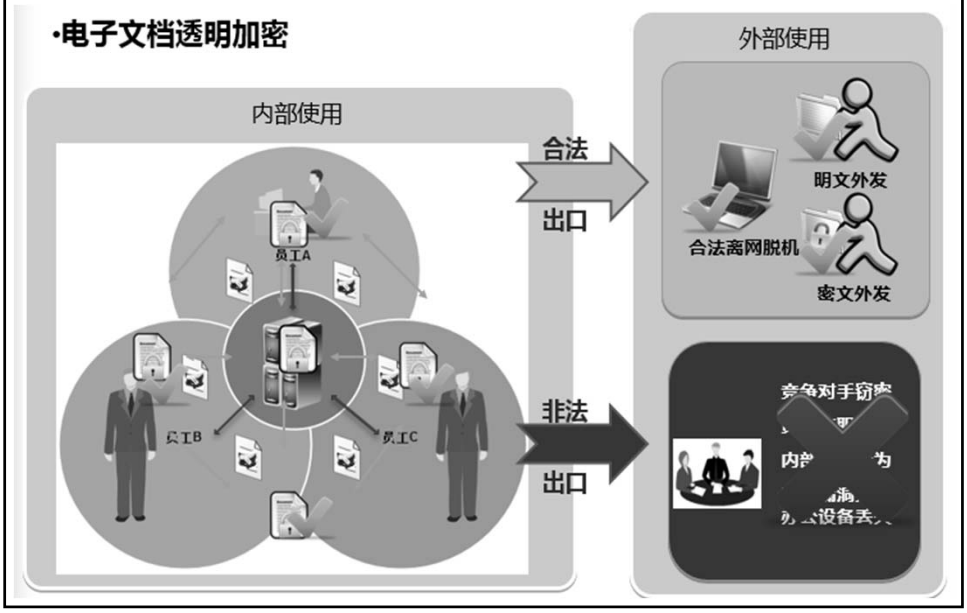
✓ 加密密钥、解密密钥

3.1 加密技术



加解密过程示意图

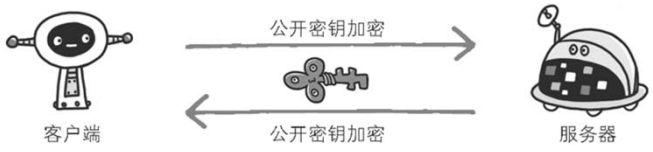
3.1 加密技术



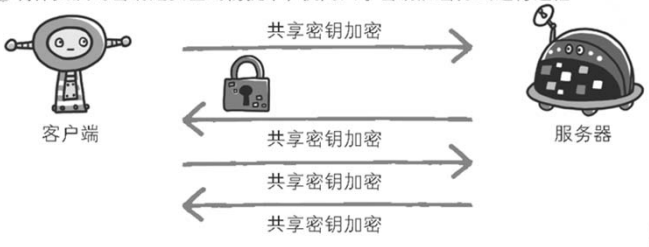
3.1 加密技术

公开密钥加密处理起来比共享密钥加密方式更为复杂，因此若在通信时使用公开密钥加密方式，效率就很低

①使用公开密钥加密方式安全地交换在稍后的共享密钥加密中要使用的密钥



②确保交换的密钥是安全的前提下，使用共享密钥加密方式进行通信



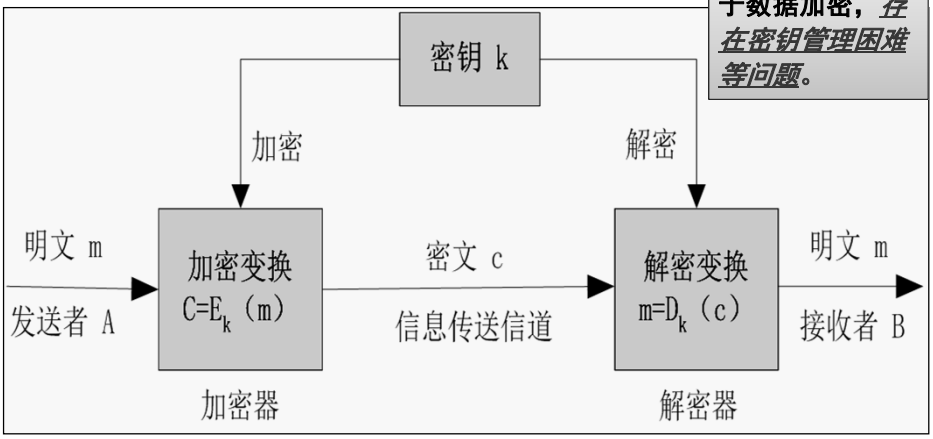
福州大学
FUZHOU UNIVERSITY

3.1 加密技术

□对称密码算法

加密密钥和解密密钥**相同**，称为**对称密钥算法**，也称为**单密钥**算法，如DES，3DES，AES算法等。

该类算法主要用于数据加密，*存在密钥管理困难等问题*。



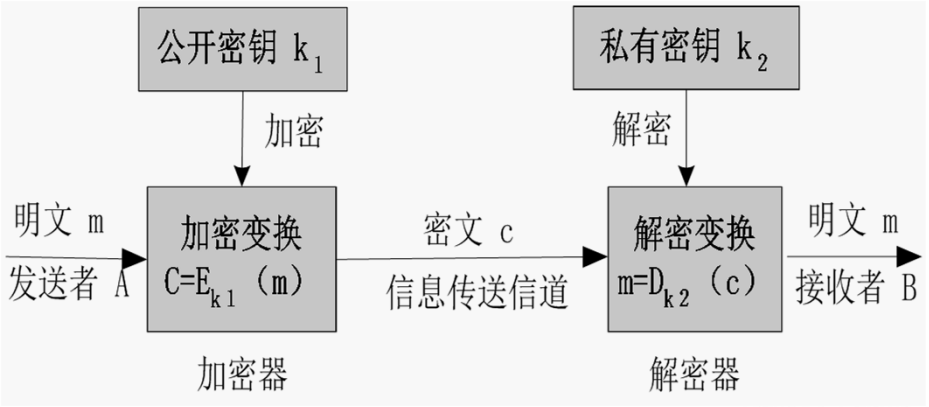
3.1 加密技术

公钥算法既可实现保密通信，也可用于数字签名。但算法速度较慢。

□公开密码算法

加密/解密的密钥**不同**，则称为**公开密钥算法**，如RSA、椭圆曲线算法等。

此时，一对密钥**公开密钥**和**私有密钥**，简称**公钥**、**私钥**。



3.1 加密技术

□ 古典密码技术

✓ 替代密码

替代密码就是明文中每一个字符被替换成密文中的另外一个字符。接收者对密文进行逆替换就恢复出明文来。

在替代法加密体制中，使用了密钥字母表。它可以由一个或多个字母表构成，分别称为单表密码和多表密码。

3.1 加密技术

□ 古典密码技术

✓ 凯撒（Caesar）密码

它是单表替代密码算法,也叫循环移位算法。

方法：把明文中所有字母都用它右边的第k个字母替代，Z后又是A，循环使用。

$$E(a)=(a+k) \bmod n$$

■ 其中：a表示明文字母；n为字符集中字母个数；k为密钥，一个正整数。

3.1 加密技术

□ 古典密码技术

✓ 凯撒（Caesar）密码

例子：设k＝3；对于明文P＝COMPUTE则：

E(C)=（3+3） mod 26 = 6 = F

E(O)=（15+3）mod 26 = 18 = R

E(M)=（13+3）mod 26 = 16 = P

所以，密文C= E_k(P) = FRPSXRWH。

在这里，字符集由用户自主设定.

3.1 加密技术

□ 古典密码技术

✓ 换位密码

换位密码是采用移位法进行加密的。它把明文中的字母进行重新排列，但位置变了。

（I）列换位法：

将明文字符分割成为n个字符一列的形式进行排列，不足一行由特定字符填充。

分组后并按列手顺序输出即得密文。

3.1 加密技术

如：WHAT YOU CAN LEARN FROM THIS BOOK

W	H	A	T	Y
O	U	C	A	N
F	R	O	M	T
H	I	S	B	O
O	K	X	X	X

密钥＝5，则密文：
WOFHOHURIKACOSXTAMBXYNTOX

3.1 加密技术

□ 古典密码技术

✓ 换位密码

（2）矩阵换位法：

把明文中的字母按给定的顺序安排在一个矩阵中，然后用另一种顺序选出矩阵的字母来产生密文。

如:将明文ENGINEERING按行排在3*4矩阵中，如所示：

一个置换矩阵 ：

$$f=\begin{pmatrix}1234\\2413\end{pmatrix}$$

1	2	3	4
E	N	G	I
N	E	E	R
I	N	G	

3.1 加密技术

□ 古典密码技术

✓ **换位密码**

（2）矩阵换位法：

按第2、4、1、3列次排列，得到密文：

NIEGERNEN IG

在这个加密方案中，密钥就是矩阵的行数m和列数n，即m*n＝3*4，以及给定的置换矩阵。也就是：k=（m*n，f）

其解密过程是将密文按3*4矩阵排列，再按置换矩阵的逆序，即第3、1、4、2列次输出，得到明文：ENGINEERING

3.1 加密技术

□ DES算法

数据加密标准DES是美国国家标准局制定的商用数据加密标准，军方除外。

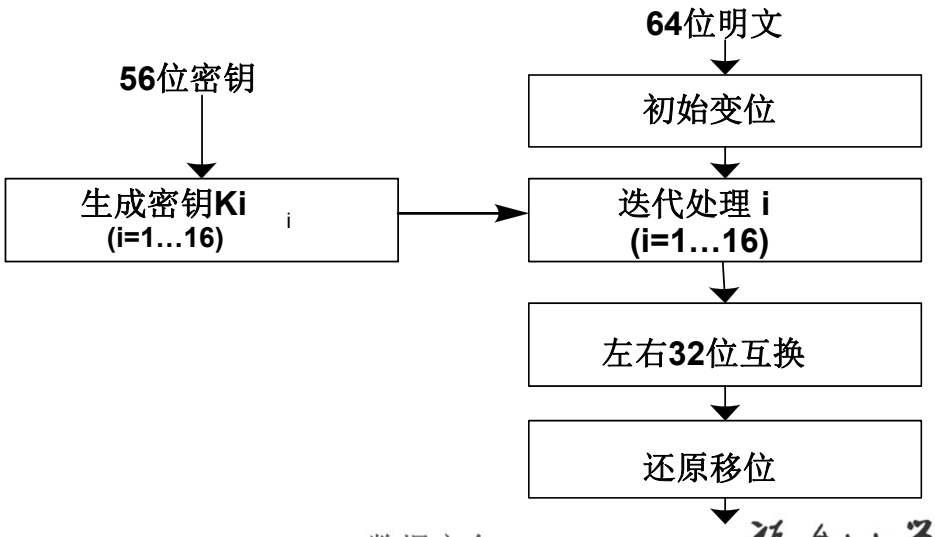
DES是一个对称密码算法：加密和解密用的是同一算法，两个密钥相同。

密钥长度为64bit，其中有效密钥长度56bit，其余8bit为奇偶校验。

DES的算法是公开的，因此系统的安全性主要依赖密钥的保密来实现。

56bit的密钥相对较短，现在多使用3DES算法或AES算法，来解决这个问题。

3.1 加密技术



3.1 加密技术

- **RSA算法**

RSA是麻省理工学院的研究成果，于1978年公布。密钥有由是两个很大质数构成，一个公开，另一个保密，前者称为“公用密钥”，后者称为“私有密钥”。

两个密钥相互配对，就是说公用密钥的密文可以用私有密钥来解密，反之也然。

3.1 加密技术

- **RSA算法**

应用时，要求每个用户都有1个密钥对：

（1）公钥：加密明文；

（2）私钥：解密密文。

采用RSA时，当用户A发信息给用户B时，用户A用B的公开密钥加密明文，用户B则用解密密钥解读密文。

3.1 加密技术

- RSA算法

RSA密钥可从40位到2048位，加密时数据块大小可变，但不超过密钥的长度。

RSA算法把每一块明文转化为与密钥长度相同的密文块。

密钥越长，加密效果越好，但计算开销也大。

如常见的SSL、PGP等都应用了RSA算法。

3.1 加密技术

- **RSA算法**

RSA密钥可从40位到2048位，加密时数据块大小可变，但不超过密钥的长度。

RSA算法把每一块明文转化为与密钥长度相同的密文块。

密钥越长，加密效果越好，但计算开销也大。

如常见的SSL、PGP等都应用了RSA算法。

RSA算法过程

- **密钥产生**

1.取两个大素数 p, q , 保密; ***p=7,q=17***

2.计算n=pq，公开n; ***n=119***

3.计算欧拉函数f(n)=(p-1)(q-1)； ***f(n)=96***

4.任取一个与f(n) 互素的小整数e：
gcd(e,f(n))=1; 1<e<f(n) ***选择e=5***

5.寻找d,d<f(n), 使得
d*e=kf(n)+1 ***5d=k×96＋1***

令 k=4, 得到求得d=77

RSA算法过程

- 公开密钥:KU={e, n} {5, 119}
- 秘密密钥: KR={d, n} {77, 119}
- 加密过程
  - 把待加密的内容分成k比特的分组，$k \leq \log_2 n$，并写成数字，设为M,则：

$$C = M^e \bmod n \qquad c = m^5 \bmod 119$$

- 解密过程

$$M = C^d \bmod n \qquad m = c^{77} \bmod 119$$

RSA算法过程

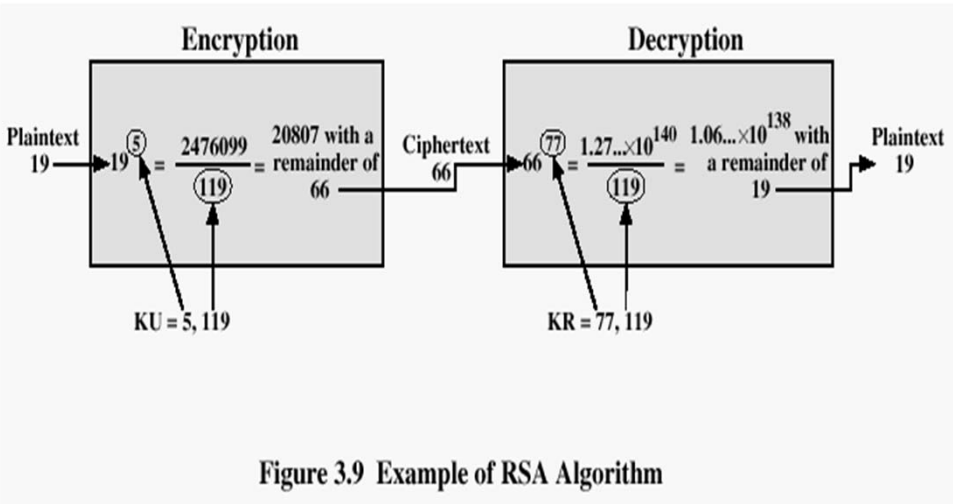


Figure 3.9 Example of RSA Algorithm

DES vs RSA

- **速度**

  硬件实现的最快的RSA算法所消耗的时间也是DES算法的1000倍。目前RSA加密速率达350Mbps的芯片已研制成功。最新？

- DES：数据传输加密；
- RSA：密钥传输（交换）加密；

3.1 加密技术

- **MD5算法**

MD5，即Message-Digest Algorithm 5（信息-摘要算法），是基于杂凑函数（HASH）的密码算法，由RSA的设计者R.Rivest于20世纪90年代初开发出来。

MD5能够将不同格式的数据信息在用数字签名软件来签署私人密钥前“压缩”成一种保密的格式，而且这种“压缩”是不可逆的。

3.1 加密技术

□ MD5算法

MD5的典型应用是对一段信息产生信息摘要，防篡改。

MD5 (tanajiya.tar.gz) = 0ca175b9c0f726a831d895e269332461

MD5算法通过其不可逆的字符串变换算法，产生了一个唯一的MD5信息摘要。

如果有第三方认证机构，则MD5就可以防止文件作者的“抵赖”，实现“数字签名”。

MD5算法

2004年8月17日美国加州圣巴巴拉的国际密码学会议（Crypto'2004）

王小云教授成功破译MD5、HAVAL-128、MD4和RIPEMD、SHA-1等密码。

数字签名算法收到巨大挑战！

加密-数字签名

◆ 数字签名体制

■ 签名算法(Signature Algorithm)

Sig(M)=S

签名算法或签名密钥K是秘密的，只有发方掌握；

■ 验证算法(Verification Algorithm)

Ver(S)={0，1}={真，伪}

验证算法公开，便于他人进行验证；

签名体制的安全性在于，从M和其签名S难以推出签名密钥K或伪造一个M'使M'和S可被证实为真。

加密-数字签名

◆ 数字签名分类

1）直接数字签名(direct digital signature)

只涉及通信双方

2）仲裁数字签名(arbitrated digital signature)

引入仲裁者，通信双方都非常信任仲裁者。

加密-数字签名

◆直接数字签名方法

1）用发送方的私钥对整条消息进行加密来产生签名.

【方式1】 A→B: $E_{KRa}[M]$

- 提供了鉴别与签名；
- 只有A具有K_{Ra}进行加密;
- 传输中没有被篡改；
- 任何第三方可以用K_{Ua} 验证签名

加密-数字签名

◆直接数字签名方法

1）用发送方的私钥对整条消息进行加密来产生签名.

【方式2】 A→B: E_{KUb} $[E_{KRa}(M)]$

提供了保密(K_{Ub})、鉴别与签名(K_{Ra})

加密-数字签名

◆直接数字签名方法

2）用发送方的私钥对消息hash码进行加密；

【方式1】 A→B: $M||E_{KRa}[H(M)]$

提供数字签名

✓H(M) 受到密码算法的保护,例如MD5或SHA-1;

✓只有A 能够生成$E_{KRa}[H(M)]$

【方式2】A→B: E_{kUb} $[M||E_{KRa}[H(M)]]$

提供保密性、数字签名。

33

福州大学 FUZHOU UNIVERSITY

加密-数字签名

◆ 仲裁数字签名方法

1）引入仲裁者。

通常的做法是所有从发送方X到接收方Y的签名消息首先送到仲裁者A，A将消息及其签名进行一系列测试，以检查其来源和内容，然后将消息加上日期并与已被仲裁者验证通过的指示一起发给Y。

34

福州大学 FUZHOU UNIVERSITY

加密-数字签名

◆ **仲裁数字签名方法**

2）仲裁者在这一类签名模式中扮演敏感和关键的角色。

所有的参与者必须相信这一仲裁机制工作正常。

数字签名的例子

现在Alice向Bob传送数字信息，为了保证信息传送的保密性、真实性、完整性和不可否认性，需要对要传送的信息进行数字加密和数字签名，其传送过程如下：

数字签名的例子

1. Alice准备好要传送的数字信息（明文）。
2. Alice对数字信息进行哈希（hash）运算，得到一个信息摘要。
3. Alice用自己的私钥（SK）对信息摘要进行加密得到Alice的数字签名，并将其附在数字信息上。
4. Alice随机产生一个加密密钥（DES密钥），并用此密钥对要发送的信息进行加密，形成密文。

数字签名的例子

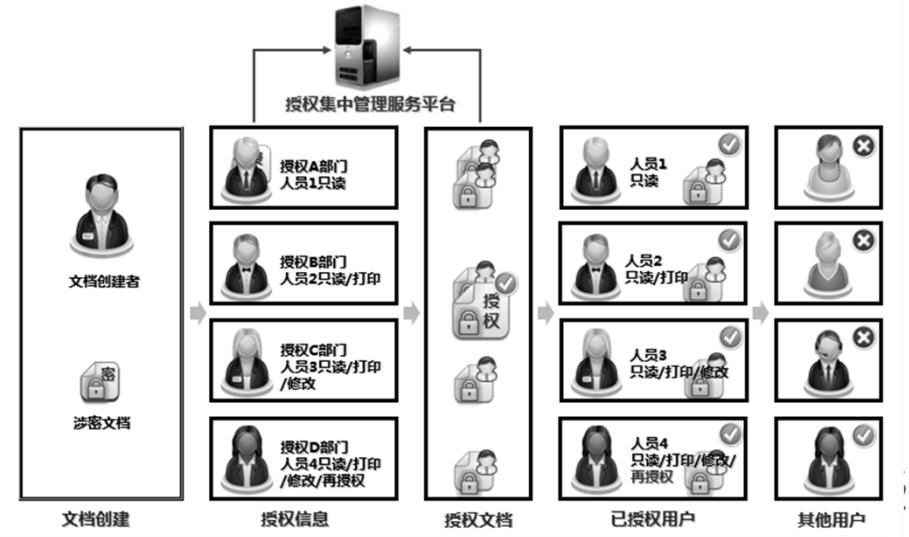
5. Alice用Bob的公钥（PK）对刚才随机产生的加密密钥进行加密，将加密后的DES密钥连同密文一起传送给Bob。
6. Bob收到Alice传送过来的密文和加过密的DES密钥，先用自己的私钥（SK）对加密的DES密钥进行解密，得到DES密钥。
7. Bob然后用DES密钥对收到的密文进行解密，得到明文的数字信息，然后将DES密钥抛弃（即DES密钥作废）。

数字签名的例子

8. Bob用Alice的公钥（PK）对Alice的数字签名进行解密，得到信息摘要。
9. Bob用相同的hash算法对收到的明文再进行一次hash运算，得到一个新的信息摘要。
10. Bob将收到的信息摘要和新产生的信息摘要进行比较，如果一致，说明收到的信息没有被修改过。

3.2 访问控制

·电子文档分级授权



3.2 访问控制

·电子文件外发管理

3.2 访问控制

- 访问控制是实现数据安全共享的重要技术手段，数据及数据应用的新特征使传统访问控制在授权管理、策略描述、细粒度控制、隐私保护、实施架构等方面都面临严峻挑战。
- 尤其是在云环境下，数据管理系统或存储平台内部管理人员存在潜在的数据窃取能力（如金融证券从业人员的数据泄露问题）

3.2 访问控制

基本概念　主体、客体和安全属性。

（1）主体（subject）：是主动的实体，行为的发起者，通常为代表用户的进程，系统中所有事件请求几乎都是由主体激发的。

□系统的合法用户可分成：

- 普通用户(进程)，
- 信息属主(进程)，
- 系统管理员(进程)

3.2 访问控制

（2）客体（object）：是被动的实体，是主体行为的承担者。可分成：

1)一般客体：信息实体，如文件、目录等。

2)设备客体：指系统内的硬件设备，如磁盘、磁带、显示器、打印机、网络节点等。

3)特殊客体：有时一些进程也是客体的一部分。

3.2 访问控制

主客体安全属性（敏感标记）

主客体安全属性是TCB维护与可被外部主体直接或间接访问到的计算机信息系统资源相关的敏感标记，这些安全标记是实施自主或强制访问访问的基础。

主体安全属性主要是用户的属性，描述用户的特征，任何一种属性都可作为访问控制决策点。

3.2 访问控制

- 常用的用户属性有：
  - a)用户ID/用户组ID
  - b)用户访问许可级别
  - c)角色
  - d)权能列表

3.2 访问控制

- 客体安全属性

与客体相关联的属性，常称为敏感标记；

敏感性标记分类：

a）按等级分：公开、机密、秘密、绝密；

B）按非等级： 即范畴，如教学区、生活区行政区等。

3.2 访问控制

用户与主体绑定

- 用户进程是为某特定用户服务的，它在运行中代表该用户对客体进行访问，其权限与所代表的用户相同，即用户与主体的绑定。
- 系统进程是动态地为所有用户提供服务的，它的权限随着服实对象的变化而改变，需要将用户的权限与为其服务的进程的权限动态地相关联。

3.2 访问控制

自主访问控制

- 按客体属主的指定方式或默认方式，即按照用户的意愿来确定某用户对某客体的访问权限，亦即对客体属主是“自主的”。
- 能提供精细的访问控制策略，能将访问控制粒度细化到单个用户(进程)。
- 能为每个客体指定用户和用户组，并规定他们对客体的访问权限，且允许由授权用户指定其他用户对客体的访问权。

3.2 访问控制

自主访问控制

```
/bin/ls
[root@acl tmp]# chown root ls
[root@acl tmp]# ls -l
-rw-r--r--      1 nobody        nobody    770   Oct 18 15:16 4011.tmp
-rw-------      1 root          users     48    Oct 28 11:41 ls
srwxrwxrwx      1 root          root      0     Aug 29 09:04 mysql.sock
drwxrwxr-x      2 duan          uan       4096  Oct 23 23:41 ssl
[root@acl tmp]# chmod   o+rw   ls
[root@acl tmp]# ls -l
-rw-r--r--      1 nobody        nobody    770   Oct 18 15:16 4011.tmp
-rw----rw-      1 root          users     48    Oct 28 11:41 ls
srwxrwxrwx      1 root          root      0     Aug 29 09:04 mysql.sock
drwxrwxr-x      2 duan          duan      4096  Oct 23 23:41 ssl
[root@acl tmp]#
```

3.2 访问控制

强制访问控制

- 在强制访问控制机制下，系统的每个主体被赋予一个许可标记或访问标记，表示许可级别；
- 同样，系统的每个客体也被赋予一个敏感性标记，以反映该客体的安全级别。
- 安全系统通过比较主、客体的相应标记来决定是否授予一个主体对客体的访问请求权限。

3.2 访问控制

Lampson访问控制矩阵模型

将与安全相关的因素概括在访问矩阵中，由三元组(S,O,A)决定，访问权限集包含读、写、追加、修改和执行等。

系统中状态的改变取决于访问矩阵A的改变，一个独立的状态机构成一个系统。

系统中所有主体对客体的访问均由“引用监视器”控制，它的任务是确保只有那些在访问矩阵中获得授权的操作才被允许执行。

3.2 访问控制

Lampson访问控制矩阵模型

	O1	O2	O3	…
S1	ps11	ps12	ps13	…
S2	ps21	ps22	ps23	…
…	…	…	…	…

福州大学
FUZHOU UNIVERSITY

3.2 访问控制

Lampson访问控制矩阵模型

	bill.doc	**edit.exe**	**fun.com**
Alice	**-**	**{x}**	**{x, r}**
Bob	**{r, w}**	**{x}**	**{x, r, w}**

福州大学
FUZHOU UNIVERSITY

3.2 访问控制

Graham-Denning模型

- 此模型更具有一般性，对主体集合S、客体集合O、权力集合R和访问控制矩阵A进行操作。
- 主体有一行，每个主体及所有客体都有一列，一个主体对于另一个主体或对于一个客体的权力用矩阵元素的内容来表示。

3.2 访问控制

Graham-Denning模型

- 对于每个客体，标明为“拥有者”的主体有特殊权力；对于每个主体，标明为“控制者”的另一主体有特殊权力。
- 模型中设计了8个基本保护权，构造一个保护系统的访问控制机制模型所必需的性质，这些权力被表示成主体能够发出的命令，作用于其他主体或客体。

3.2 访问控制

Graham-Denning模型

- Lampson模型和Denning模型的实质是定义了一个访问控制矩阵。
- 为其他访问控制类型的安全模型奠定了良好的理论和设计基础。

3.2 访问控制

Bell-LaPadula模型

- 是最早和最常用的适用于军事安全策略的操作系统多级安全模型，其目标是详细说明计算机的多级安全操作规则。
- 多级安全策略的算术模型，用于定于安全状态机的概念、访问模式以及访问规则。
- 主要用于防止未经授权的方式访问到保密信息。
- BLP模型属于状态机模型。

3.2 访问控制

Bell-LaPadula模型

- BLP模型中，将主体定义为能发起行为的实体，如进程；
- 将客体定义为被动的主体行为的承担者，如文件、目录、数据；
- 将主体对客体的访问分为：只读、读写、只写、执行、控制等访问模式，控制是指主体用来授予或撤销另一主体对某客体的访问权限的能力。

3.2 访问控制

Bell-LaPadula模型

- BLP模型定义了两种按策略：自主安全策略和强制安全策略。
- 自主安全策略使用一个访问矩阵表示，其中，第i行第j列的元素M_{ij} 表示主体S_i对客体O_j的所有允许的访问模式，主体只能按在访问矩阵中被授予对客体的访问权限对客体进行访问。

3.2 访问控制

Bell-LaPadula模型

- BLP模型定义了两种按策略：自主安全策略和强制安全策略。
- 强制安全策略包括简单安全特性和*特性，系统对所有主体和客体都分配一个访问类属性，包括主体和客体的密级和范畴，系统通过比较主体和客体的访问类属性控制主体对客体的访问。

3.2 访问控制

Bell-LaPadula模型

- 简单安全特性规则

一个主体对客体进行读访问的必要条件是主体的安全级支配客体的安全级、即主体的安全级别不小于客体的保密级别，主体的范畴集包含客体的全部范畴，或者说主体只能向下读，不能向上读。

该规则即“读”规则；

3.2 访问控制

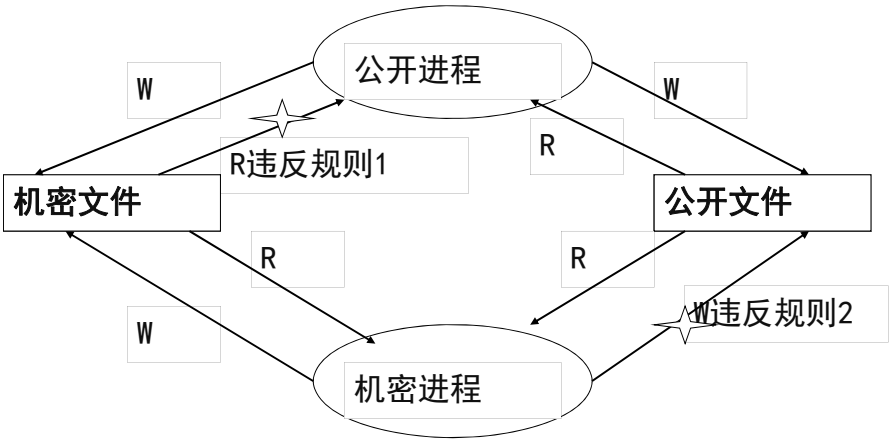
Bell-LaPadula模型

- *特性规则

一个主体对客体进行写访问的必要条件是客体的安全级支配主体的安全级、即客体的保密级别不小于主体的保密级别，客体的范畴集包含主体的全部范畴，或者说主体只能向上写，不能向下写。

该规则即“写”规则；

Bell-LaPadula模型



3.2 访问控制

Bell-LaPadula模型

□BLP模型是最典型的保密性访问控制模型。包括MAC和DAC两个部分，MAC由简单安全特性和*特性组成，通过安全级强制性约束主体对客体的存取，总结为下读上写；DAC通过访问控制矩阵按用户的意愿进行访问控制。

3.2 访问控制

Bell-LaPadula模型

BLP模型的不足

□只涉及机密性，没有涉及完整性。

通过防止非授权信息的扩散保证系统的安全，但不能防止非授权修改系统信息。

□只定义了主体对客体的访问，未说明主体对主体的访问，则该模型难以应用于网络环境。

□该模型不能很好解决隐蔽通道问题…

3.2 访问控制

Bell-LaPadula模型

- 应用中的问题
  - 内存管理能够在所有级别客体进行读和写，在实际应用中有悖于模型本身。除了对它进行“可信假设”外别无他法。
  - 当低级别进程将数据写入高级别进程时（即上写），由于模型的限制，低级别主体无法得到任何反馈，仿佛碰到了“黑洞”一般。

3.2 访问控制

Bell-LaPadula模型

- 应用中的问题
  - 同样数据库系统中，如果高级别用户发送了一批机密货物到轮船上，而系统不会把这个信息传递给低级别用户（否则就是泄密），那么低级别用户将会认为船是空的，并分配其他货物或改变航行的目的地。

3.2 访问控制

Biba模型

1977年由Biba提出，类似BLP模型，保证信息的完整性，包括自主访问控制和强制访问控制。

□模型简介

- 涉及计算机完整性的第一个模型；
- 一个计算机系统由多个子系统组成；
- 子系统是按照功能或权限将系统（主体和客体）进行划分的；
- 在子系统级进行评估系统的完整性；

3.2 访问控制

Biba模型

□模型简介

- 系统完整性威胁来源

✓ 内部威胁：子系统的一个组件是恶意的/不正确的。

✓ 外部威胁：一个子系统通过提供错误数据/不正确的函数调用来修改另一个子系统。

- Biba认为可以通过程序测试和检验来消除内部威胁，因此，该模型仅针对外部模型。

3.2 访问控制

Biba模型

- 完整级别：密级和范畴。
- 完整级别构成服从偏序关系的格。
- 四种存取方式：
  - ✓ Modify，写
  - ✓ Invoke，用于两个主体间，允许相互通信
  - ✓ Observe，读
  - ✓ Execute，执行

3.2 访问控制

Biba模型

- 完整性策略
  - ➢ 最低点策略
  - ➢ Ring环策略
  - ➢ 严格的完整性策略

3.2 访问控制

Biba模型

□严格完整性策略(强制控制策略)

1) 完整*规则：S modify O : L(O)≤L(S)

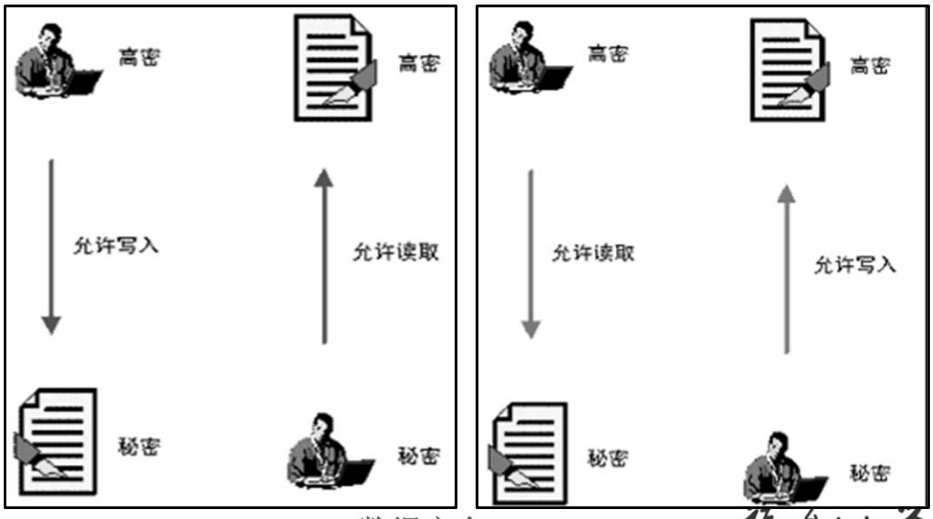
2) 调用规则：S1 invoke S2 : L(S2)≤L(S1)

3) 简单完整条件：S observe O: L(S)≤ L(O)

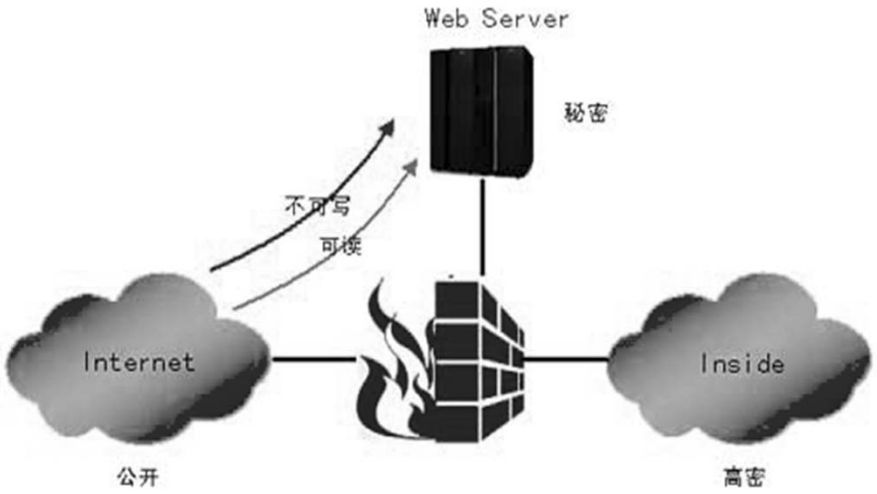
该策略被认为是标准的“Biba模式”，即是BLP模型的对偶：

No Read-Down, No Write-Up

Biba模型



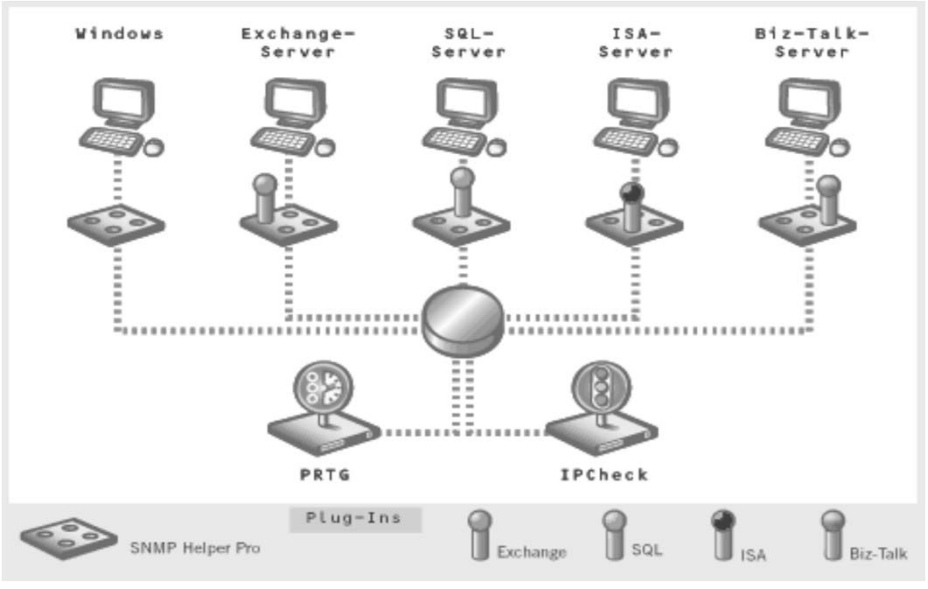
Biba模型-Web实例



数据安全

福州大学 FUZHOU UNIVERSITY

Biba模型-SNMP实例



3.2 访问控制

D.Denning信息流模型

- 有些信息泄露问题(如隐蔽信道)不是因为访问控制机制不完善，而是由于缺乏对信息流的必要保护引起的。
- 在系统中，一个主体S能否获得资源R所包含的信息?这种情况下，主体S不必具有对R的实际访问权限，信息可能经由其他主体到达S，或者信息只是简单地被复制到S可以访问的资源中。

3.2 访问控制

D.Denning信息流模型

- 信息流模型是存取控制模型的一种变形，它不检查主体对客体的存取，而是试图控制从一个客体到另一个客体的信息传输过程，根据两个客体的安全属性来决定是否允许当前操作的执行。
- 隐蔽信道的核心是低安全级主体对高安全级主体所产生的信息的间接存取，**信息流分析**能保证操作系统在对敏感信息存取时，不会把数据泄露给调用者。

自主/强制访问控制的问题

- 自主式太弱
- 强制式太强
- 二者工作量大，不便管理

例：1000主体访问10000客体，须1000万次配置。如每次配置需1秒，每天工作8小时，就需10，000，000/（3600*8）=347.2天；

自主/强制访问控制的问题

- 自主访问控制：配置的粒度小；配置的工作量大，效率低；
- 强制访问控制：配置的粒度大，缺乏灵活性；
- 两者可以结合执行；

3.2 访问控制

RBAC基于角色的访问控制模型

- 起因：
  - 主体和客体的数量级增大，传统模型很难适用；
  - Web、OS、DB等领域；
- 简化策略配置：RBAC发展的动力是在简化安全策略管理的同时,允许灵活地定义安全策略；
- 应用：目前,RBAC 被应用在各个企业领域,包括操作系统、数据库管理系统、PKI、工作流管理系统和Web 服务等领域；

3.2 访问控制

RBAC基于角色的访问控制模型

- 基本思想

基于角色的访问控制是一个复合的规则，每一用户都被分配给一个角色（即被授权的组）。

✓ 提出“角色” （Role）作为授权中介。

3.2 访问控制

RBAC基于角色的访问控制模型

- 基本思想

将访问许可权分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权；

RBAC从控制主体的角度出发，根据管理中相对稳定的职权和责任来划分角色，将访问权限与角色联系，通过给用户分配合适的角色，让用户与访问权限相联系。

RBAC基于角色的访问控制模型

- 实例分析1：

在银行环境中，用户角色可以定义为出纳员、分行管理者、顾客、系统管理员和审计员；

（1）允许一个出纳员修改顾客的帐号记录；

（2）允许一个分行管理者修改顾客的帐号记录，并允许查询所有帐号的注册项，也允许创建和终止帐号；

（3）允许一个顾客只询问他自己的帐号的注册项；

（4）允许系统管理员询问系统的注册项和开关系统，但不允许读或修改用户的帐号信息；

（5）允许一个审计员读系统中的任何数据，但不允许修改任何事情；

RBAC基于角色的访问控制模型

□实例分析2：

Tch1，Tch2，Tch3……Tchi是对应的教师;Stud1，Stud2，Stud3 …Studj是相应的学生;

- ✓Mng1，Mng 2，Mng3…Mngk是教务处管理人员;
- ✓老师的权限为TchMN={查询成绩、上传所教课程的成绩}；
- ✓学生的权限为StudMN={查询成绩、反映意见}；
- ✓教务管理人员的权限为MngMN={查询、修改成绩、打印成绩清单}。

RBAC基于角色的访问控制模型

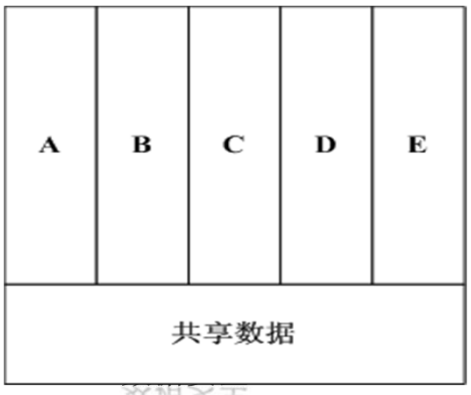
□RBAC的优点：

- ➢ 便于授权管理；
- ➢ 便于根据工作需要分级；
- ➢ 便于赋予最小特权，只有必要时方能拥有特权；
- ➢ 便于任务分担，不同的角色完成不同的任务；
- ➢ 便于文件分级管理，文件本身也可分为不同的角色，如信件、账单等，由不同角色的用户拥有；

3.2 访问控制

多边安全模型

- 共享信息结构
- 多边安全控制模型控制数据在A、B、C、D、E之间的流动。



福州大学 FUZHOU UNIVERSITY

3.2 访问控制

布鲁尔-纳什模型（Brewer and Nash model）动态变更可存取控制

多边安全模型-Chinese Wall模型

- 模型简介

中国墙模型是一种同等地考虑保密性与完整性的安全模型。

该模型主要解决商业中的利益冲突问题，其重要性等同于BLP模型在军事中的意义。

福州大学 FUZHOU UNIVERSITY

3.2 访问控制

多边安全模型-Chinese Wall模型

□模型简介

中国墙模型通常用于股票交易所或者投资公司的经济活动等环境中。在这种意义上，中国墙模型的目标就是防止利益冲突的发生。

当交易员代理两个客户的投资，并且这两个客户的最大利益相互冲突时，交易员就有可能帮助其中一个客户盈利，而导致另一个客户的损失。

3.2 访问控制

多边安全模型-Chinese Wall模型

□模型安全策略

- 主体只能访问那些与已经拥有的信息不冲突的信息。
- 一个主体一旦已经访问过一个客体，则该主体只能访问位于同一公司数据集中的客体，或在不同兴趣冲突组中的信息。
- 在一个兴趣冲突组中，一个主体最多只能访问一个公司数据集

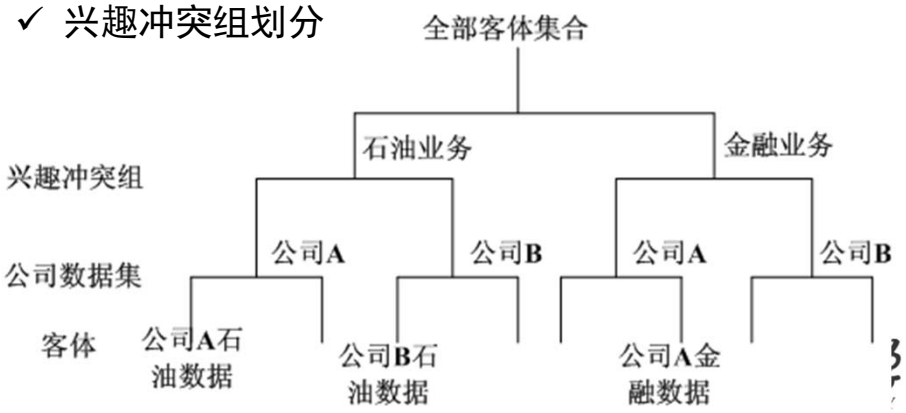
3.2 访问控制

多边安全模型-Chinese Wall模型

□应用实例分析

✓ 有公司A、B，数据为石油业务数据、银行数据；

✓ 兴趣冲突组划分



3.2 访问控制

多边安全模型-Chinese Wall模型

□应用实例分析

□访问控制

➢第一次访问是自由的，设访问A石油业务数据集；

➢可以访问A金融数据集；不可以访问B石油数据集。

□总结：

1）可以访问与主体曾经访问过的信息同属于同一个公司的数据集，即墙内信息；

2）可以访问一个完全不同的兴趣冲突组。

3.3 身份识别与认证

- 随着互联网的不断发展，越来越多的人们开始尝试在线交易。然而病毒、黑客网络钓鱼以及网页仿冒诈骗等恶意威胁，给在线交易的安全性带来了极大的挑战。近些年国内外网络诈骗事件层出不穷，给银行和消费者带来了巨大的经济损失
- 层出不穷的网络犯罪，引起了人们对网络身份的信任危机，如何证明“我是谁？”及如何防止身份冒用等问题是必须要解决的问题 .

3.3 身份识别与认证

- 身份认证的概念
- 基于口令的身份认证
- 基于USB Key的身份认证
- 基于生物特征的身份认证
- 网络实名制

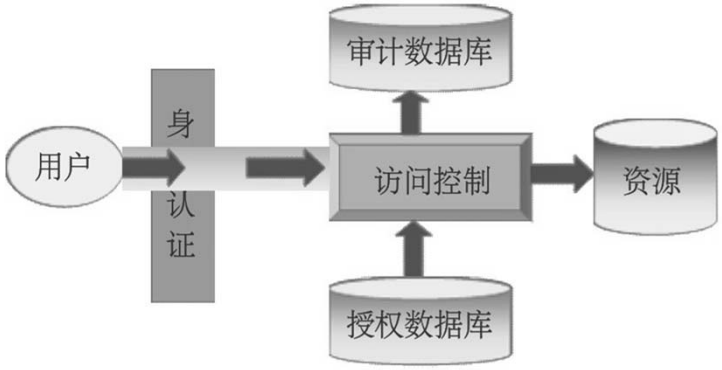
身份认证的概念

身份认证是指计算机及网络系统确认操作者身份的过程在数字世界中，一切信息包括用户的身份信息都是用一组特定的数据表示的，计算机只能识别用户的数字身份，所有对用户的授权也是针对用户数字身份的授权。

身份识别是安全体系的第一道大门，是网络安全的基石，是名副其实的网络安全体系的“门禁”.

数据安全

身份认证在安全中的作用



✓ **用户认证有两个理由：**

用户身份是访问控制决策的一个参数，计算机安全在将安全相关事件记入审计日志时，需要记录用户身份。

FUZHOU UNIVERSITY

3.3 身份识别与认证

安全系统有时必须检查请求服务的用户的身份，认证就是验证用户身份的过程.

例如：张三其人 – 外部实体；用户id – 身份；用户进程– 主体

- ✓ 外部实体必须提供信息，允许系统证实他的身份；实体身份控制与其关联的主体可以进行的操作；因此一个主体必须绑定到外部实体的身份；认证过程由从实体获取鉴别信息、分析数据和确定鉴别 信息是否与被认证的实体相关联。这样，计算机必须存储一些关于实体的信息.

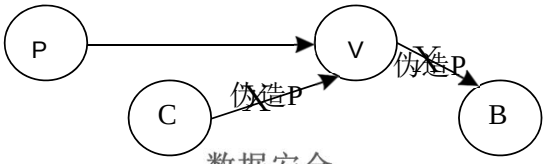
认证系统

认证系统（Authentication system）由五个部分组成：

- ➢鉴别信息的集合A 实体用来证明其身份的特定信息的集合。如Unix的明文口令的集合；
- ➢辅助信息的集合C 系统存储并且用来证实鉴别信息的信息集合。如Unix的密文口令的集合；
- ➢辅助函数的集合F 由鉴别信息产生辅助信息的函数的集合。即，f∈F，f：A →C。如Unix的Hash函数的集合；
- ➢鉴别函数的集合L 验证身份的函数的集合。即，对于l ∈ L，l：A×C →{true，false}；
- ➢选择函数的集合S 允许实体创建或改变鉴别信息和辅助信息。如创建、修改口令；选择加密算法.

身份认证协议

- 身份认证协议涉及一个证明者P和验证者V，P要让验证者V相信“他是P”。他们必须做到：
  - P和V在诚实的情况下，P能让V成功的识别自己，即在协议完成时，V接受了P的身份；
  - V不能重新使用自己和P识别过程中的信息伪装成P, 向第三者B证明自己是P；
  - 除了P以外的第三者C以P的身份执行该协议，能让V 相信C是P的概率可以忽略不计.



可供选择的身份认证方法

- 从一般的观点看，可以选择基于以下信息进行身份认证：
  - **你知道的事情**
  - **你拥有的东西**
  - **你是谁**
  - **你做什么**
  - **你在哪里**

你知道的事

- 用户必须知道一些“ 秘密” 才能被认证。例如，用户拥有的口令、个人身份识别号码（PIN）或者类似的令牌(tokens)、信用 卡电话银行确认在这种认证模式中，关键是如何认证“ 秘密” 而又
- 不泄漏秘密

可能存在的问题

- 认证中心是否可信？
- 钓鱼攻击

你拥有的东西

- 用户必须出示一个被认证的物理令牌
- 例如，能打开锁的钥匙，用于控制进入公司大门的卡片或身份标志（identity tag）。智能卡（smart cards）可能成为口令的替代物；
- 物理令牌可能会遗失或被盗；
- 为了增加安全性，物理令牌通常与所知道的事结合起来使用，如银行卡与PIN一起使用，或者它们包含能够识别合法用户的信息，如银行卡上的照片；
- 典型应用：USB key

你是谁

- 为了准确地认证每一个用户，可以使用生物测定技术。例如，带有照片的卡片（如身份证、护照等），更复杂的方法使用掌纹、指纹、虹膜图案或视网膜图案来识别一个人；
- 生物测定技术或许能够为个人认证提供最终解决方案；
- 在生物认证中，比较常见的是指纹，例如：
  上班打卡机

你做什么

- 人们往往以一种独特和可重复的方式做一些机械性的工作：
  - 检查手写签名就是来自纸质文档世界的一个例子，在这里伪造并不是那么困难的。为获得更高的安全性，用户可以在一个特殊的垫子上签名，垫子可以测量出像书写速度和书写力度这样的特征；
  - 在一个键盘上，打字速度以及击键之间的间隔被用来认证用户个人。如前所述，认证系统必须建立起来，使得假肯定和假否定减少到相关应用可以接受的程度；

你在哪里

- 在用户登录时，系统可能还要考虑用户在哪里;
  - 例如，限制用户从某个特定的终端注册时才允许访问；如系统管理员只能从操作员控制台注册；类似地，作为用户只允许他从他所在办公室的工作站上登录，ip认证;
  - 在移动和分布式计算中, 系统可以使用全球定位系统（GPS, Global Position System）来确定确定用户登录的位置，也有助于解决过后关于用户真实身份的争端;

常见的身份认证方法

- 基于用户名和口令的认证
- 基于USB Key的身份认证
  - 基于对称密码/公钥密码的认证
- 基于生物特征的身份认证
  - 指纹
  - 视网膜
  - 语音

只认证“身份”，不认证“人”

- **口令等**身份认证并不能认证人，只是认证了用户知道一个特定的秘密，但没有办法区分合法用户.or.获得了该用户口令等特征的入侵者；
- 身份的主题贯穿在人类经历中，计算机也不例外。在计算机科学，身份是特权指派的基础，且在保护域意义上是完整的；
- **身份的2个主要用途**：可审计性和访问控制

基于口令的身份认证

- ✓概述
- 口令管理和选择
- 欺骗攻击
- 保护口令文件
- 一次签到
- 口令的缺点

基于口令的身份认证

- 口令又称个人识别码或通信短语，通过输入口令进行认证的方法便称为基于口令的认证方式；
- 口令认证是最常用的一种认证技术。目前各类计算资源主要靠固定口令的方式来保护；
- 大多数计算机系统使用基于用户名和口令的身份识别和认证技术作为它们的第一道防线；

用户名与口令

- 登录计算机时要求输入用户名和口令
  - 第一步称为身份识别，即声明你是谁
  - 第二步称为认证，即证明你是所声称的那个人
- 实体认证　验证一个被声称的身份的过程;
- 为了防止攻击者以注册用户身份使用计算机，不仅可以在会话开始时要求认证，也可以在会话期间定期要求认证（重复认证）；
  - 可以选择锁住屏幕，或当某个用户空闲太久时自动关闭其会话;
  - 而操作系统在会话开始时检查用户身份，但是在后期会话过程中一直使用这个身份来进行访问控制决策;

口令认证机制的安全性

- 作为认证机制的口令的实际安全性：
  - 遗忘口令 重新设置口令
  - 口令猜测 弱口令，用户信息，家庭成员的信息
  - 口令欺骗 通过假冒的登录程序或社会工程骗取口令口令
  - 文件泄漏 脱机的字典攻击
- 基于用户名和口令的身份验证机制不能防止窃听攻击：
  - 键盘记录器
  - 口令明文传输
  - 网络嗅探
  - 旁道攻击，如输入键盘上的灰尘分布、击键声音等

口令管理

- 口令存放到正确的位置
- 一次性登录口令，供他人临时使用；
- 最常用的口令，切记不要告诉他人；
- 若干套口令，相互隔离
  - 银行卡、电子邮件、论坛等
- 遗忘口令时的口令恢复
  - 防患于未然

选择口令

- 口令选择是一个重要的安全问题
  - 不能完全避免攻击者意外地猜测出有效的口令，但可以努力使这种事件的发生率尽可能的低；
- 攻击者基本上遵循以下两种猜测策略：
  - 穷尽搜索（exhaustive search）又称蛮力攻击，在一定长度范围内，尝试有效符号所有可能的组合；
    - 口令空间，口令字符集和口令长度

选择口令

- 智能搜索（intelligent search空间进行搜索
  - ✓尝试那些与用户有联系的口令，像名字、朋友和亲戚的名字、汽车商标、车牌号、电话号码、生日等；
  - ✓尝试那些较常流行的口令。这种方法的一个典型例子是字典攻击，它尝试来自于一个在线字典的所有口令；

防卫口令猜测的措施

- **设置口令**
  - guest账户
  - 系统初始安装时administrator口令为空；
- **更改默认口令**
  - 默认帐户口令有助于安装系统；但如果不改变口令，则为攻击者留下了后门，且攻击者在进入该系统后，使用该系统来攻击其它系统
  - SQL Server的sa管理员密码为空；
  - Movable Type blog系统的默认用户名/密码为Melody/Nelson

防卫口令猜测的措施（续）

- 口令长度
  - 为了挫败穷尽搜索，必须规定一个最小口令长度。口令长度和每个口令字符的取值范围决定了系统的口令空间 ；
- 口令格式
  - 在口令中混合使用大、小写字母，并且包含数字和其他非字母符号－特殊符号等；
  - sina邮箱密码不能使用特殊符号；
- 避免显著口令
  - 目前字典攻击已经大大扩展了“ 易于猜测”的范围；
  - 123456 → i23456，!23456；infosec → 1nf0sec

弱口令

rank	密码	次数	rank	密码	次数
1	123456	4,138,464	11	123321	183,741
2	123456789	1,070,028	12	666666	134,599
3	111111	1,033,040	13	1234567	127,268
4	123123	471,036	14	111222tianya	116,015
5	000000	428,307	15	7758521	115,560
6	12345678	409,722	16	1314520	115,227
7	wodima123	392,869	17	888888	110,647
8	5201314	298,458	18	a321654	106,441
9	a123456	195,049	19	654321	100,137
10	11111111	186,429	20	woaini	99,977

福州大学 FUZHOU UNIVERSITY

系统进一步提高口令的安全性

- 口令检查器：检查弱口令，以阻止针对系统的字典攻击
- 口令生成：使用口令发生器，生成随机的和可推断的口令。用户不允许选择自己的口令，而必须采用系统建议的口令。**如附加码**
- 口令老化：设置口令到期的日期，迫使用户定期改变口令
- 限制登录尝试：系统可以监视不成功的登录企图并作出反应，完全锁住用户帐户，或至少锁住一段时间，以防止或阻止进一步的尝试。如ATM、windows登录

福州大学 FUZHOU UNIVERSITY

系统进一步提高口令的安全性

- 通知用户：在成功登录之后，系统可以显示上一次登录的时间以及从那以后失败的登录企图次数，从而提醒用户有关最近的攻击企图。
- 密码输入器、软键盘、随机键盘：防止键盘记录、密码窃取；

口令管理

- 不能孤立地看待安全机制
  - 口令保管得当；
  - 口令的复杂性 VS. 人的记忆能力；
  - 更改口令时，重复输入多次；
  - 有效的口令恢复机制；

欺骗攻击

- 通过用户名和口令的身份识别和认证提供了单向认证（unilateral authentication），即计算机认证用户；
- 单向认证导致了第二类口令威胁 欺骗攻击
  - 攻击者在某些终端或工作站上给出一个假的登录屏幕；
  - 受害者通过标准登录菜单的引导被要求输入用户名和口令，这些信息被攻击者保存下来。
  - 然后执行可能被移交给用户，或者用一个（假的）出错消息中止登录，欺骗程序终止运行。控制被返回到操作系统，运行操作系统的登录程序，进行第二次登录；
  - 例如：网络上的用户名/密码诱骗，MSN，银行自助服务区门禁；

欺骗攻击

- 防范这样的欺骗攻击的对策
  - 显示失败的注册次数 可以暗示用户已经发生过这样的攻击；
  - 可信通路: 保证用户是与操作系统（可信计算机基TCB）通信而不是与一个欺骗程序在通信;
  - 相互认证: 在用户和可信计算基之间进行相互认证；

口令的“查找”和“截获”问题

- 除了欺骗攻击，入侵者还可以有其他“查找”口令的方法
  - **口令缓存**，特别是在分布式系统中的**对象重用**:
  - 口令会被临时存放在中间存储位置，如缓冲器、高速缓存，或者甚至是一个网页。这些存储位置的管理通常超出用户的可控范围，而口令在这些位置的存放时间可能会比用户预料的要长;
- 认证基于秘密信息；如果在网络环境下使用用户名和口令来认证用户身份，明文口令会在网上传输，则导致口令泄漏。即使在网上传输密文口令，密文口令也容易遭到重放攻击;

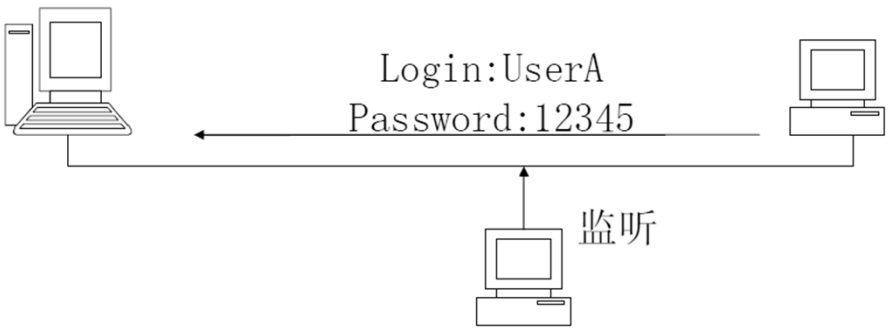
口令的“查找”和“截获”问题

重放攻击：主机A给主机B发送的报文被攻击者C截获了，然后C伪装成A给B发送其截获来的报文，而B会误以为C就是A，就把回应报文发送给了C。

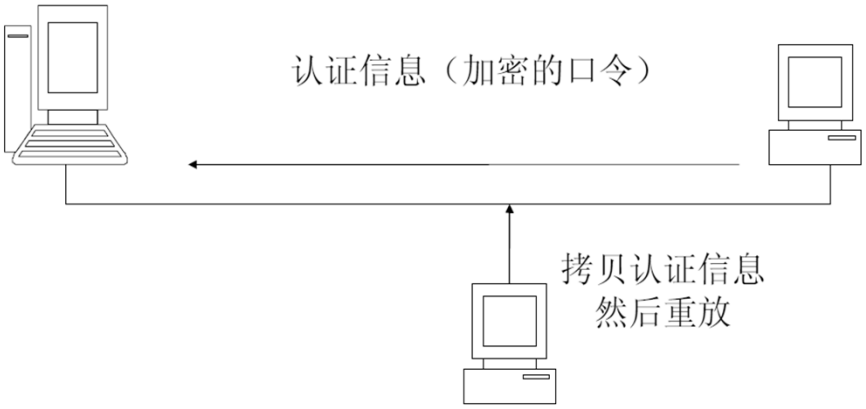
口令的重用问题

- 口令有一个基本问题：口令可以重用
  - 如果攻击者获取了口令，他可以重放口令。系统不可能区分知道口令的攻击者和合法用户。在网络环境下，必须进行双向认证
  - 可选择的解决方法：每次传送的口令改变（一次性口令）
- 一次一密最安全
  - 密钥随机产生，不重复使用
  - 密钥与明文的长度一致，异或产生密文量子密钥

口令攻击：窃听



口令攻击：截取/重放



福州大学
FUZHOU UNIVERSITY

保护口令文件

- 未加密的口令文件内容泄漏或者是文件内容的修改，构成了第三类口令威胁
- 加密的口令文件的泄露也会导致离线处理的字典攻击
- 为保护口令文件，可采取如下措施：
  - 加密保护（Hash加密，单向加密），存储加密后口令的密文；
  - 由操作系统执行访问控制，限制对口令文件的访问；
    - 操作系统中的访问控制机制只允许拥有适当权限的用户访问文件和其它资源。只有特权用户才能访问口令文件
  - 组合加密保护和访问控制，为了减慢字典攻击的速度，甚至可以使用更多的增强措施，如Unix在加密口令时增加了12位的盐值（salt），称为口令盐化（password salting）
    - 即使是相同的算法，相同的原始口令，使用不同的salt，也会得到不同的加密口令

福州大学
FUZHOU UNIVERSITY

单向函数

- 单向函数就是易于计算但很难逆推的函数。即给定x很容易计算f(x)，但给定f(x)很难计算x
  - 单向函数用来保护存储的口令
- Unix系统选择使用单向函数crypt(3)，该函数使用略加修改的DES（Data Encryption Standard，数据加密标准）算法，用全零的数据块和12位（bits）的盐值作为初始值（52位的0＋12位的salt），用口令作为密钥（56位），重复运行算法25次

Unix的口令文件

- Unix将加密的口令保存在一个不可公开访问的文件中，这样的文件被称为影子口令文件 (shadow password files) 。Linux：/etc/shadow ；
- 专用存储格式提供了一种较弱的读保护形式，比如Windows NT以专门的二进制格式保存加密的口令；
- 三个安全设计的问题：
  - 几种机制的组合可以增强保护。加密和访问控制用来保护口令文件；
  - 通过隐匿而获得的安全性只能防御不经心的入侵者。
    不要对这种策略抱太多的信任；
    Windows的文件隐藏功能

Unix的口令文件

- 如果可能的话，将安全相关的数据和那些要被公开访问的数据隔离开来；
- 在Unix中，/etc/passwd包含有以上两种数据。影子口令文件（ /etc/shadow)能够获得所希望的隔离性；

一次签到

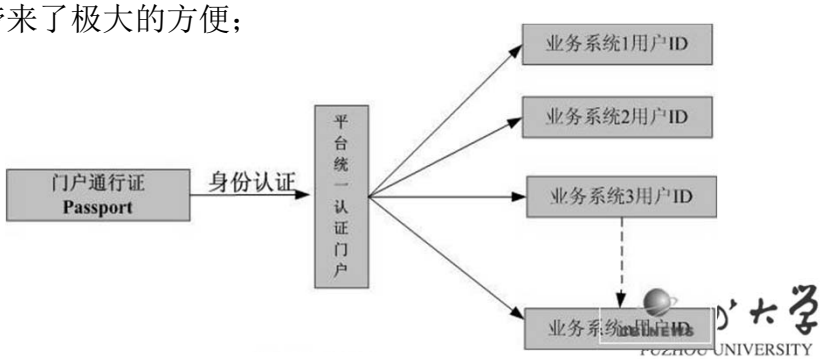
- 在IT环境中，用户名和口令用来控制对计算机、网络、程序和文件等的访问。但如果为获取一点信息而在信息空间漫游时必须一遍又一遍地输入口令，这会令人不快；
- 一次签到服务（single sign-on service）解决了这个问题。用户只要输入一次口令，系统保存这个口令，并在需要重新认证时使用保存的口令进行认证
  - 网站上的记住用户名、密码选项；
  - Cookie；

一次签到（续）

- 一次签到服务的安全问题
  - 系统现在需要以明文的形式存储口令？
  - 如何保护存储的口令？
  - 如何传输明文形式的口令？
- 注：系统设计者必须均衡考虑方便性和安全性。易于使用是使得IT系统真正有用的一个重要因素，不幸的是，许多方便的举措也引入了新的脆弱性；

门户的“一次签到”

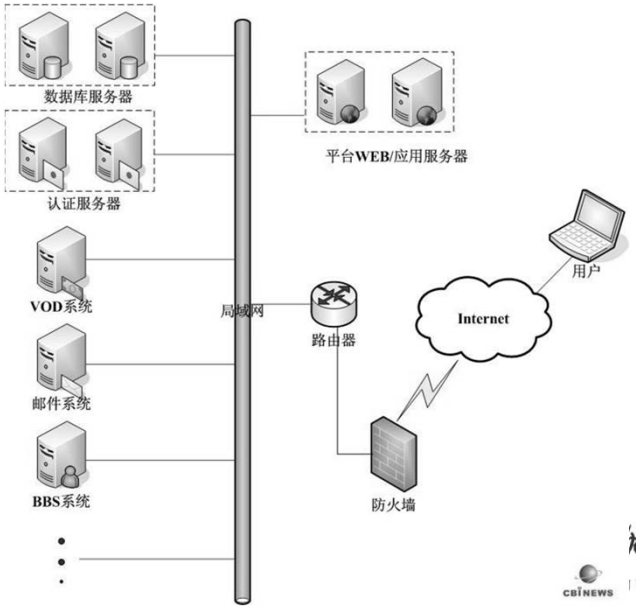
- 门户通行证和注册入口：首先用户通过在平台上注册信息，成为平台用户；
- 通过门户通行证登录门户系统，经平台认证的用户可以根据自己权限访问各个具体的业务系统，而且用户在通过平台认证后，只要IE浏览没有关闭，用户可在各业务系统间随意切换，不需要再次的输入用户登录信息，给网站用户带来了极大的方便；



门户网站的统一身份认证

- 门户网站是一个集新闻、电子邮件、短信以及各种网络增值业务和无线资讯为一体的综合平台；
- 解决方案：集身份认证、单点登录、集中管理和安全通道为一体；
- 统一身份认证平台由管理系统、认证服务器、认证数据库以及业务系统的认证前置程序组成；

门户网站的统一身份认证平台



门户网站的统一身份认证

- 门户系统增加用户与业务系统帐户的Mapping页面：用户在使用门户通行证登录门户后，第一次访问业务系统时，需要完成与业务系统帐户的映射（mapping），该页面根据认证平台中业务系统的配置自动生成；
- 门户首页中各业务系统的链接地址更改为虚拟地址：实施统一认证后，门户首页中的各业务系统链接地址均改为虚拟地址，用户点击该地址时，平台首先检查用户是否已登录门户通行证，如果没有则跳转到门户通行证的登录页面，登录后在再通过认证服务器和业务系统认证前置程序之间的SSL加密通道自动认证，直接进入要访问的业务系统；

门户网站的统一身份认证

- 资源整合：认证平台以资源整合为中心，通过平台的管理系统和数据库，统一用户资源和各增值业务系统，实现用户的统一管理和访问控制，实现各系统资源的统筹管理；
- 身份认证和单点登录：认证平台通过统一的用户帐户对用户身份进行认证，在通过平台认证后，用户可直接访问各个业务系统，实现用户身份认证信息的共享，从而达到多业务系统的单点登录；
- 安全通道：认证平台提供两种安全通道：一种是单向SSL加密，一种是双向SSL加密安全通道，充分保证登录认证过程和业务系统访问过程的安全性；

口令的缺点

- 口令在网络中传输时是很容易被窃取或攻击的，这是口令认证的明显缺点。比较常见的攻击和窃取方式主要有以下几种：
- 网络数据流窃听：由于认证信息要通过网络传递，并且很多认证系统的口令是未经加密的明文，攻击者很容易的通过窃听网络数据，分辨出某种特定系统的认证数据，并提取出用户名和口令；
- 认证信息截取/重放：有些系统会将认证信息进行简单加密后进行传输，如果攻击者无法用网络数据流窃听方式推算出密码，将使用截取/重放方式，再进行分辨和提取；

口令的缺点（续）

- 字典攻击：大多数用户习惯使用有意义的单词字符或数字作为密码，如名字、生日；某些攻击者会使用字典中的单词来尝试用户的密码。所以大多数系统都建议用户在口令中加入特殊字符，以增加口令的安全性；
- 穷举尝试：这是一种属于字典攻击的特殊攻击方式，它使用字符串的全集作为字典，然后穷举尝试进行猜测。如果用户的密码较短，则很容易被穷举出来，因而很多系统都建议用户使用较长的口令，最好采用数字、字符混合的方式并加入特殊字符；

口令的缺点（续）

- 窥探口令：攻击者利用与被攻击系统接近的机会，安装监视器或亲自窥探合法用户输入口令的过程，以得到口令。所以用户在输入口令时，应该注意旁边的人是否可疑；
- 骗取口令：攻击者冒充合法用户发送邮件或打电话给管理人员，以骗取用户口令；
- 垃圾搜索：攻击者通过搜索被攻击者的废弃物，得到与被攻击系统有关的信息；

本章内容

- 身份认证的概念
- 基于口令的身份认证
- ✓ 基于USB Key的身份认证
- 基于生物特征的身份认证
- 网络实名制

USB Key

福州大学
FUZHOU UNIVERSITY

USB Key历史

- USB Key产品最早是由加密锁厂商提出来。 原先的USB加密锁主要用于防止软件破解和复制，保护软件不被盗版，又叫“ 加密狗 ”；
- USB Key的目的不同，USB Key主要用于网络认证，锁内主要保存数字证书和用户私钥；

福州大学
FUZHOU UNIVERSITY

USB Key特点

- USB Key结合了现代密码学技术、智能卡技术和USB技术，是新一代身份认证产品，它具有以下特点：
- 双因子认证
  - 每一个USB Key都具有硬件PIN码保护，PIN码和硬件构成了用户使用USB Key的两个必要因素，即所谓“双因子认证”；
  - 用户只有同时取得了USB Key和用户PIN码，才可以登录系统；
    - 即使用户的PIN码被泄漏，只要用户持有的USB Key不被盗 取，合法用户的身份就不会被仿冒；
    - 如果用户的USB Key遗失，拾到者由于不知道用户PIN码；
      也无法仿冒合法用户的身份；

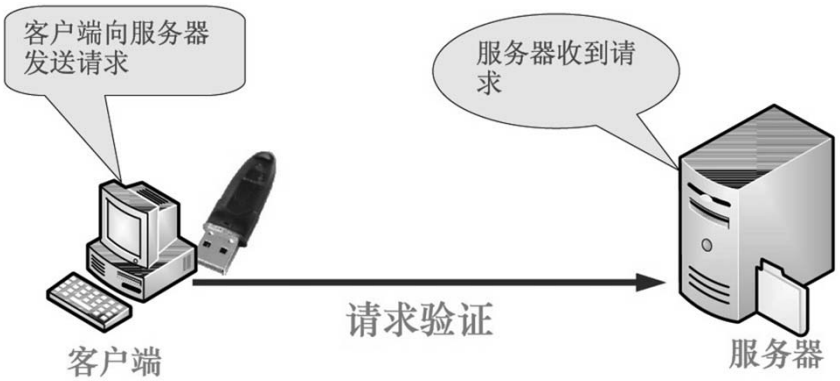
USB Key特点（续）

- 带有安全存储空间
  - USB Key具有8K-128K的安全数据存储空间，可以存 储数字证书、用户密钥等秘密数据；
- 硬件实现加解密算法
  - USB Key 内置CPU或智能卡芯片，可以实现PKI体系中使用的数据摘要、数据加解密和签名的各种算法，加解密运算在USB Key内进行，保证了用户密钥不会出现在计算机内存中，从而杜绝了用户密钥被黑客截取的可能性；
- 便于携带，安全可靠
  - 如拇指般大的USB Key非常方便随身携带，并且密钥和证书不可导出，Key的硬件不可复制，更显安全可靠；

USB Key应用模式

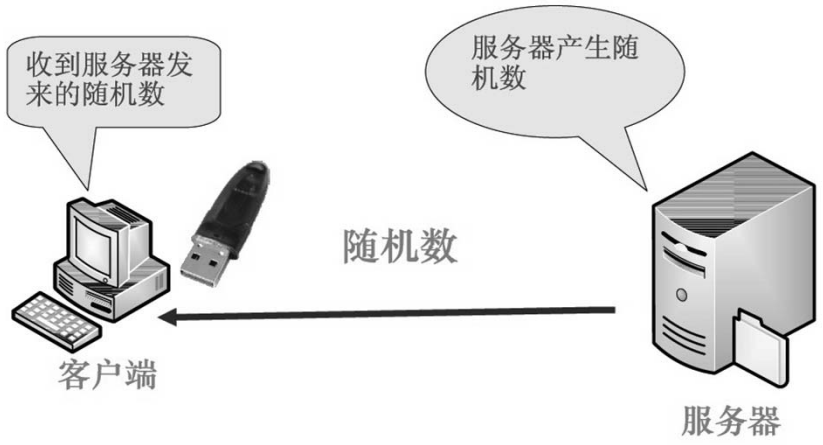
- 1）基于冲击-响应认证模式
  - USB Key内置单向散列算法（MD5），预先在USB Key和服务器中存储一个证明用户身份的密钥；
  - 当需要在网络上验证用户身份时，先由客户端向服务器发出一个验证请求；
  - 服务器接到此请求后生成一个随机数回传给客户端PC上插着的USB Key，此为“冲击”；
  - USB Key使用该随机数与存储在USBKey中的密钥进行MD5运算得到一个运算结果作为认证证据传送给服务器，此为“响应”；
  - 与此同时，服务器使用该随机数与存储在服务器数据库中的该客户密钥进行MD5运算，如果服务器的运算结果与客户端传回的响应结果相同，则认为客 户端是一个合法用户；

基于冲击-响应认证模式的认证流程



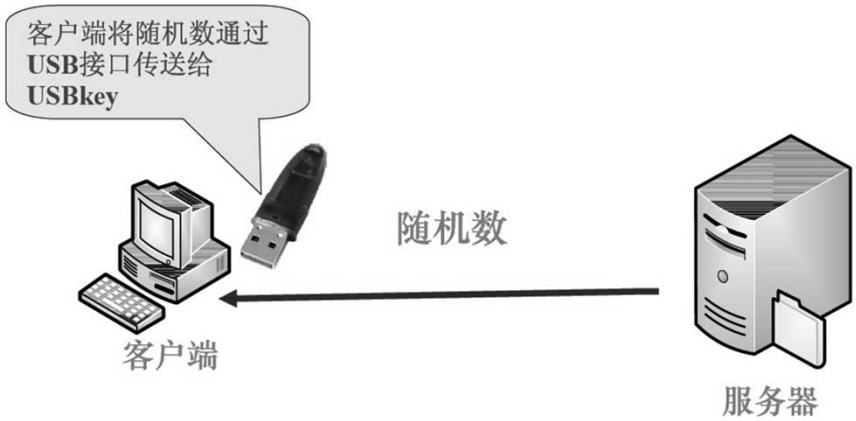
福州大学 FUZHOU UNIVERSITY

基于冲击-响应认证模式的认证流程



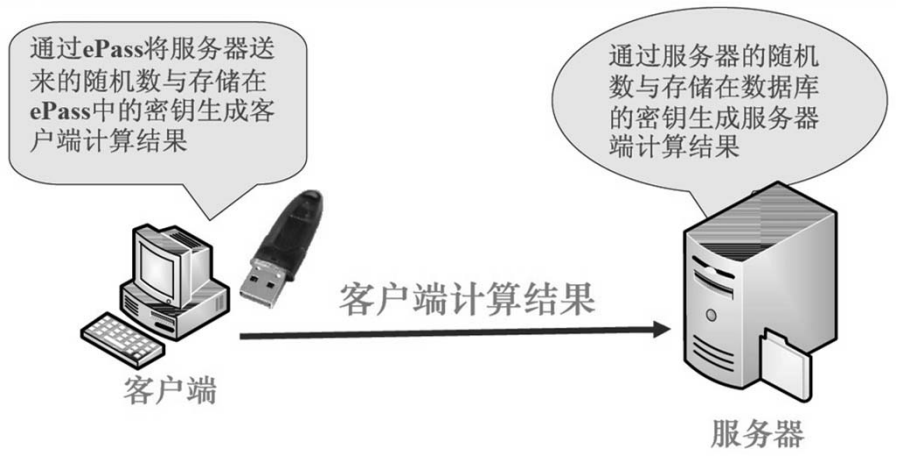
福州大学
FUZHOU UNIVERSITY

基于冲击-响应认证模式的认证流程



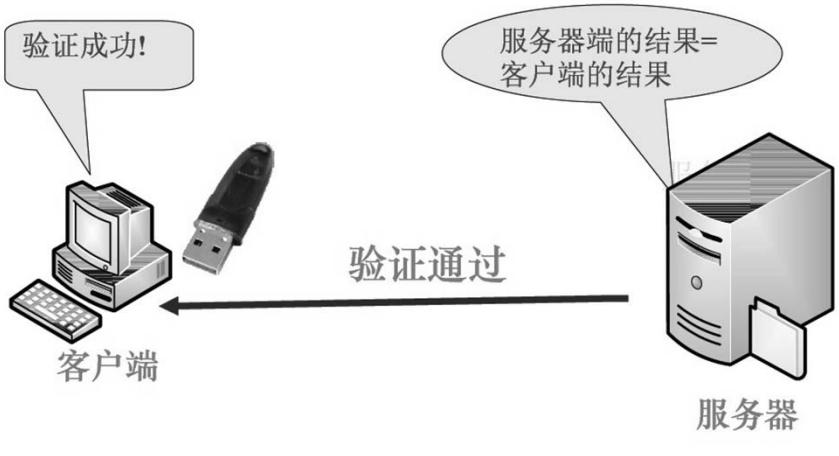
福州大学
FUZHOU UNIVERSITY

基于冲击-响应认证模式的认证流程



福州大学
FUZHOU UNIVERSITY

基于冲击-响应认证模式的认证流程

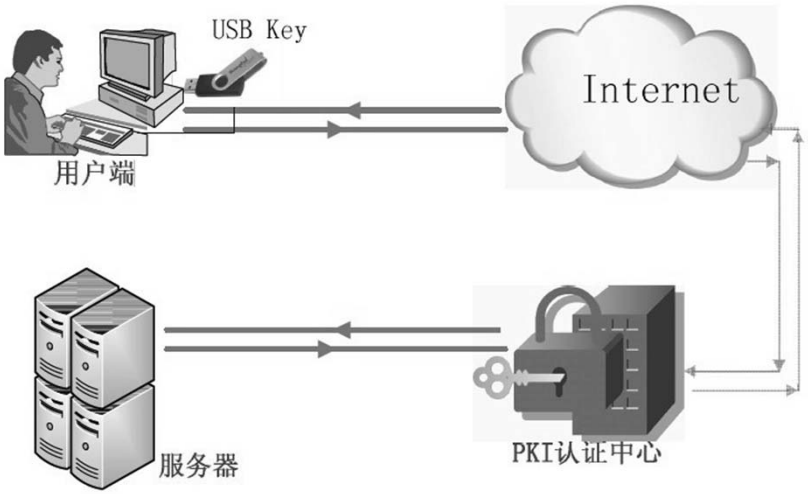


福州大学
FUZHOU UNIVERSITY

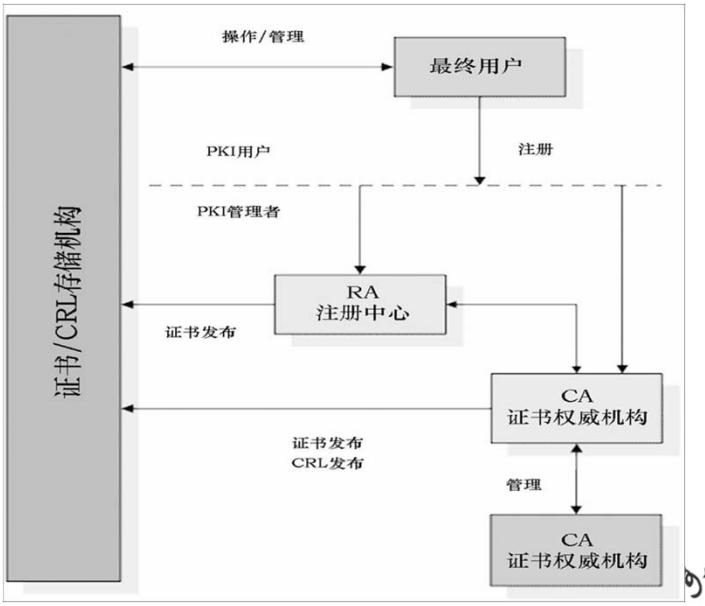
USB Key应用模式

- 2）基于数字证书的认证方式
  - PKI（Public Key Infrastructure）即公共密钥体系，即利用一对互相匹配的密钥进行加密、解密；
  - 一个公共密钥（公钥，public key）和一个私有密钥（私钥，private key）；
  - 其基本原理是：由一个密钥进行加密的信息内容，只能由与之配对的另一个密钥才能进行解密；
  - 公钥可以广泛地发给与自己有关的通信者，私钥则需要十分安全地存放起来

基于数字证书的认证方式



以CA认证为中心的PKI系统



FUZHOU UNIVERSITY

USB Key应用

- 网银。目前工行的USB Key产品为“U 盾”，招行的USB Key产品为“友Key”，两者的主要供应商都是USB Key的专业厂商捷德公司；
- 现行网银客户端的保障方面，主流是使用USB Key，还有使用动态口令牌、短信密码等；

USB Key安全问题

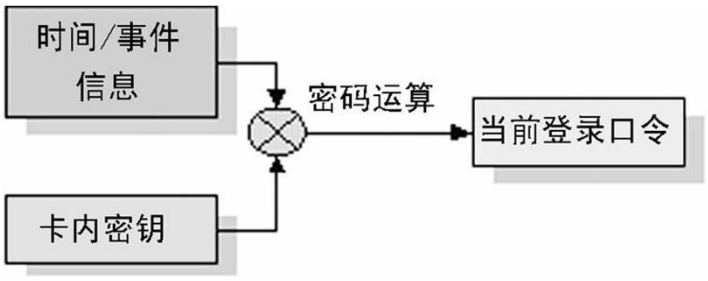
- 客户端的交互操作存在漏洞。由于PIN码是在用户电脑上输入的，因此黑客依然可以通过程序截获用户PIN码，如果用户不及时取走USB Key，那么黑客可以通过截获的PIN码来取得虚假认证。黑客可以远程控制，冒用客户的USB Key进行身份认证，而客户无法知晓
  - 这种漏洞的解决方式是在USB Key上增加一个确认键，用户按USB Key上的确认键后才能进行一次认证
- 无法防止数据被篡改。客户的一笔交易在送入USB Key加密前，可能会被黑客拦截屏篡改为另外一笔交易，这样可以在用户不知情的情况下篡改交易而认证通过
  - 这种漏洞的解决也需要变更USB Key的硬件，在USB

动态口令牌

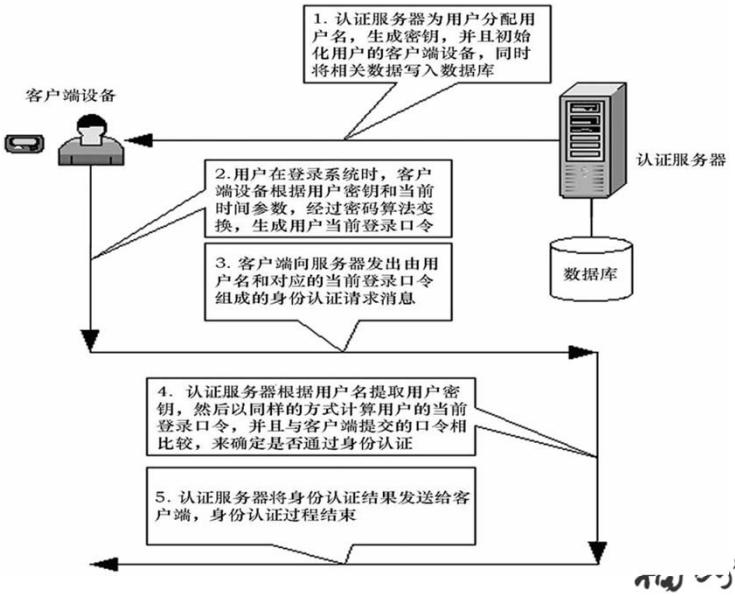
- 动态口令牌，又叫动态密码锁
  - 动态密码锁是透过1组数学加密算法，使用者手中会持有1组显示器(token)，该显示器会与后端服务器同步计算，并出现1组密码数字，使用者必须在一定的时间内(如30秒钟)完成密码输入，才能完成帐号登入，若是超过时限则会出现新的密码数字，必须重新执行帐号登入；
  - 采用动态口令的认证方式就是在每次用户登录时除了输入常规的静态口令外，还要再输入一个每次都会变化的动态口令；

动态口令认证系统

- 动态口令认证系统利用用户密钥和时间双因素，产生随时间变化的有效用户口令，对用户身份进行认证；



动态口令身份认证原理

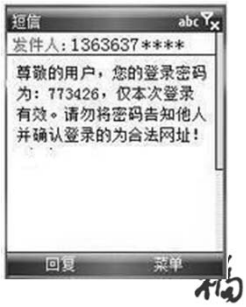


动态口令牌 – 优点

- 无须安装软件，操作简单。与客户电脑无关，不需要安装其他任何程序即可直接使用网上银行服务；
- 一次一密，解决了客户密码被盗的问题。这应该是动态口令牌在安全性方面带来的最大好处：很大程度上解决了传统的用户名/静态口令认证方式存在的口令易泄露，用户身份容易被冒充的安全隐患，增强了用户名/ 口令份认证机制的安全性；

短信密码

- 短信密码以手机短信形式请求包含6位随机数的动态密码，身份认证系统以短信形式发送随机的6位密码到客户的手机上；
- 客户在登录或者交易认证时候输入此动态密码，从而确保系统身份认证的安全性。利用what you have方法；



短信密码 – 优点

- **安全性**：由于手机与客户绑定比较紧密，短信密码生成与 使用场景是物理隔绝的，因此密码在通路上被截取几率降至最低；
- **普及性**：只要会接收短信即可使用，大大降低短信密码技术的使用门槛，学习成本几乎为0，所以在市场接受度上面不会存在阻力；
- **易收费**：由于移动互联网用户天然养成了付费的习惯，这和PC时代互联网截然不同的理念，而且收费通道非常的 发达，如果是网银、第三方支付、电子商务可将短信密码作为一项增值业务，每月通过SP收费不会有阻力，因此也可增加收益；
- **易维护**：由于短信网关技术非常成熟，大大降低短信密码系统上马的复杂度和风险，短信密码业务后期客服成本低，稳定的系统在提升安全同时也营造良好的口碑效应.

基于生物特征的身份认证

- ✓ 概述
- 基于指纹的身份认证
- 基于视网膜的身份认证
- 基于语音的身份认证

基于生物特征的身份认证

- 目前用于身份验证的特征主要有两类：
  - 非生物特征是指用户所知道的东西（如口令、个人密码等）及所拥有的东西（如智能卡、身份证、护照、密钥盘等）；
  - 生物特征是指人体本身所固有的物理特征（如指纹、掌纹、虹膜、视网膜等）及行为特征（如语音、签名等）；
- 非生物特征虽然简单却不可靠，个人所知道的内容想获得非法访问权限的人也可能知道，如口令可能被忘记或被猜测，甚至被窃取，这是基于非生物特征认证方法的缺点；

基于生物特征的身份认证（续）

- 基于生物认证的方式是以人体唯一的、可靠的、稳定的生物特征为依据，采用计算机的强大计算功能和网络技术进行图像处理和模式识别；
- 由于基于生物特征的身份认证主要是通过生物传感器、光学、声学、计算机科学和统计学原理等；高科技手段的密切结合来实现的，在验证方式上无疑是一个质的飞跃；
- 与传统的身份认证方法相比有如下优点：
  - 更具安全性(生物特征基本不存在丢失、遗忘或被盗的问题)；
  - 更具保密性(用于身份认证的生物特征技术很难被伪造)
  - 更具方便性(生物特征具有随身“携带”的特点以及随时随地可用的特点)；

基于生物特征的身份认证（续）

- 理想上，一种好的生物认证特征应具有下列条件：
  - 普遍性，即每个人皆具有的特征；
  - 唯一性，即没有任何二人具有完全相同的特征；
  - 恒久性，即此特征必须持久且不能改变；
  - 可测量性，即这种特征必须能被测量成可定量描述的数据指标；
- 在设计实用的生物认证系统时，还有许多方面需要纳入考量，如
  - 效能，即认证的速度以及结果的可靠度；
  - 接受度，即民众是否愿意接受并使用此系统；
  - 闪避容易度，即是否容易用其他手段来愚弄或欺骗这套系统；

基于生物特征的身份认证（续）

- 目前有七种生物认证技术已被广泛的使用或正在进行大规模的实验评估，他们分别是脸形、人脸热感应、指纹、掌形、视网膜、眼球虹膜和语音识别；
- 目前，利用生物特征验证的操作结果还不是很精确，无法做到很精确的原因在于对人的解剖学和生物学特征的测量存在误差。事实上，用于生物识别的设备需要在拒绝正确的用户（错误类型一）和允许假冒的用户（错误类型二）之间进行折衷调整；
- 在众多的认证方式中，生物特征认证方式前景十分广阔；

各种生物认证的比较

技术	描述	开销	误识别率
视网膜识别	通过扫描视网膜识别	较大	1/10，000，000
虹膜识别	通过扫描虹膜识别	大	1/13100
指纹识别	通过扫描指纹识别	一般	1/500
手形识别	通过3个照相机从不同角度扫描手形	一般	1/500
声纹识别	通过读取预定义的短语的声音识别	小	1/50
签名识别	通过一种特殊的笔在数字化的面板上的签名识别	小	1/50

基于生物特征的身份认证

- 概述
- ✓ 基于指纹的身份认证
- 基于视网膜的身份认证
- 基于语音的身份认证

基于指纹的身份认证

- 指纹是一种由手指皮肤表层的隆起脊线和低洼细沟所构成的纹理，而指纹影像看起来就像一种由许多图形线条依照某种特殊排列方式所组合而成的影像

民间对指纹特别看重

- 一螺穷
- 二螺富
- 三螺四螺开当铺
- 五螺六螺骑花马
- 七螺八螺种庄稼
- 九螺十螺大叫花

民间谚语，各地不同

指纹识别技术

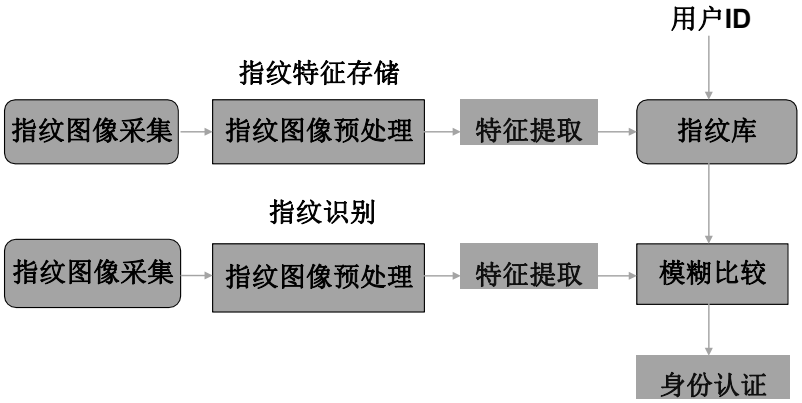
- 指纹识别技术就是通过分析指纹的全局特征和指纹的局部特征来确定身份，特征点如嵴、谷和终点、分叉点或分歧点，从指纹中抽取的特征值非常的详尽，足以可靠地通过指纹来确认一个人的身份；

指纹识别系统原理

- 指纹识别技术主要涉及指纹图像采集、指纹图像预处理、指纹特征提取、指纹特征入库、特征值的比对和匹配等过程
  - 通过指纹读取设备读取到人体指纹图像，并对原始图像进行初步的处理，使之更清晰；
  - 指纹辨识算法建立指纹的数字表示——特征数据，这是一种单方向的转换，可以从指纹转换成特征数据但不能从特征数据转换成指纹，而且两枚不同的指纹产生不同的特征数据。特征文件存储从指纹上找到被称为“细节点”的数据点，也就是那些指纹纹路的分叉点或末梢点。这些数据通常称为模板；

    通过计算机把两个指纹的模板进行比较，计算出它们的相似程度，得到两个指纹的匹配结果；

指纹识别系统工作过程



指纹注册

- 注册(Enrolment) 获取指纹的参考模板；
- 注册失败 (FTR, Failure-to-enrol)：并不是每个人都有可用的指纹；
- 为了更准确，需要收集好几个模板，可能要收集不同手指的指纹；
- 用户指纹模板存储在安全数据库中；
- 在用户登录时，再次读取用户指纹，并将该指纹同存储的模板进行比较；

采用生物技术有以下两个目的

身份识别：1:n比较，试图从数据库中的n个人中找出用户；

验证：1:1比较，对一个给定用户，检查是否存在匹配；

基于口令的认证，能够明确地拒绝或接受用户认证

在生物测定中，存储的参考模板几乎从来都不能精确匹配实际测量的模板；

采用生物技术有以下两个目的

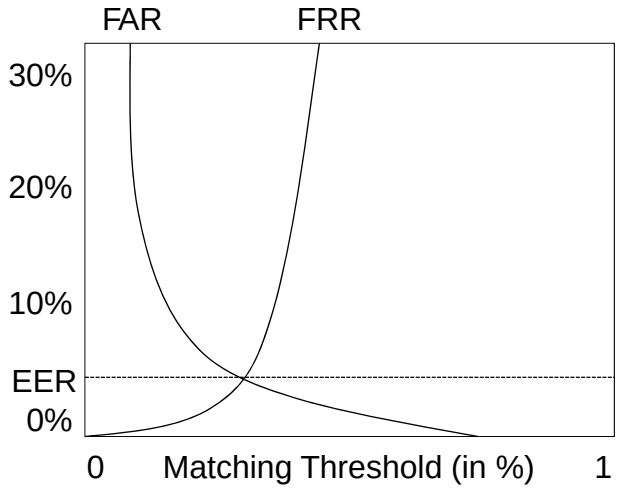
需要一个计算参考模板和当前模板之间相似值的匹配算法；

如果相似值超过了预先定义的阈值，就接受用户必须面对一个新的问题，就是假阳性（假肯定，**false positives**，误报）和假阴性（假否 定，**false negatives**，漏报）

错误地接受一个用户（假肯定）显然是一个安全问题，而拒绝一个合法用户（假否定）则会造成 尴尬的及低效的工作环境；

- **通过设置匹配算法的阈值，可以交换错误接受率(false acceptance rate, FAR)和错误拒绝率(false rejection rate, FRR)**
- 在FAR和FRR之间找到合理的平衡，而这 种平衡依赖于具体应用；
- 如果FAR和FRR相等，那么阈值为同等错误率(equal error rate, EER)
  - 目前，最先进的指纹识别系统的ERR为1%~2%
  - 虹膜模式识别性能更加优越；

FAR, FRR, EER



- **注册失败率(failure to enroll rate, FER) 指系统无法注册用户的频率**
  - 伪造的指纹。指纹以及一般意义上的生理特征或许是唯一的，但绝不是秘密；
    - 许多地方可能留有你的指纹；
  - 用户会接受生物认证技术吗？
    - 提取指纹– 感觉像罪犯？是否会被他用？
    - 激光扫描视网膜– 会不会伤害视网膜？

基于指纹身份认证系统的应用

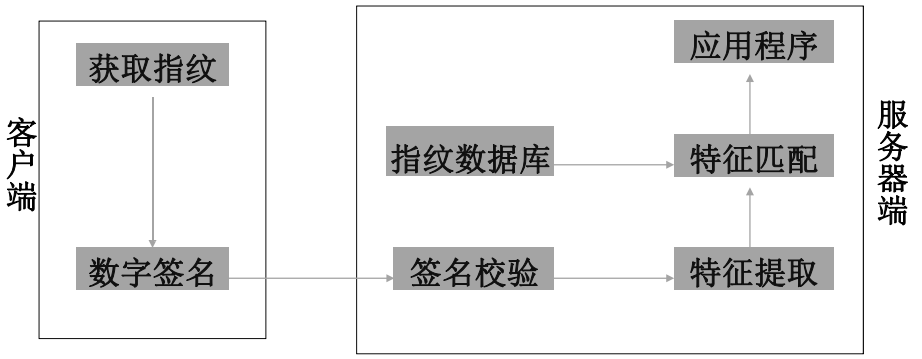
- 指纹识别技术的发展趋于成熟，其应用领域也非常广泛，主要包括：
  - 刑事侦破 门禁系统 、 金融证券
  - 户籍管理 员工考勤

  - 其它方面如计算机及网络，社会保险，移动 通信等等领域。

基于指纹特征的网络认证系统结构

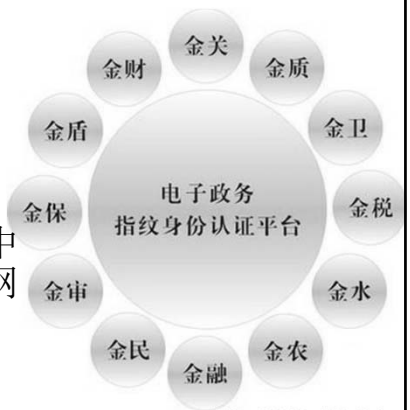
- 用户作为客户端如果要访问远程服务器所管理的信息资源，在获得相关资源访问权限之前，必须通过指纹身份认证
- 为增强系统安全性，在客户端和服务器之间传输的所有数据包括指纹模板、用户的访问请求、服务器的反馈信息都经过加密。同时，指纹模板及相关的用户认证、注册信息都保存在一个本地安全数据库中，此数据库只有本地进程能访问，以防用户信息泄漏；
- 在基于指纹的网络身份认证系统中，采用数字签名技术来保证重要信息——指纹特征值不被非法用户所获得；

基于指纹特征的网络认证系统结构



电子政务指纹身份认证解决方案

- 电子政务指纹身份认证平台解决的信任问题包括：可信的身份，即“我是谁”的问题
  - 通过指纹认证平台，提供可信的身份验证服务，解决用户身份是否可信这一安全策略的核心问题。 可信的数据，即数据的安全问题
  - 利用电子政务指纹身份认证平台，我们可以对电子政务中每一项应用如数据库访问、网页访问、文件转发等建立起安全统一的身份识别和认证



指纹识别的优缺点

- **优点**：独一无二；复杂度高；如果想增加可靠性，还可以鉴别更多的手指；读取方法可靠；扫描的速度很快；使用方便；对人体没有任何伤害；价格低廉；
- **缺点**：某些人或某些群体的指纹特征很少，故而很难成像；一般人在使用指纹辨识系统时会有心理障碍而产生排拒现象；占用大量的硬件资源；老年人指纹的识别有障碍；每一次的使用指纹时都会在指纹采集头上留下用户的指纹印痕，而这些指纹痕迹存在被用来复制指纹的可能性；

插曲：国家电子政务“金”字工程

- “金”字工程全部由国家主导，目的是实现电子化政府；
- 目前有金税工程、金财工程、金贸工程、金关工程、金审工程、金卡工程、金农 工程、金水工程、金盾工程、金桥工程、 金旅工程、金智工程和金卫工程；

金税、金财

- 金税工程：“金税工程”始于1994年，是整个 税收管理信息系统工程的总称。
  - 目的在于通过先进的计算机网络技术，实现全国税务机关信息共享，全面加强对税收各税种、各环节的监控和管理 ；
  - 目前运行的金税工程二期于2001年开始运作，主要监控对象是增值税专用发票；
- 金财工程：“金财工程”即 政府财政管理信息系统，简称GFMIS.

  它是在总结我国财政信息化工作实践，借鉴其它国家财政信息化管理先进理念和成功经验的基础上，提出的一套先进信息管理系统，是我国正在实施的电子政务战略工程建设的重要组成部分；

金贸、金关

- 金贸工程：“金贸工程”是电子商务在经贸流 通领域的应用工程，也是我国电子贸易体系建设的一项试点工程；
  - 引导帮助企业运用全新的观念和方式进行运作，给每一个企业提供一个用先进的信息技术手段进行平等贸易竞争的环境；
- 金关工程：“金关工程”是以推动海关报关业 务的电子化，取代传统的报关方式以节省单据传送的时间和成本为目的应用系统工程。2001年“金关”工程正式启动；
  - 金关的核心有两块，一是海关内部的通关系统；二是外部口岸电子执法系统；
  - 基于海关内部的联通基础上，由海关总署等12个部委牵头建立电子口岸中心；

数据安全

福州大学 FUZHOU UNIVERSITY

金审、金卡

- 金审工程：“金审工程”是审计信息化系统建 设项目的简称，是《国家信息化领导小组关于我国电子政务建设指导意见》中确定的12个重点业务系统之一；
  - 2002年7月28日，国家计委批准审计署开工申请，并下达2002年中央预算内基建投资5000万元，专项用于审计信息化系统一期工程建设；
- 金卡工程：“金卡工程”是以发展我国电子货币为目的、以电子货币应用为重点的各类卡基应用系统工程；
  - 金卡工程广义是金融电子化工程，狭义上是电子货币工程。它是我国的一项跨系统、跨地区、跨世纪的社会系统工程；
  - 它以计算机、通信等现代科技为基础，以银行卡等为介质，通过计算机网络系统，以电子信息转帐形式实现货币流通；

数据安全

福州大学 FUZHOU UNIVERSITY

金农、金水

- 金农工程：金农工程是1994年12月在“国家经济信息化联席会议”第三次会议上提出的，目的是加速和推进农业和农村信息化，建立“农业综合管理和服务信息系统”；
- 金水工程：“金水工程”又称“ 国家防汛指挥系统工程”
  - 计划用五年左右时间，搭建一个先进、实用、高效、可靠并且具有国际先进水平的国家防汛抗旱指挥系统；
  - 金水系统将覆盖7大江河重点防洪地区和易旱地区，能为各级防汛抗旱部门及时、准确地提供各类防汛 抗旱信息，并能较准确地作出降雨、洪水和旱情的预测报告，为防洪抗旱调度决策和指挥抢险救灾提 供有力的技术支持和科学依据；

金盾、金桥

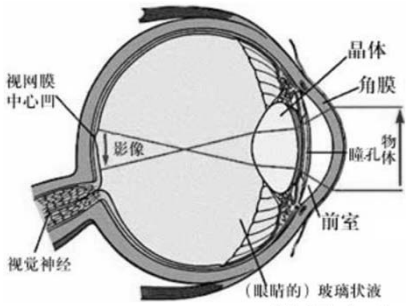
- 金盾工程：“金盾工程” 实质上就是公安通信网络与计算机信息系统建设工程；
  - 增强公安机关快速反应、协同作战的能力；提高公安机关的工作效率和侦察破案水平，适应新形式下社会治安的动态管理；
  - 目的是实现以全国犯罪信息中心（CCIC）为核心，以各项公安业务应用为基础的信息共享和综合利用，为各项公安工作提供强有力的信息支持；
- 金桥工程：金桥工程是以建设我国重要的信息化基础设施为目的的跨世纪重大工程；
  - 国家公用经济信息网工程
  - 活动的主要特征为：中国科协组织实施，发挥科协系统专家群体优势，运用各级学会和各级科协的组织网络体系,动员广大科技工作者积极参与、有关政府部门支持的公益性科技服务实践活动；
  - 项目实施的主要特征为：面向基层，面向企业，面向农村，以项目为核心，以架桥为手段，以转化为目的，多学科、多领域、多层面广泛深入地进行“金桥工程”项目的实施；

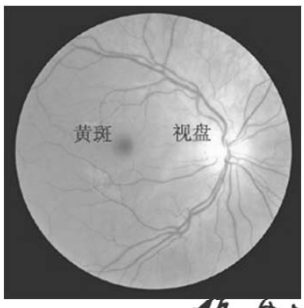
基于生物特征的身份认证

- 概述
- 基于指纹的身份认证
- ✓ 基于视网膜的身份认证
- 基于语音的身份认证

视网膜

- 人类视网膜上分布着许多大大小小的血管，绝无二者的眼底血管图完全相同，即使是同一个人的左眼与右眼也相差甚远。因此，视网膜影像可以被当作一种重要的生物认证特征，用于身份认证；





视网膜识别技术

- 视网膜识别技术是利用激光照射眼球的背面的。在拍摄视网膜时，受拍摄者需要将眼睛贴近一个圆形孔状的小孔，注视孔内所出现的小白点，此时会有微弱的红外光线打在视网膜上，使得视网膜能够清楚的成像。扫描摄取几百个视网膜的特征点，经数字化处理后形成记忆模板存储于数据库中，供以后对比验证时使用；

基于视网膜的身份认证

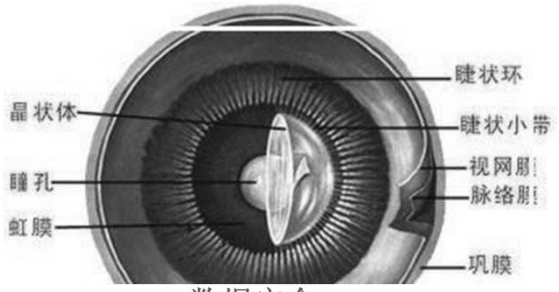
- 视网膜身份认证技术是利用视网膜终身不变性和差异性的特点来识别身份的；
- 视网膜技术与相应的算法结合，可以达到非常优异的准确度，即使全人类的视网膜信息都录入到一个数据中，出现认假和拒假的可能性也相当的小，但这项技术的无法录入问题已经成为它同其他技术抗衡的最大障碍。但是，视网膜识别技术的高精度使它能够在众多的识别技术中占有一席之地；

视网膜识别的优缺点

- **优点：**极其稳定的生物特征，不可能受到磨损、老化或是为疾病影响，精确度较高；视网膜图形具有良好的区分能力；不容易被改变、复制或伪造；
- **缺点：**扫描视网膜影像时需要使用者高度的配合，而且一般的民众会担心长期使用红外光线会影响视网膜的功能，因此这种认证技术至今还没有广泛的应用于日常生活；视网膜认证系统所需要的花销很大，而且也很难进一步降低他的成本，对于一般消费者吸引力不大；视网膜识别技术使用起来比较困难，不适用于直接数字签名和网络传输；

视网膜 vs. 虹膜

- 虹膜是一种在眼睛中瞳孔内的织物状各色环状物，每一 个虹膜都包含一个独一无二的基于像冠、水晶体、细丝、斑点、结构、凹点、射线、皱纹和条纹等特征的结构；
- 视网膜也是一种用于生物识别的特征，有人甚至认为视网膜是比虹膜更唯一的生物特征，视网膜识别技术要求激光照射眼球的背面以获得视网膜特征的唯一性；



基于生物特征的身份认证

- 概述
- 基于指纹的身份认证
- 基于视网膜的身份认证
- ✓ 基于语音的身份认证

基于语音的身份认证

- 语音身份认证技术是一种基于行为特征的识别技术，这是它与视网膜、指纹识别技术本质上的不同之处；
- 它是用声音录入设备反复不断地测量、记录声音波形变化，进行频谱分析，经数字化处理之后做成声音模板加以存储。语音识别实际上就是声纹识别；
- 声纹是指借助一定的仪器描绘出来的人说话声音的图像，即人的声音的频谱图。任何两个人的声纹频谱图都有差异，而对于每个人而言， 就可以通过声纹鉴别进行个人身份识别
- 语音身份认证，就是通过对所记录的语音与被鉴人声纹的比较,进行身份认证；

语音识别系统原理

- 语音识别是一项根据语音波形中反映说话人生理和行为特征的语音参数，自动识别说话人身份的技术；
- 基本原理是通过分析言者的发声和听觉,为每个人构造一个独一无二的数学模型,由计算机对模型和实际输入的语音进行精确匹配,根据匹配结果辨认出说话人是谁；
- 语音识别的步骤是：首先对鉴别对象的声音进行采样，即输入语音信号，然后对采样数据进行滤波等处理，再进行特征提取和模式匹配；
- 在声纹的鉴别过程中最主要的两部分内容就是**特征提取**和**模式匹配**。
  - **特征提取**，就是从声音中选取唯一表现说话人身份的有效且稳定可靠的特征；
  - **模式匹配**，就是对训练和鉴别时的特征模式做相似性匹配。

声纹身份认证基本方法

- 概率统计方法：语音中说话人信息在短时内较为平稳，通过对稳态特征如基音、低阶反射系数、声门增益等的统计分析,可以利用均值、方差等统计量和概率密度函数进行分类判决；
- 动态时间规整方法：说话人信息不仅有稳定因素（发声器官的结构和发声习惯）,而且有时变因素（语速、语调、重音和韵律）。将识别模板与参考模板进行时间对比,按照某种距离测定得出两模板间的相似程度；
- 矢量量化方法：它最早是基于聚类分析的数据压缩编码技术。Helms 首次将其用于声纹识别,把每个人的特定文本编成码本,识别时将测试文本按此码本进行编码,以量化产生的失真度作为判决标准；

声纹身份认证基本方法（续）

- 长时平均法：该方法对说话人身份的表征是通过将语音特征在长时间上进行平均来实现。这种方法缺乏对短时特征的描述；
- 人工神经网络方法：它在某种程度上模拟了生物的感知特性，是一种分布式并行处理结构的网络模型，具有自组织和自学习能力、很强的复杂分类边界区分能力，其性能近似理想的分类器。其缺点是训练时间长，动态时间规整能力弱，网络规模随说话人数目增加时可能大到难以训练的程度；

声纹身份认证基本方法（续）

- 隐马尔可夫模型方法（HMM）：它是一种基于转移概率和传输概率的随机模型，它把语音看成由可观察到的符号序列组成的随机过程，符号序列则是发声系统状态序列的输出。在使用HMM 识别时，为每个说话人建立发声模型，通过训练得到状态转移概率矩阵和符号输出概率矩阵。识别时计算未知语音在状态转移过程中的最大概率，根据最大概率对应的模型进行判决；
- 高斯混和模型：高斯混和模型可被认为是隐含马尔可夫模型的单一状态的特殊情形，对于与文本无关的身份认 ； 证，该方法能够达到很好的效果；

基于声纹身份认证的应用（续）

- **军事和国防**：基于声纹的身份认证技术可以察觉电话交谈过程中是否有关键说话人出现，继而对交谈的内容进行跟踪(战场环境监听)；在通过电话发出军事指令时，可以对发出命令的人的身份进行确认；
- **保安和证件防伪**：如机密场所的门禁系统；

基于声纹身份认证的应用

- **信息领域**：如在自动总机系统中；
- **银行、证券系统**：鉴于密码的安全性不高，可用声纹识别技术对电话银行、远程证券交易等业务中的用户身份进行确认；
- **公安司法**：对于各种电话勒索、绑架、电话人身攻击等案件，基于声纹的身份认证技术可以在一段录音中查找出嫌疑人或缩小侦察范围；也可以在法庭上提供身份确认的旁证；

语音应用大行其道

福州大学
FUZHOU UNIVERSITY

本章内容

- 身份认证的概念
- 基于口令的身份认证
- 基于USB Key的身份认证
- 基于生物特征的身份认证
- ✓网络实名制

福州大学
FUZHOU UNIVERSITY

网络实名制

- 实体身份认证
  - 数字身份 ←→ 实体身份
- 对于身份认证，不仅从技术上，还可以从管理和政策方面着手；

网络实名制的源头

- 李希光事件
  - 2002年清华大学新闻学教授李希光在南方谈及新闻改革时提出建议 “ 中国人大应该禁止任何人网上匿名” ；
  - 之后李希光自己也称已经对网络实名的话题丧失了兴趣， “ 禁止网上匿名是非常不现实的，在法律上和技术上都行不通” ；

网络实名制的基础

- VIEID (Virtual identity electronic identification)
  即俗称的网络身份证，VIEID的普 及是互联网
- 实名制的根本前提；

  VIEID是互联网络信息世界中标识用户身份的工具，用于在网络通讯中识别通讯各 方的身份及表明我们的身份或某种资格；

网络身份证

- 2011年1月7日，美国商务部部长骆家辉在斯坦福大学 经济政策研究院表示，美政府将通过推出网络身份证，构建一个网络生态系统。近期，在美国总统奥巴马的推动下，作为国家网络安全战略重要组成部分，美国商务部将启动网络身份证战略；
- 奥巴马提出的网络身份证国家战略，也称“网络空间可信身份标识国家战略”（NSTIC）。自互联网问世以来，由于网络空间存在的虚拟性和自由性，它在提供极度自由性的同时，也使得网络诚信存在巨大漏洞。在网络空间，全球一直没有可靠、公认和通用的身份识别技术；

  由于没有真实可靠的身份认证，互联网本身应有的巨大社会和经济价值难以全部得到发挥，黑客入侵和网络欺诈屡见不鲜；

发展进程

- 2003：网吧实名制
- 2004：高校BBS实名制，电子邮箱实名制；
- 2005：网站通过IDC或ISP来备案登记QQ群创建者和管理员实名制；
- 2006：博客实名制
- 2010：手机实名制
- 2011：微博实名制
- 2012：火车票实名制

网络实名制的争议

- 实名制是社会交往和社会活动的基础，是网络环境下整体社会诚信体系建立的必要条件
- 实名制 VS. 隐私保护；
- **网络实名制**：实际操作太困难；

韩国“网络实名制”失败

- 2005年9月，在大型门户网站实行有限实名制，减少以匿名进行诽谤等副作用；
- 2007年7月，正式开始实施实名制；
- 2011年7月，韩国一著名门户网站和一社交网站被黑客攻击，约3500万名网民（韩国2010年的总人口为4800余万）的个人信息外泄；
- 2012年8月24日，韩国宪法法院废除2007年生效的网络实名制法案， 8位法官一致裁决认为网络实名制破坏了言论自由；

小结

- 了解基于口令/USB Key/生物特征的认证
- 常见的口令威胁方式
  - 口令猜测
  - 口令欺骗
  - 口令文件泄露
- 提高安全意识
  - 讲起来都知道，但有时就会不知不觉犯同样的错误

谢谢大家，一起交流学习！

QQ: 10068 0 2383