第三章
身份认证与访问控制

第三章　身份认证与访问控制

3.1 身份标识与鉴别

身份标识与鉴别服务的目的

- 保证消息的可靠性

实现身份认证的主要方法

- 口令
- 数字证书
- 基于生物特征（如指纹、声音、虹膜、视网膜等）的认证。

3.1.1 身份标识与鉴别概念

- 身份标识就是能够证明用户身份的用户独有的生物特征或行为特征，此特征要求具有唯一性，如用户的指纹、视网膜等生物特征及声音、笔迹、签名等行为特征；或他所能提供的用于识别自己身份的信息，如口令、密码等。
- 相比较而言，后一种的安全系数较低，密码容易被遗忘或被窃取，身份可能会被冒充。

3.1.1 身份标识与鉴别概念（续）

鉴别服务

对网络中的主体进行验证的过程

对等实体鉴别服务

用于两个开放系统同等层中的实体建立连接或数据传输阶段，对对方实体的合法性、真实性进行确认。这里的实体可以是用户或进程

数据源认证服务

用于确保数据发自真正的源点，防止假冒。认证或鉴别的过程是为了限制非法用户的访问权限，防止其非法访问网络资源，提高网络信息的安全性。它是其他一切安全机制的基础

3.1.2 身份认证的过程

基于物理安全性的身份认证

基于行为特征的身份认证

基于信息秘密的身份认证

利用数字签名的方法实现身份认证

身份认证的过程根据身份认证方法的不同而不同

基于信息秘密的身份认证过程

基于信息秘密的身份认证一般是指依赖于所拥有的东西或信息进行验证

- 口令认证
- 单向认证
- 双向认证

口令认证：也属于单向认证

- 口令认证是鉴别用户身份最常见也是最简单的方法。
- 系统为每一个合法用户建立一个用户名并设置相应的口令。
- 当用户登录系统或使用某项功能时，提示用户输入自己的用户名和口令。
- 系统核对用户输入的用户名、口令与系统内已有的合法用户的用户名和口令对是否匹配。
- 如果匹配，则该用户的身份得到了认证，用户便可以登陆或使用所需的某项功能。

口令认证（续）

这种方法有如下缺点：

- 其安全性仅仅基于用户口令的保密性，而用户口令一般较短且容易猜测，因此这种方案不能抵御口令猜测攻击。
- 攻击者可能窃听通信信道或进行网络窥探，口令的明文传输使得攻击者只要能在口令传输过程中获得用户口令，系统就会被攻破。

口令认证（续

多名业内人士告诉南都记者，“WiFi万能钥匙”类App的真

接过的WiFi账号和密码，并上传、存储到App的服务器上

从用

。

对此

作原

能钥

议的

回忆

设置为“自动分享热点”，也就是说，提供WiFi账号和密码

者，而这些被分享的WiFi热点真正的所有者（为之缴网费

App。只要自家的WiFi信号被一台装有此应用的手机成功

一无线网络就向所有“WiFi万能钥匙”的用户免费开放了。

单向认证

通信的双方只需要一方被另一方鉴别身份

- 口令核对法实际也可以算是一种单向认证
- 与密钥分发相结合的单向认证方案
  - 一类采用对称密钥加密体制，需要可信赖的第三方，通常称为KDC或AS（认证服务器），由第三方来实现通信双方的身份认证和密钥分发
  - 另一类采用非对称密钥加密体制，无需第三方参与

双向认证

- 通信的双方需要同时验证对方的身份。
- 在双向认证过程中，通信双方需要互相认证鉴别各自的身份，然后交换会话密钥。
- 双向认证的典型方案是NeedhaD/Schkeder协议。

基于物理安全性的身份认证过程

- 尽管前面提到的身份认证方法在原理上有很多不同，但他们有一个共同的特点，就是只依赖于用户知道的某个秘密的信息。
- 与此对照，另一类身份认证方案是依赖于用户特有的某些生物学信息或用户持有的硬件。

基于智能卡的身份认证机制

- 基于智能卡的身份认证机制在认证时认证方要求一个硬件如智能卡（智能卡中往往存有秘密信息，通常是一个随机数），只有持卡人才能被认证。
- 可以有效的防止口令猜测。
- 严重的缺陷：系统只认卡不认人，而智能卡可能丢失，拾到或窃得智能卡的人很容易假冒原持卡人的身份。
- 综合前面提到的两类方法，即认证方既要求用户输入一个口令，又要求智能卡。

基于生物学信息的身份认证机制

- 基于生物学信息的方案包括基于指纹识别的身份认证以及基于视网膜识别的身份认证等。

采样：生物识别系统捕捉到生物特征的样品，唯一的特征将会被提取并且转化成数字的符号存入此人的特征模板

抽取特征：用户在需要验证身份时，与识别系统进行交互，设备提取用户的生物信息特征

比较：用户的生物信息特征与特征模板中的数据进行比较

匹配：如果匹配，则用户通过身份验证

基于行为特征的身份认证过程

- 基于行为特征的身份认证过程指通过识别行为的特征进行验证。
- 常见的验证模式有语音认证、动作识别、签名等。验证过程遵循模式识别的基本步骤。
- 模式识别的工作原理：首先是构造一个签名鉴别系统，然后进行签名的鉴别。

签名鉴别系统的鉴别过程

用户注册：从签名数据库中调出用户所宣称的人的参考签名

数据获取：通过扫描仪或手写板等设备获得签名数据

预处理：包括去噪声、平滑原始数据等。对于离线签名来说，还要进行图像的二值化、细化或轮廓提取等工作

抽取：从预处理之后的数据中，选择和提取出能够充分反映签名的书写风格与个性，同时又相对稳定的特征

识别：根据从被鉴别签名中抽取出的特征，采用某种模式识别方法与从第一步中得到的参考签名的相应特征进行比较

出鉴别结果，即拒绝或接受

利用数字签名实现身份认证

- 数字签名是通过单向函数对要传送的报文进行处理得到的用以认证报文来源并核实报文是否发生变化的一个字母数字串。数字签名主要有3种应用广泛的方法：RSA签名、DSS签名和Hash签名。
- Hash签名是最主要的数字签名方法：报文的发送方从明文中生成一个128比特的散列值(数字摘要)，发送方用自己的私钥对这个散列值进行加密，形成发送方的数字签名。该数字签名将作为附件和报文一起发送给接收方。报文的接收方从接收到的原始报文中计算出128比特的散列值(数字摘要)，接着用发送方的公钥对报文附加的数字签名解密。

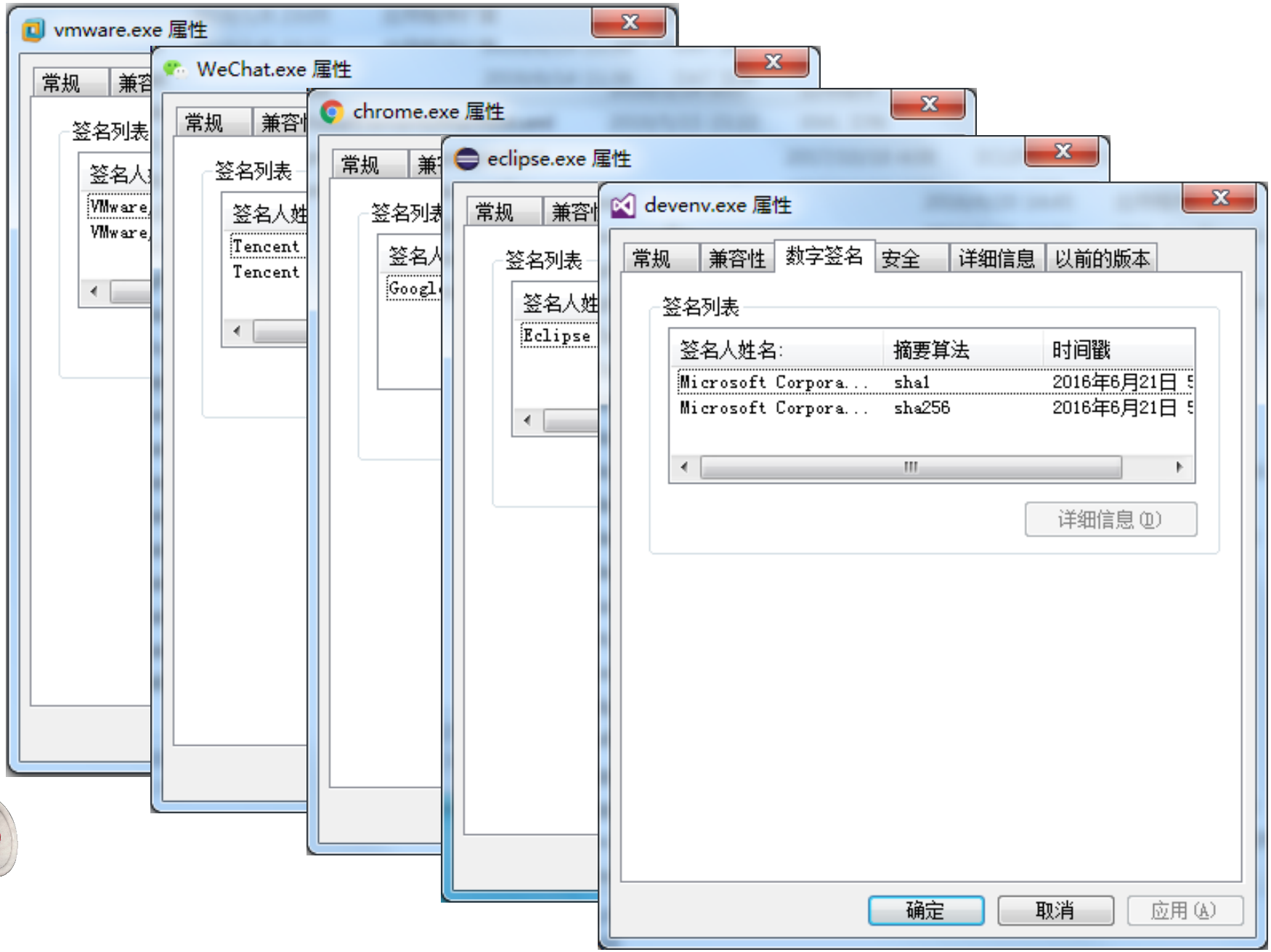
利用数字签名实现身份认证（续）

数字签名可以解决否认、伪造、篡改及冒充等问题。

在安全性问题上，数字签名要求：

发送者事后不能否认发送的报文签名
接收者能够核实发送者发送的报文签名
接收者不能伪造发送者的报文签名
接收者不能对发送者的报文进行部分篡改
网络中的某一用户不能冒充另一用户作为发送者或接收者

利用数字签名实现身份认证（续）



3.2 口令认证方法

- 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。

3.2.1 口令管理

- 口令管理是一个非常重要而且非常费时间的任务。
- 用户不仅试图要创造一个不同的口令，而且要记住他们。
- 系统管理员要花费很多时间来存储用户创造的口令或帮助用户恢复忘记的口令。
- 在保护敏感信息的过程中，许多公司都需要用户提供口令或其他信物才能进入网络资源或应用程序。
- 密码是最简单的口令管理系统，类似个人通讯录，仅仅提供个人登录应用系统，服务器或网络的密码查询维护功能，起到了帮助记忆众多口令的作用。

口令的存储

直接明文存储口令

- 直接明文存储口令是指将所有用户的用户名和口令都直接存储于数据库中，没有经过任何算法或加密过程。
- 这种存储方法风险很大，任何人只要得到了存储口令的数据库，就可以得到全体用户的用户名及口令，冒充用户身份。

口令的存储（续）

哈希散列存储口令

- 哈希散列函数的目的是为文件、报文或其他分组数据产生“指纹”。
- 从加密学的角度讲，好的散列函数H具备如下性质：H的输入可以是任意长度的；H产生定长的输出；对于任何给定的x，H(x)的计算要较为容易；对于任何给定的码h,要寻找x，使得H(x)=h在计算上是不可行的，称为单向性；对于任何给定的分组x,寻找不等于x的y，使得H(x)=H(y)在计算上是不可行的，称为弱抗冲突；寻找任何的（x，y）对，使得H(x)=H(y)在计算上是不可行的，称为强抗冲突。

好的哈希函数的特征
① 任意长度得到定长输出
② 只能单向计算

口令的存储（续）

例如，可以定义一个哈希函数H(x)=[x mod 10]，其中x∈ R,y∈ [0,9]。对于每一个用户，系统存储账号和散列值对在一个口令文件中，当用户登陆时，用户输入口令x，系统计算H(x)，然后与口令文件中的相对应的散列值进行比较，成功则允许用户访问，否则拒绝其登陆。在文件中存储的是口令的散列值而不是口令的明文，优点在于黑客即使得到口令的存储文件，想要通过散列值得到用户的原始口令也是不可能的。这就相对增加了安全性。

常用口令管理策略

- 所有活动账号都必须有口令保护；
- 口令输入时不应将口令的明文显示出来，应该采取掩盖措施，如输入的字符用“*”取代；
- 口令不能以明文形式保存在任何电子介质中；
- 可以在PGP或强度相当的加密措施的保护下将口令存放在电子文件中；
- 口令最好能够同时含有字母和非字母字符；
- 口令不能在工作组中共享，以保证可以通过用户名追查到具体责任人；

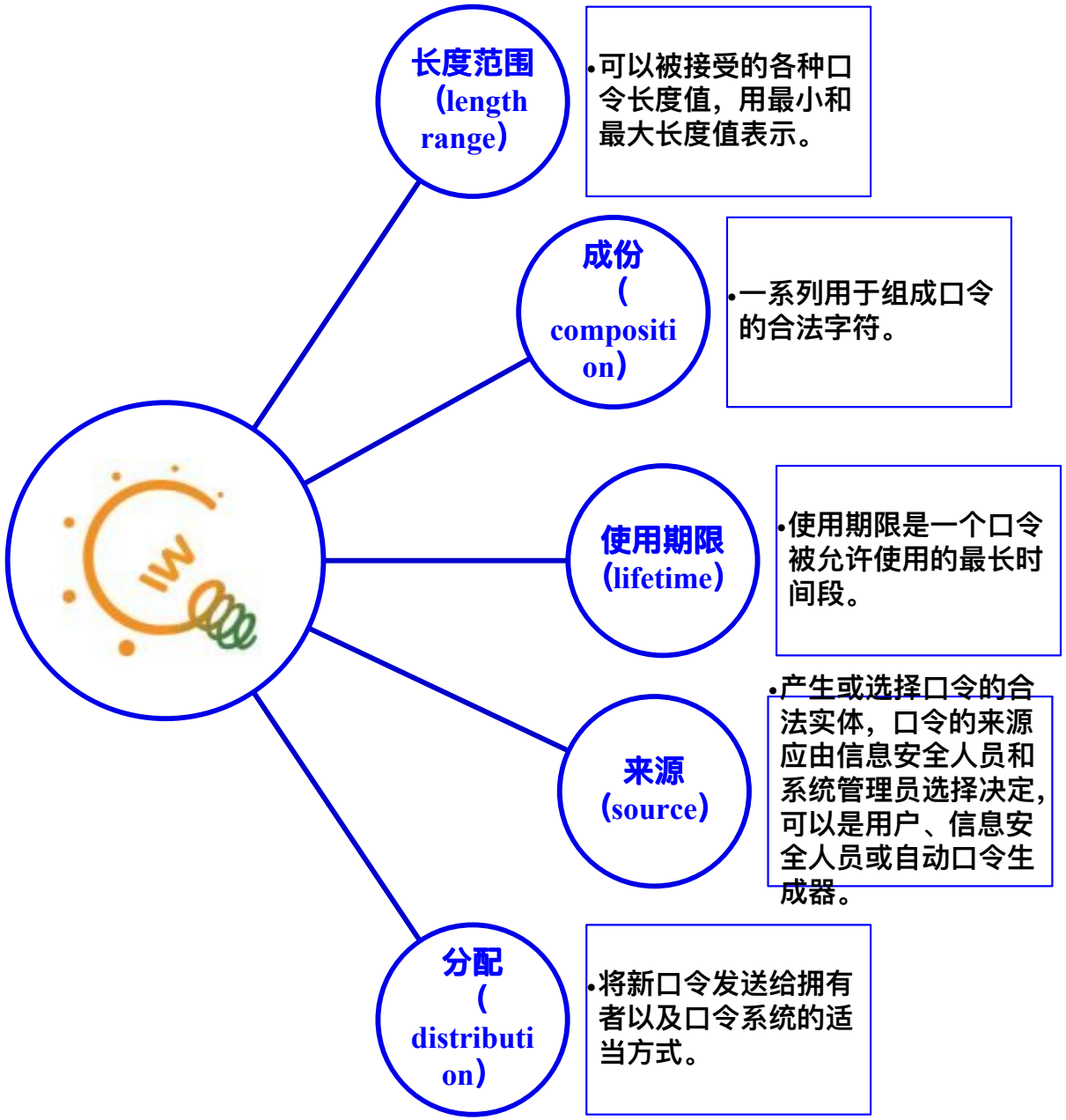
常用口令管理策略（续）

- 口令不能和用户名或登录名相同；
- 口令使用期限和过期失效必须由系统强制执行；
- 口令长度最好能多于8个字符；
- 口令最好不要相同，用户应该在不同的系统中使用不同的口令；
- 当怀疑口令被攻破或泄漏就必须予以更改；
- 用户连续输错3次口令后账号将被锁定，只有系统管理员可以解锁；

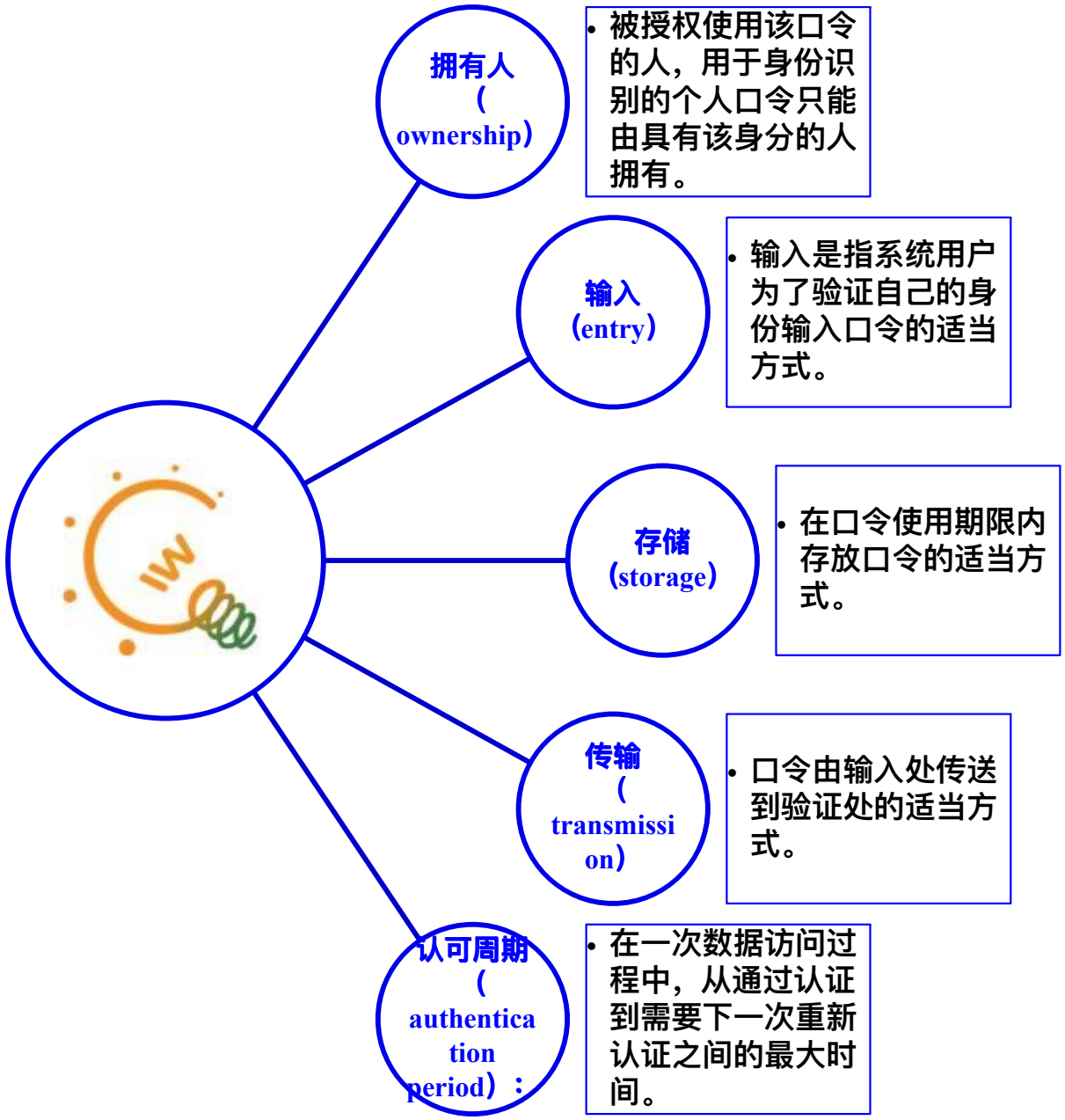
3.2.2 脆弱性口令

- 跟踪系统的登陆过程，发现口令的计算是非常脆弱的。
- 口令的脆弱性一般体现在两个方面：登陆时候的口令加密算法的脆弱和数据库存储的口令加密算法的脆弱。
- 因此在设计口令时要考虑到影响口令的因素。

影响口令的因素


长度范围（length range）
可以被接受的各种口令长度值，用最小和最大长度值表示。
成份（composition）
一系列用于组成口令的合法字符。
使用期限（lifetime）
使用期限是一个口令被允许使用的最长时间段。
来源（source）
产生或选择口令的合法实体，口令的来源应由信息安全人员和系统管理员选择决定，可以是用户、信息安全人员或自动口令生成器。
分配（distribution）
将新口令发送给拥有者以及口令系统的适当方式。

影响口令的因素（续）


拥有人（ownership）
被授权使用该口令的人，用于身份识别的个人口令只能由具有该身分的人拥有。
输入（entry）
输入是指系统用户为了验证自己的身份输入口令的适当方式。
存储（storage）
在口令使用期限内存放口令的适当方式。
传输（transmission）
口令由输入处传送到验证处的适当方式。
认可周期（authentication period）：
在一次数据访问过程中，从通过认证到需要下一次重新认证之间的最大时间。

口令的明显缺点

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。

口令的明显缺点（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。

口令的明显缺点（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。

3.3 生物身份认证

目前用于身份验证的特征主要有两类：非生物特征和生物特征。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。

3.3 生物身份认证 （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)。

3.3 生物身份认证 （续）

- 理想上，一种好的生物认证特征应具有下列条件：（1）普遍性，即每个人皆具有的特征；（2）唯一性，即没有任何二人具有完全相同的特征；（3）恒久性，即此特征必须持久且不能改变；（4）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（1）效能，即认证的速度以及结果的可靠度；（2）接受度，即民众是否愿意接受并使用此系统；（3）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。

3.3 生物身份认证 (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，利用某些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。

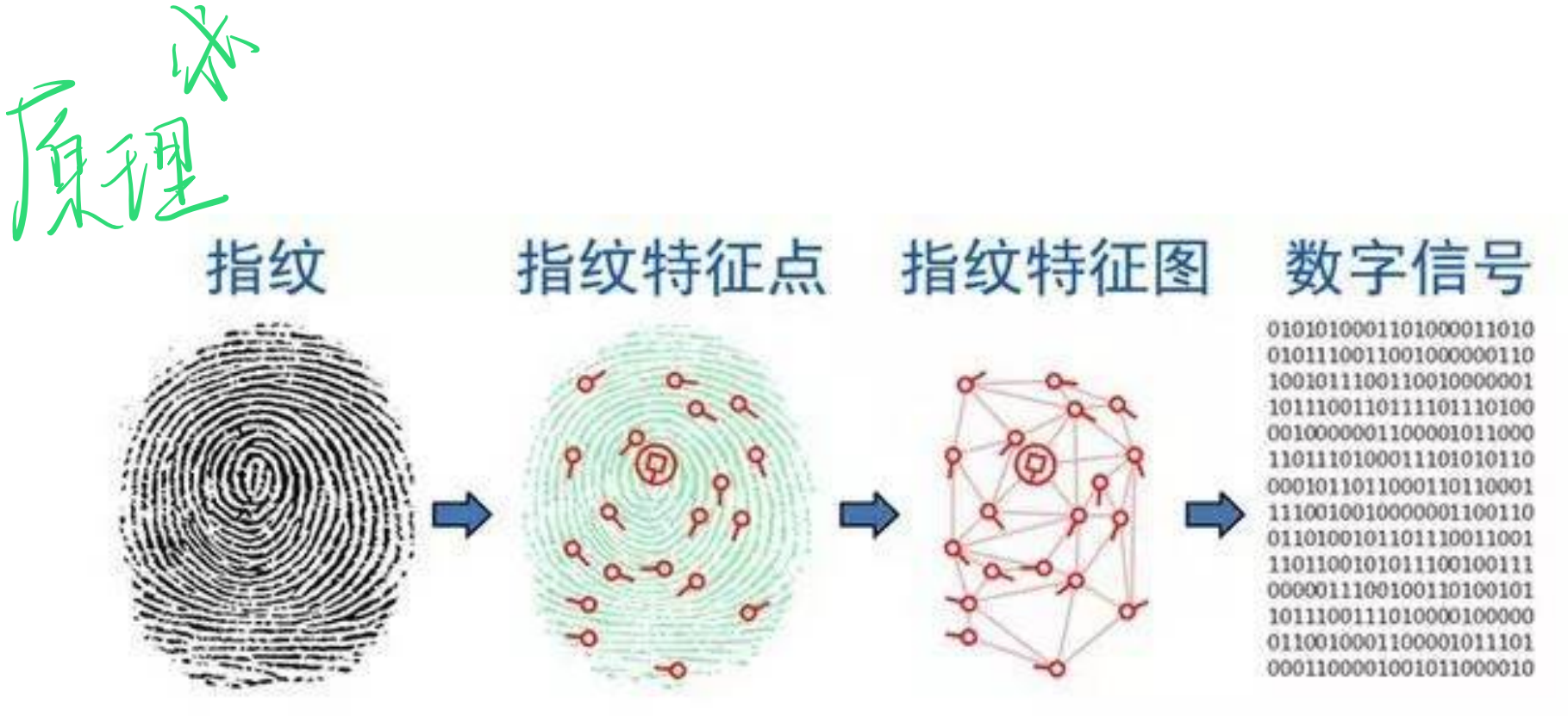
3.3.1 指纹身份认证技术

- **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。
- **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（续）

欧洲

指纹识别系统原理（续）


指纹
指纹特征点
指纹特征图
数字信号
01010100011010000011010
01011100110010000000110
10010111001100100000001
10111001101111101110100
00100000011000001011000
11011101000111010101110
00010110110001101100001
11100100100000011001110
01101001011011100110001
11011001010111001001111
00000111001001101001010
10111001110100001000000
01100100011000010111010
00011000010010110000010

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


用户ID
指纹特征存储
指纹图像采集
指纹图像预处理
特征提取
指纹库
指纹识别
指纹图像采集
指纹图像预处理
特征提取
模糊比较
身份认证

指纹识别系统原理（续）

- 指纹的特征

  人的指纹有两类特征:全局特征和局部特征。

- 指纹取像

  将一个人的指纹采集下来输入计算机进行处理的过程称为指纹取像，它是指纹自动识别的首要步骤。

- 图像的预处理

  无论采取哪种方法提取指纹,总会给指纹图像带来各种噪声。预处理的目的就是去除图像中的噪声,把它变成一幅清晰的点线图,以便于提取正确的指纹特征。

指纹识别系统原理（续）

- 指纹细节特征的提取

  指纹特征的提取采用链码搜索法对指纹纹线进行搜索,提取出各种特征及其特征的坐标位置。

- 指纹特征入库

  指纹特征入库是指将于预处理好的指纹图像以及各种提取出来的指纹信息存入指纹识别系统的指纹库中。

指纹识别系统原理（续）

- 匹配及识别

指纹识别系统的核心步骤是指纹匹配，基本包括如下几类：细节点匹配、脊线匹配以及指纹特征向量匹配等。指纹匹配首先是进行指纹的校准，然后进行匹配点对的计算。应用系统利用指纹识别技术可以分为两类，即验证和辨识 。验证就是通过把一个现场采集到的用户指纹与指纹库中已经登记的相应用户的指纹进行一对一的比对（one-to-one matching），来确认身份的过程。

基于指纹身份认证系统的应用

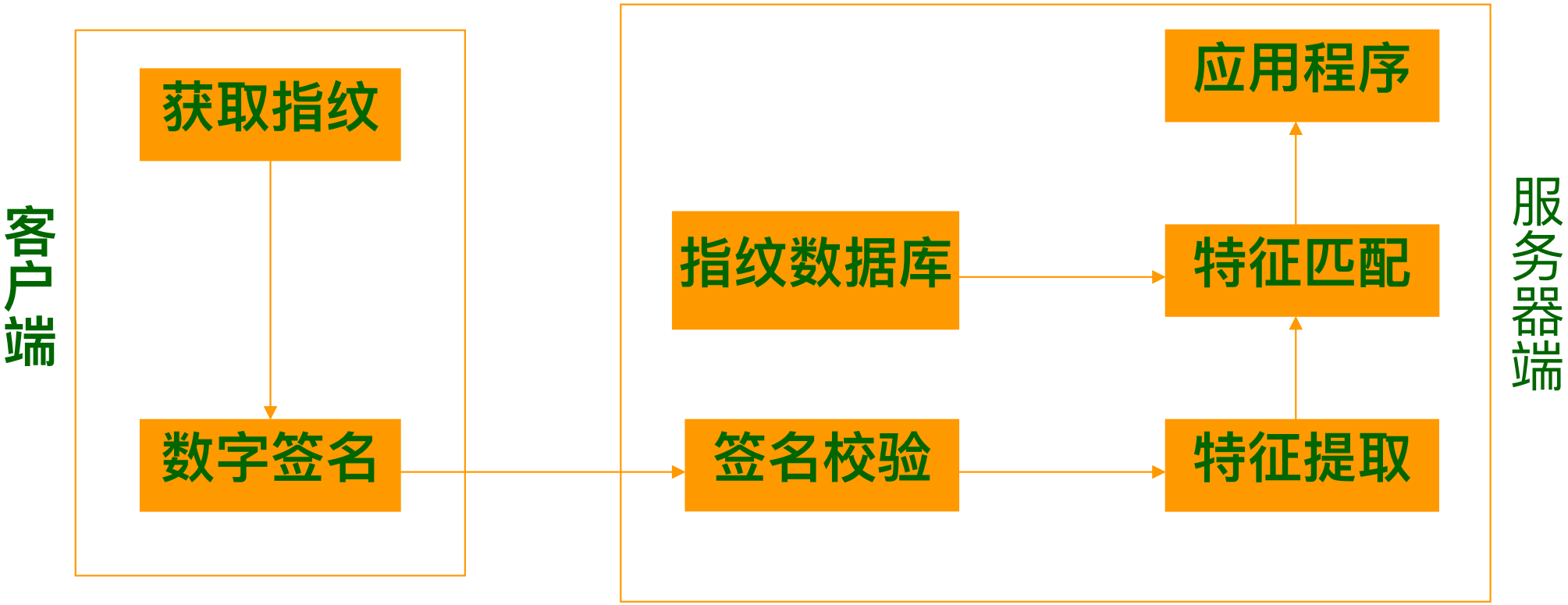
指纹识别技术的发展趋于成熟，其应用领域也非常广泛，主要包括：

- 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。

基于指纹特征的电子商务身份安全认证系统结构

- 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。
- 在基于指纹的电子商务身份认证系统中，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。

基于指纹特征的电子商务身份安全认证系统结构（续）



基于指纹特征的电子商务身份认证系统结构

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。

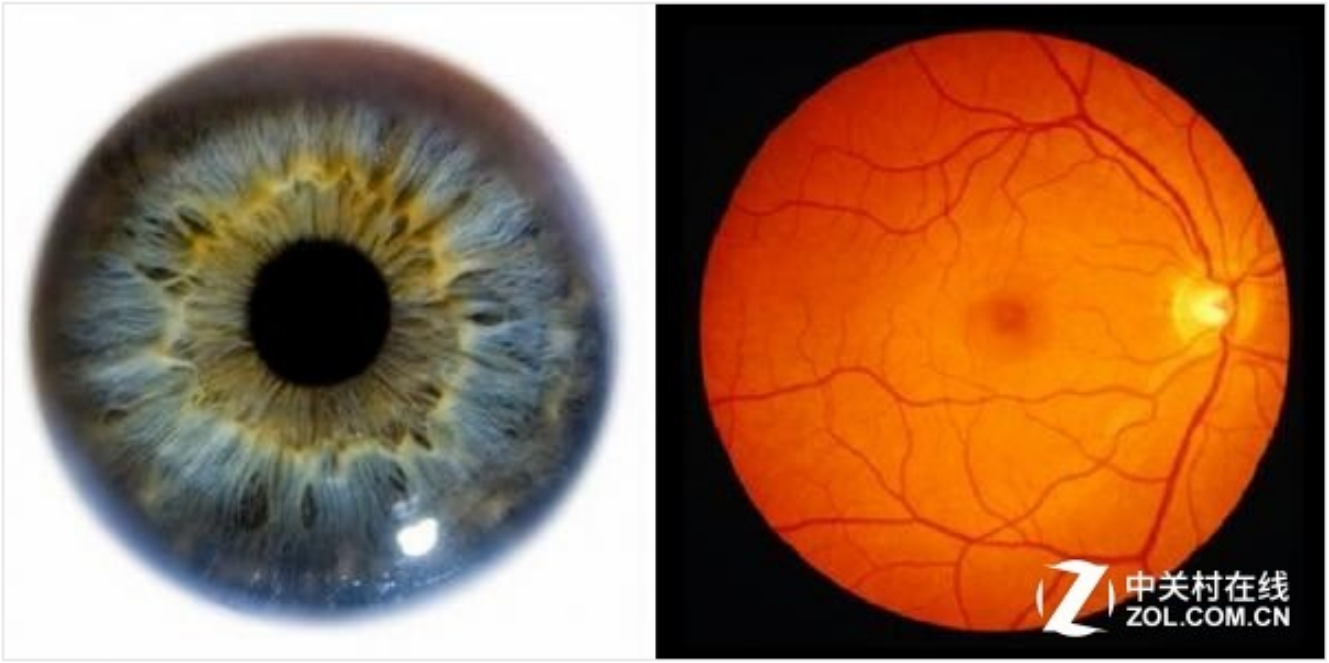
3.3.2 视网膜身份认证技术

- **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。

视网膜特征

- 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。
- 视网膜识别技术是利用激光照射眼球的背面。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。

视网膜特征



左：虹膜识别图像　右：视网膜识别图像

视网膜识别的优缺点

- 优点：极其稳定的生物特征，受到磨损、老化或是为疾病影响概率小，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。

虹膜vs视网膜vs眼纹

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

3.3.3 语音身份认证技术

- 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。
- 语音识别的主要步骤是：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

- 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；
- 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。

3.4 访问控制

先进行身份认证，再进行访问控制

在网络安全环境中，访问控制能够**限制和控制**通过通信链路对主机系统和应用的访问。为了达到这种控制，每个想获得访问的实体都必须经过**鉴别或身份验证**，这样才能根据个体来制定访问权利。访问控制服务用于防止未授权用户非法使用系统资源。它包括**用户身份认证，也包括用户的权限确认**。这种保护服务可提供给用户组。

3.4.1 访问控制概念

- 访问控制是通过某种途径显式地准许或限制访问能力及范围的一种方法。通过限制对关键资源的访问，防止非法用户的侵入或因为合法用户的不慎操作而造成的破坏，从而保证网络资源受控地、合法地使用，它是针对越权使用资源的防御措施。
- 访问控制技术是建立在身份认证的基础上的，简单的描述，身份认证解决的是“你是谁，你是否真的是你所声称的身份”，而访问控制技术解决的是“你能做什么，你有什么样的权限”这个问题。

3.4.1 访问控制概念

访问控制系统一般包括以下几个实体：

- **主体（subject）**：发出访问指令、存取要求的主动方，通常可以是用户或用户的某个进程等。
- **客体（object）**：被访问的对象，通常可以是被调用的程序、进程，要存取的数据、信息，要访问的文件、系统或各种网络设备、设施等资源。
- **安全访问策略**：一套规则，用以确定一个主体是否对客体拥有访问能力。

访问控制概念原理

- 访问控制的目的为：限制主体对访问客体的访问权限，从而使计算机系统资源能被在合法范围内使用；决定用户能做什么，也决定代表一定用户利益的程序可以做什么。访问控制机制可以限制对关键资源的访问，防止非法用户进入系统及合法用户对系统资源的非法使用。

访问控制实现方法

较为常见的访问控制的实现方法主要有以下四种：访问控制矩阵、访问能力表、访问控制表和授权关系表。

访问控制的四种实现
1. 访问控制矩阵
2. 访问能力表
3. 访问控制表
4. 授权关系表

访问控制矩阵

从数学角度看，访问控制可以很自然的表示成一个矩阵的形式：行表示客体（各种资源），列表示主体（通常为用户），行和列的交叉点表示某个主体对某个客体的访问权限（比如读、写、执行、修改、删除等）。

访问控制矩阵（续）

有own权限可以将读写权限授权给他人。

	file1	file2	file3	file4	account1	account2
Jack	own r w		own r w		inquiry credit	
Mary	r	own r w	w	r	inquiry debit	inquiry credit
Lily	r w	r		own r w		inquiry debit

访问控制矩阵（续）

上表是一个访问控制矩阵的例子。在这个例子中，Jack、Mary、Lily是三个主体，客体有四个文件（file）和两个账户（account）。从该访问控制矩阵可以看出，Jack是file1、file3的拥有者（own），而且能够对对其进行读（r）、写操作（w），但是Jack对 file2、file4就没有访问权。需要注意的是拥有者的确切含义会因不同的系统而拥有不同的含义，通常一个文件的拥有（own）权限表示可以授予（authorize）或者撤销（revoke）其他用户对该文件的访问控制权限，比如Jack拥有file1的own权限，他就可以授予Mary读或者Lily读、写的权限，也可以撤销给予他们的权限。

访问控制矩阵（续）

对账户的访问权限展示了访问可以被应用程序的抽象操作所控制。查询（inquiry）操作与读操作类似，它只检索数据而并不改动数据。借（debit）操作和贷（credit）操作与写操作类似，要对原始数据进行改动，都会涉及读原先账户平衡信息、改动并重写。实现这两种操作的应用程序需要有对账户数据的读、写权限，而用户并不允许直接对数据进行读写，他们只能通过已经实现借、贷操作的应用程序来间接操作数据。

间接的读写

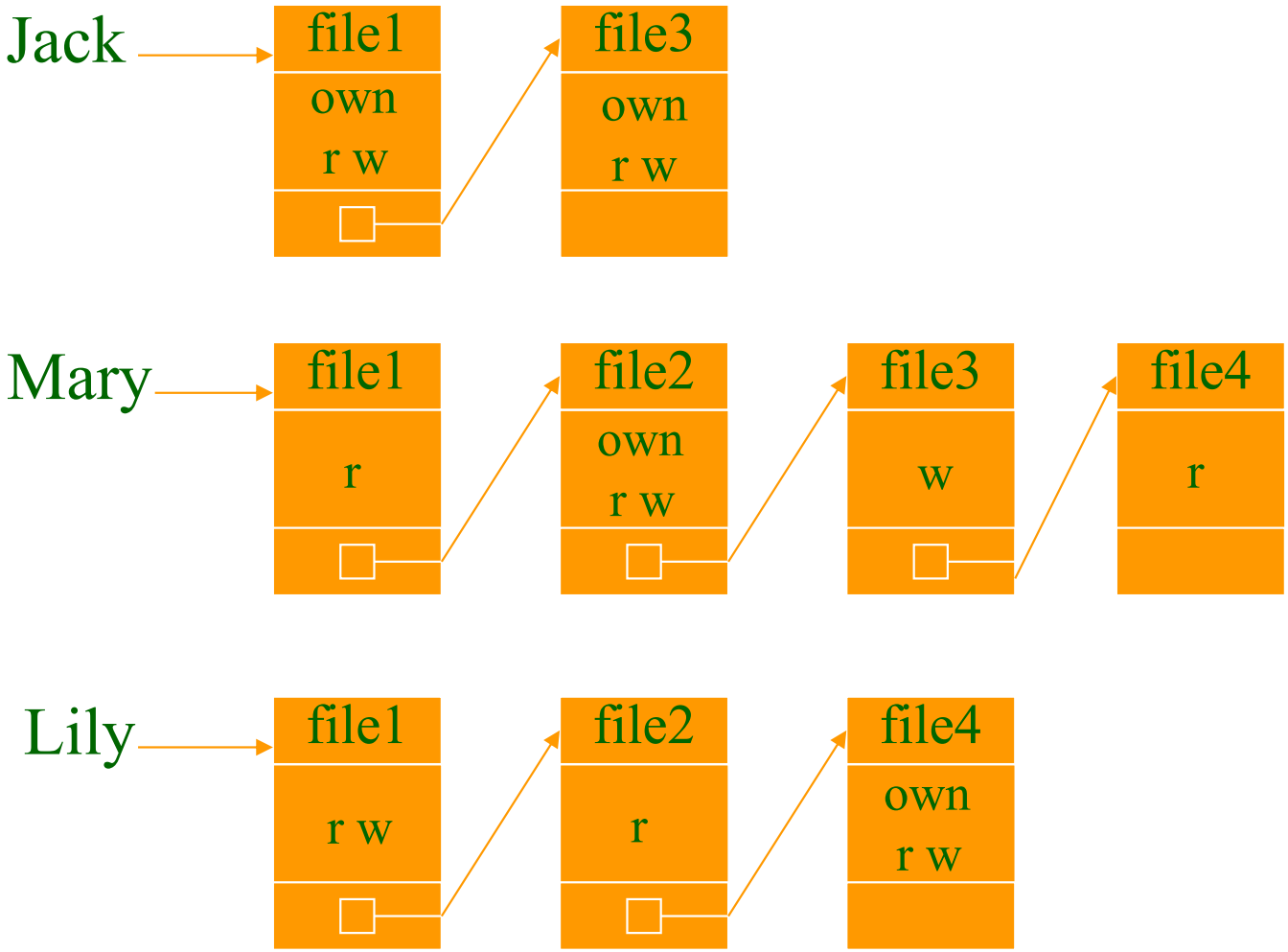
借、贷操作、间接性的读写

访问能力表

解决稀疏矩阵问题

- 实际的系统中虽然可能有很多的主体和客体，但主体和客体之间的关系可能并不多，这样的话就存在着很多的空白项。为了减轻系统开销与浪费，我们可以从主体（行）出发，表达矩阵某一行的信息，这就是访问能力表（capability）。也可以从客体（列）出发，表达矩阵某一列的信息，这便成了访问控制表（access control list）。
- 能力（capability）是受一定机制保护的客体标志，标记了客体以及主体（访问者）对客体的访问权限。只有当一个主体对某个客体拥有访问能力的时候，它才能访问这个客体。

访问能力表（续）

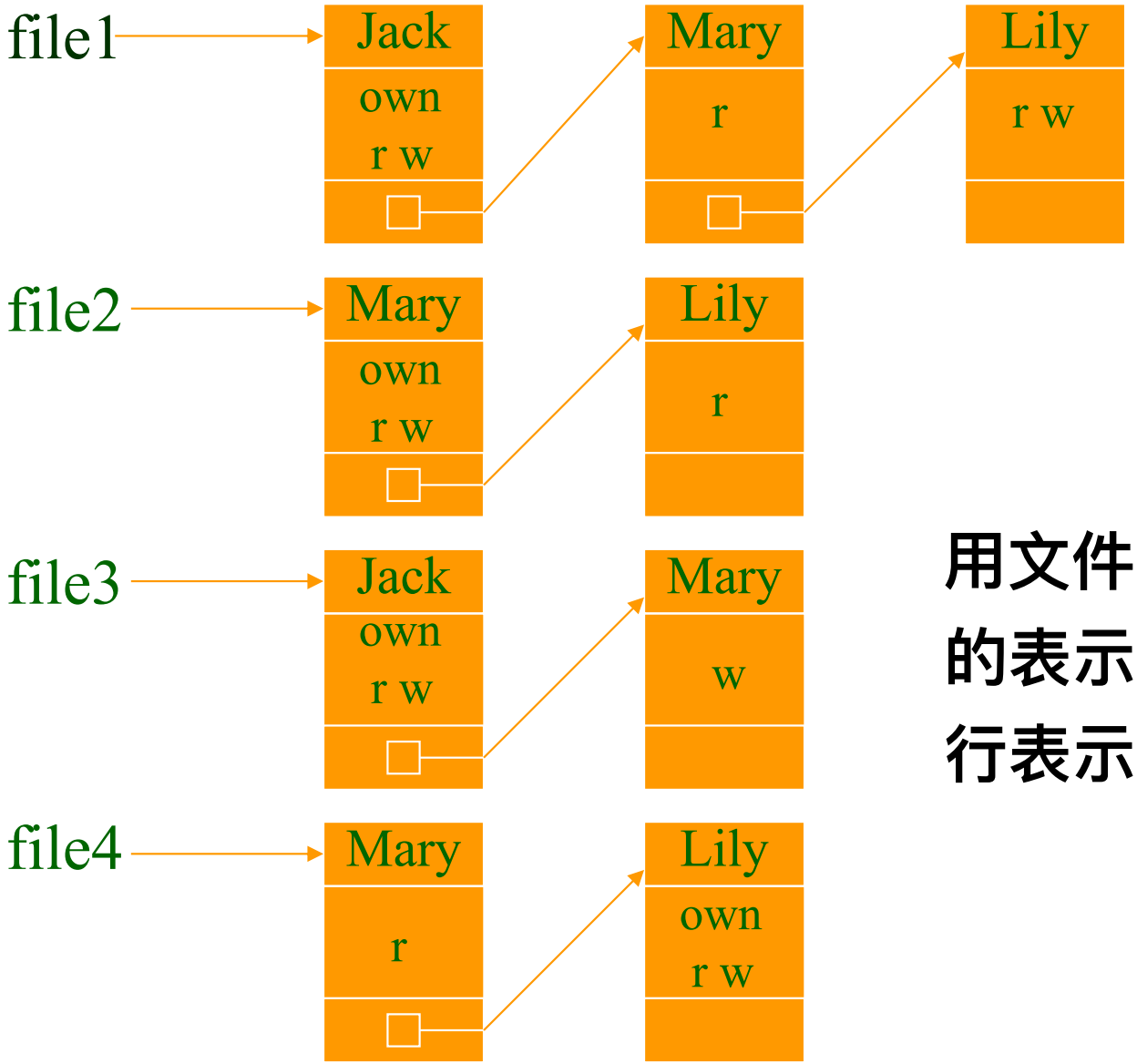


用文件的访问能力表的表示方法前例进行表示

访问能力表（续）

- 在访问能力表中，很容易获得一个主体所授权可以访问的客体及其权限，但如果要求获得对某一特定客体有特定权限的所有主体就比较困难。
- 在一个安全系统中，正是客体本身需要得到可靠的保护，访问控制服务也应该能够控制可访问某一客体的主体集合，能够授予或取消主体的访问权限，于是出现了以客体为出发点的实现方式——ACL（访问控制表）， 现代的操作系统都大体上采用基于ACL的方法。

访问控制表



用文件的访问控制表的表示方法对前例进行表示

访问控制表（续）

- ACL的优点：表述直观、易于理解，而且比较容易查出对某一特定资源拥有访问权限的所有用户，有效地实施授权管理。
- ACL的缺点：①ACL需要对每个资源指定可以访问的用户或组以及相应的权限。访问控制的授权管理费力而繁琐，且容易出错。②单纯使用ACL，不易实现最小权限原则及复杂的安全策略。

授权关系表（续）

基于ACL和基于访问能力表的方法都有自身的不足与优势，下面我们来看另一种方法——授权关系表（authorization relations）。每一行（或称一个元组）表示了主体和客体的一个权限关系，因此Jack访问file1的权限关系需要3行。这种实现方式特别适合采用关系数据库。

授权关系表

主体	访问权限	客体
Jack	own	file1
Jack	r	file1
Jack	w	file1
Jack	own	file3
Jack	r	file3
Jack	w	file3

用文件的授权关系表的表示方法对前例的一部分进行表示

主流访问控制技术

- 主流访问控制技术有：自主访问控制（DAC）、强制访问控制（MAC）、基于角色的访问控制（RBAC）等。自主访问控制和强制访问控制，都是由主体和访问权限直接发生关系，主要针对用户个人授予权限。

3.4.2 自主访问控制

- 自主访问控制DAC（discretionary access control）是目前计算机系统中实现最多的访问控制机制。
- DAC是在确认主体身份及所属组的基础上，根据访问者的身份和授权来决定访问模式，对访问进行限定的一种控制策略。
- 所谓自主，是指具有授予某种访问权力的主体（用户）能够自己决定是否将访问控制权限的某个子集授予其他的主体或从其他主体那里收回他所授予的访问权限。owner决定是否授予
- 基本思想是：允许某个主体显式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。DAC将访问规则存储在访问控制矩阵中，通过访问控制矩阵可以很清楚地了解DAC。

DAC的优缺点

- DAC的优点是其自主性为用户提供了极大的灵活性，从而使之适合于许多系统和应用。
- 由于这种自主性，在DAC中，信息总是可以从一个实体流向另一个实体，即使对于高度机密的信息也是如此，因此自主访问控制的安全级别较低。另外，由于同一用户对不同的客体有不同的存取权限，不同的用户对同一客体有不同的存取权限，用户、权限、客体间的授权管理复杂。

DAC的局限性

- 首先，DAC将赋予或取消访问权限的一部分权力留给用户个人，管理员难以确定哪些用户对那些资源有访问权限，不利于实现统一的全局访问控制。
- 其次，在许多组织中，用户对他所能访问的资源并不具有所有权，组织本身才是系统中资源的真正所有者。
- 而且，各组织一般希望访问控制与授权机制的实现结果能与组织内部的规章制度相一致，并且由管理部门统一实施访问控制，不允许用户自主地处理。显然DAC已不能适应这些需求。

3.4.3 强制访问控制

- 强制访问控制MAC（mandatory access control）依据主体和客体的安全级别来决定主体是否有对客体的访问权。
- 最典型的例子是Bell and LaPadula提出的BLP模型。
- BLP模型以军事部门的安全控制作为其现实基础，恰当地体现了军事部门的安全策略，然后用到计算机的安全设计中去。它侧重于信息的保密性。
- BLP模型已经成为许多系统或原型的实现的理论基础。

BLP模型

- 在BLP模型中，所有的主体和客体都有一个安全标签，它只能由安全管理员赋值，普通用户不能改变。这个安全标签就是安全级，客体的安全级表现了客体中所含信息的敏感程度，而主体的安全级别则反映了主体对敏感信息的可信程度。
- 在一般情况下，安全级是线性有序的。用λ标志主体或客体的安全标签，当主体访问客体时，需满足如下两条规则：

（1）简单安全属性：如果主体s能够读客体o，则λ(s)≥λ(o)

（2）保密安全属性：如果主体λ(s)能够写客体o，则λ(s)≤λ(o)

BLP模型（续）

主体向低级写

主体低于客体写

- BLP模型中，主体按照“向下读，向上写”的原则访问客体，即只有当主体的密级不小于客体的密级并且主体的范围包含客体的范围时，主体才能读取客体中的数据；只有当主体的密级不大于客体的密级，并且主体的范围包括客体的范围时，主体才能向客体中写数据。
- BLP模型保证了客体的高度安全性，它的最大优点是：它使得系统中的信息流程为单向不可逆的，保证了信息流总是低安全级别的实体流向高安全级别的实体。MAC能有效地阻止特洛伊木马。

MAC策略的优缺点

- 由于MAC策略是通过梯度安全标签实现信息的单向流通，从而很好地阻止特洛伊木马的泄漏，也因此而避免了在自主访问控制中的敏感信息泄漏的情况。
- 缺点是限制了高安全级别用户向非敏感客体写数据的合理要求，而且由高安全级别的主体拥有的数据永远不能被低安全级别的主体访问，降低了系统的可用性。BLP模型的“向上写”的策略使得低安全级别的主体篡改敏感数据成为可能，破坏了系统的数据完整性。另外强制访问控制MAC由于过于偏重保密性，造成实现工作量太大，管理不便，灵活性差。

3.5 本章知识点小结

- 身份标识与鉴别
  - （1）身份标识与鉴别概念
  - （2）身份认证的过程
- 口令认证方法
  - （1）口令管理
  - （2）脆弱性口令
- 生物身份认证
- 访问控制
  - （1）访问控制概念
  - （2）自主访问控制

身份认证 {指纹 / 虹膜

访问控制：矩阵 / 能力表 / 授权表 / 关系表

身份认证的方法

访问控制的技术 {口令 / 从机

基于唯一认证

基于生物信息，称为特征