

# 访问控制概念及实践

唐龙

# 访问控制概念

- ▶ 访问控制领域的机制能够使系统授予或撤销用户进行访问数据或对某一信息系统执行操作的权限。
- ▶ 访问控制系统包括：
  - ▶ 文件权限，如在文件服务器上执行“新建”、“只读”、“编辑”或“删除”。
  - ▶ 程序权限，如在应用服务器上执行程序权限。
  - ▶ 数据权限，如在数据库中提取或更新信息的权限。

# 目录



访问控制概念及模型

访问控制技术

访问控制实践

# 访问控制基本概念

信息安全的根本所在就是通过控制信息资源如何被访问来防范资源泄露或未经授权的修改。.....实现手段的本质都是出于技术、物理或管理的层面。

- ▶ 访问控制：针对越权使用资源的防御措施
- ▶ 目标：防止对任何资源（如计算资源、通信资源或信息资源）进行未授权的访问，从而使资源在授权范围内使用，决定用户能做什么，也决定代表一定用户利益的程序能做什么。

# 访问控制的作用

- ▶ 未授权访问：包括未经授权的使用、泄露、修改、销毁信息以及颁发指令等。
  - ▶ 非法用户对系统资源的使用
  - ▶ 合法用户对系统资源的非法使用
- ▶ 作用：机密性、完整性和可用性

*It is critical that security professionals understand all of the possible ways these principles can be provided and circumvented.*

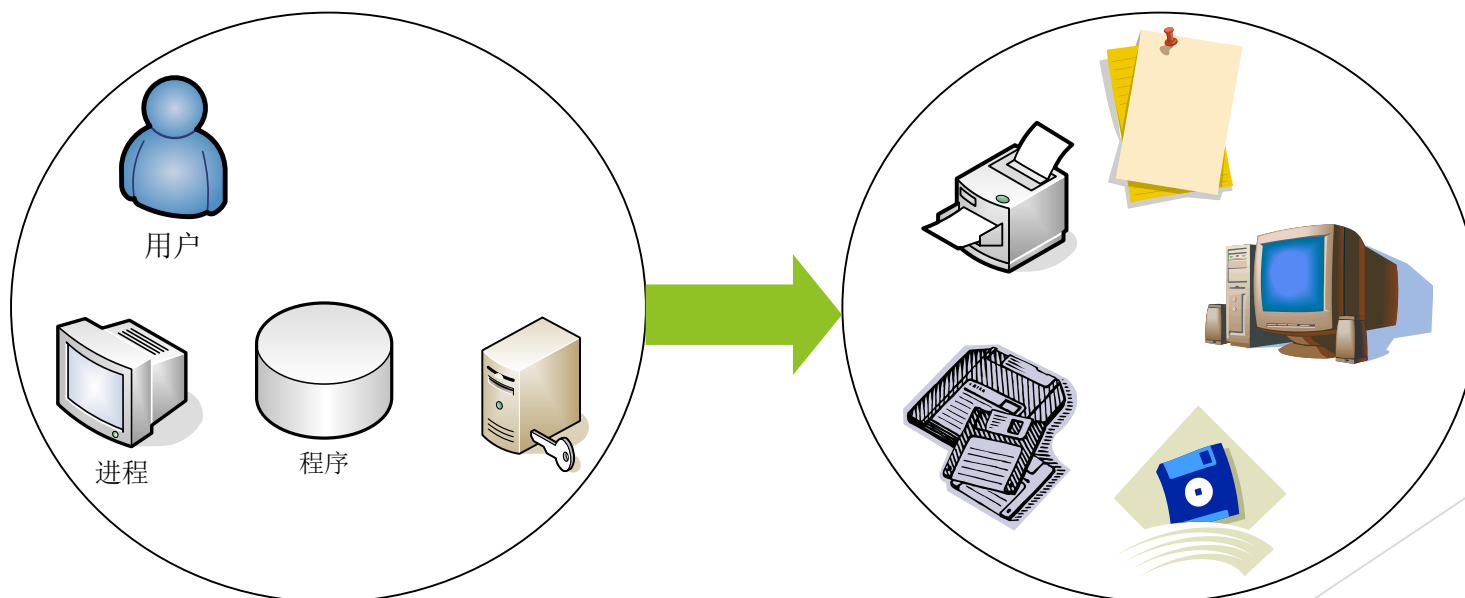
# 主体与客体

## ► 主体

- 发起者，是一个主动的实体，可以操作被动实体的相关信息或数据

## ► 客体

- 一种被动实体，被操作的对象，规定需要保护的资源



# 主体与客体的关系

- ▶ 主体：接收客体相关信息和数据，也可能改变客体相关信息
- ▶ 一个主体为了完成任务，可以创建另外的主体，这些子主体可以在网络上不同的计算机上运行，并由父主体控制它们
- ▶ 客体：始终是提供、驻留信息或数据的实体
- ▶ 主体和客体的关系是相对的，角色可以互换
  - ▶ 访问是主体和客体之间的信息传输



# 安全原则

## ► 可用性

- 确保那些已被授权的用户在他们需要的时候，确实可以访问到所需信息。即信息及相关的信息资产在授权人需要的时候，可以立即获得。

## ► 完整性

- 保证信息和处理方法的正确性和完整性。信息完整性一方面指在使用、传输、存储信息的过程中不发生篡改信息、丢失信息、错误信息等现象；另一方面指信息处理的方法的正确性，执行不正当的操作，有可能造成重要文件的丢失，甚至整个系统的瘫痪。

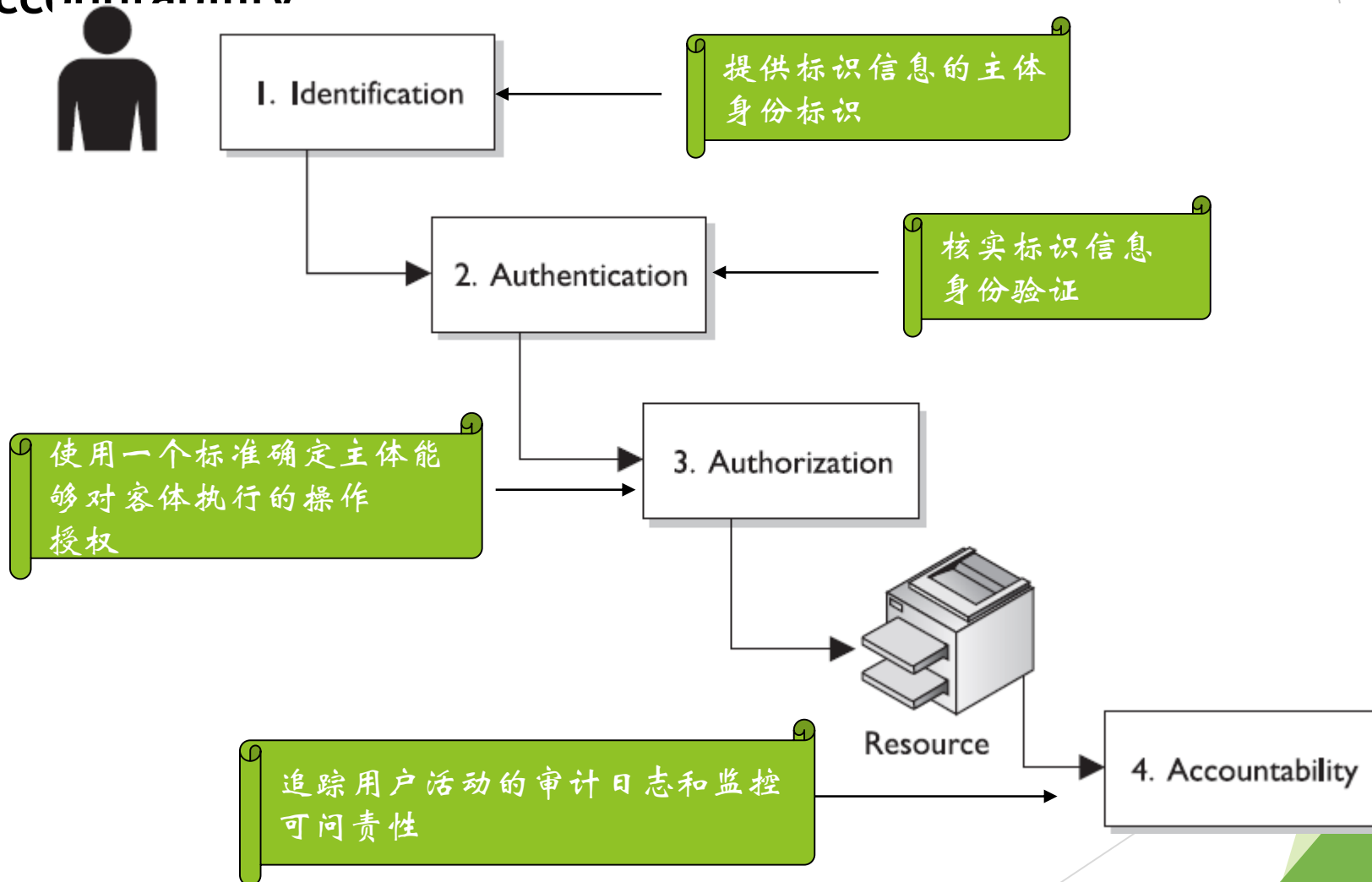
## ► 机密性

- 确保只有那些被授予特定权限的人才能够访问到信息。



# 标识、认证、授权和稽核

Identification, Authentication, Authorization, and Accountability



# 访问控制手段

## ► 管理 (administrative) 控制

- 组织和管理手段和机制控制人的行为以确保信息资产的安全，如安全策略，职务分离、强制假期、工作轮换等人事制度，教育培训，安全检查和安全审计等；

## ► 技术 (technical) 控制

- 使用现代电子技术手段和机制确保信息资产的安全，如电子门禁、防火墙、入侵检测系统、审计跟踪、生物识别等；

## ► 物理 (physical) 控制

- 使用传统物理实体安全手段和机制确保信息资产的安全，如传统锁具、证件、保险柜、警卫、栅栏、灯光等。

# 标识 ( Identification )

- ▶ 标识是实体身份的一种计算机表达，每个实体与计算机内部的一个身份表达绑定
- ▶ 标识的主要作用：访问控制和审计
  - ▶ 访问控制：标识用于控制是否允许特定的操作
  - ▶ 审计：标识用于跟踪所有操作的参与者，参与者的任何操作都能被明确地标识出来

# 认证 ( Authentication )

- ▶ 认证的三种方式
  - ▶ 他知道的内容 (*something a person knows*)
    - ▶ 根据知识进行认证
  - ▶ 他持有的证明 (*something a person has*)
    - ▶ 根据所有权进行认证
  - ▶ 他就是这个人 (*something a person is*)
    - ▶ 根据特征进行认证

概念性的问题：这个人是不是他所宣称的那个人吗？  
The conceptual question is, “Who is this person?”

# 认证 ( Authentication )

- ▶ 确认实体是它所声明的，提供了关于某个实体身份的保证，某一实体确信与之打交道的实体正是所需要的实体
  - ▶ 口令、挑战-应答、生物特征鉴别
- ▶ 所有其它的安全服务都依赖于该服务
- ▶ 需求：某一成员（声称者）提交一个主体的身份并声称它是那个主体
- ▶ 目的：使别的成员（验证者）获得对声称者所声称的事实信任

# 授权 ( Authorization )

► 规定主体可以对客体执行的操作：

► 读

► 写

► 执行

► 拒绝访问

► ...

# 访问控制模型

- ▶ 自主访问控制
- ▶ 强制访问控制
- ▶ 角色型访问控制

# 自主访问控制

- ▶ **Discretionary access control (DAC)**
- ▶ 允许客体的属主（创建者）决定主体对该客体的访问权限
- ▶ 灵活地调整安全策略
- ▶ 具有较好的易用性和可扩展性
- ▶ 常用于商业系统
- ▶ 安全性不高
- ▶ 计算机领域访问权限

不能访问	读	写	执行	删除	更改	完全控制
-	R	W	X	D	C	-

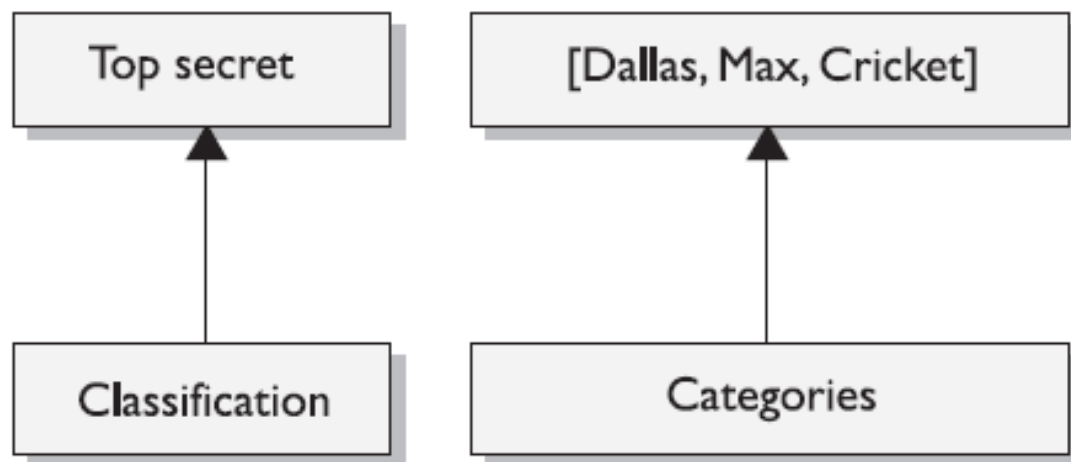


# 强制访问控制

- ▶ ***Mandatory access control (MAC)***
- ▶ 主体对客体的所有访问请求按照强制访问控制策略进行控制，客体的属主无权控制客体的访问权限，以防止对信息的非法和越权访问
- ▶ 主体和客体分配有一个安全属性
- ▶ 应用于军事等安全要求较高的系统
- ▶ 可与自主访问控制结合使用

# 强制访问控制

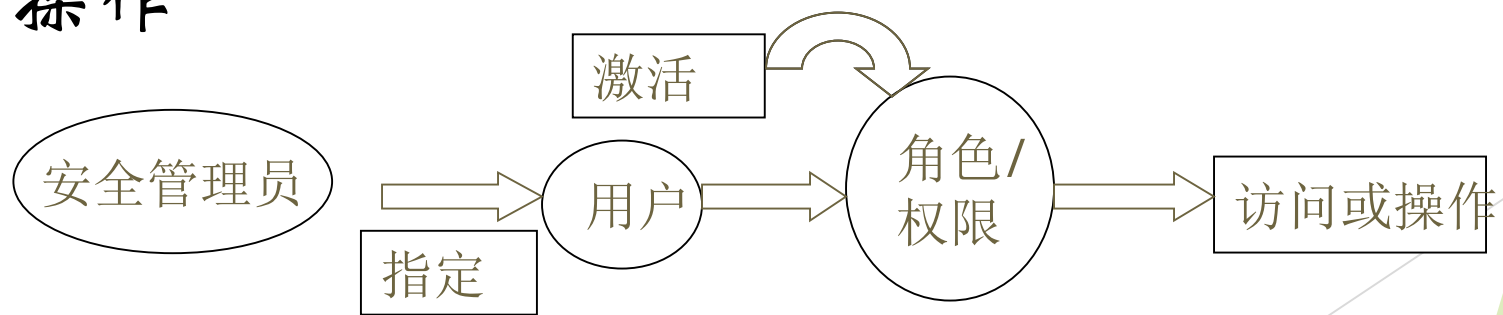
- ▶ 采用MAC模型每一个主体和客体必须有一个敏感性标签，也称为安全标签



一个敏感标签由一个分类和不同的类别组成

# 角色型访问控制

- ▶ RBAC的基本思想是根据用户所担任的角色来决定用户在系统中的访问权限。
- ▶ 一个用户必须扮演某种角色，而且还必须激活这一角色，才能对一个对象进行访问或执行某种操作



# RBAC的组成

## ▶ 核心RBAC

- ▶ 用户与权限之间存在一种多对多的关系
- ▶ 会话是某个用户与少数几个角色之间的对应关系
- ▶ 提供传统但稳健的机遇群组的访问控制

## ▶ 层级RBAC

- ▶ 角色关系定义了用户成员与权限继承
- ▶ 反映组织结构和功能描述
- ▶ 两种类型的层级
  - ▶ 有限层级-只允许一个层级
  - ▶ 普通层级：允许多个层级

# 目录



访问控制概念及模型

访问控制技术

访问控制实践

# 访问控制方法和技术

- ▶ 规则型访问控制
- ▶ 限制性用户接口
- ▶ 访问控制矩阵
- ▶ 内容相关访问控制
- ▶ 上下文相关访问控制

# 规则型访问控制

- ▶ 使用特定的规则来规定主体和客体之间可以做什么，不可以做什么。
- ▶ 遵循“知其所需”原则
- ▶ 用于MAC强制访问控制模型
- ▶ 内容过滤采用“如果-那么 (If-Then)”模式
- ▶ 规则由管理员制定，用户不能修改

# 限制性用户接口

- ▶ 通过不允许请求某些功能、信息或访问特定的系统资源，限制性的用户接口能够限制用户的访问能力。

- ▶ 菜单和外壳
- ▶ 数据库视图
- ▶ 物理限制接口

Harris, D	\$45,000	8am-5pm
Torkelson, T	\$60,000	6pm-2am
Kowtko, J	\$45,000	8am-5pm
Swenson, J	\$65,000	6pm-2am

工资员数据库视图

Harris, D	Work history	8am-5pm
Torkelson, T	Work history	6pm-2am
Kowtko, J	Work history	8am-5pm
Swenson, J	Work history	6pm-2am

经理数据库视图



# 访问控制矩阵

- ▶ 包含主体和客体的表，它规定每个主体对每个客体所能执行的动作
- ▶ 具有DAC自主访问控制模型属性
- ▶ 访问权限可以直接分配给主体或客体

User	File 1	File2	File3
Diane	Read and execute	Read, write, and execute	No access
Katie	Read and execute	Read	No access
Chrissy	Read, write, and execute	Read and execute	Read
John	Read and execute	No access	Read and write

访问控制矩阵示例

# 访问控制矩阵

- ▶ 功能表

- ▶ 指定某些主体对待客体进行操作的访问权限

- ▶ 访问控制列表

- ▶ 主体被授权访问特定客体的权限列表，并且定义了授权程度

访问控制列表

功能	主体	文件1	文件2	文件3	文件4
	Larry	读	读和写	读	读和写
	Curl y	完全控制	不能访问	完全控制	读
	Mo	读和写	不能访问	读	完全控制
	Bob	完全控制	不能访问	不能访问	不能访问

功能表与主体绑定  
ACL与客体绑定

ACL

# 内容相关访问控制

- ▶ 对客体的访问取决于客体的内容
  - ▶ 需要对所访问客体的内容进行扫描，所以系统开销比较大；
  - ▶ 具有比较细的控制粒度，适合对一类数据中某些敏感信息进行保护；
  - ▶ 系统管理开销比较大，需要进行大量的配置工作；
- ▶ 此类控制首先被用于保护数据库中某些敏感数据，如护士被允许查看病人的化验结果，但如果化验项目是HIV检验，系统将不允许一般护士查看结果，而只允许特定人员访问。

# 上下文相关访问控制

- ▶ 基于一组信息的上下文做出访问决策
- ▶ **是否授予主体访问客体的权限不仅取决于主体和客体本身的特点而且取决于访问事件的当前状况，如：**
  - ▶ 在防火墙应用中，是否允许数据包穿越防火墙不仅根据防火墙所设置的静态规则决定，而且根据连接的当前状况（如是否与已有连接存在逻辑关系）决定；
  - ▶ 在存储配额管理应用中，是否允许用户使用存储空间不仅取决于所授予用户的静态访问权限，而且根据用户已经占用的存储空间数量决定。

# 集中式访问控制管理

- ▶ **集中式管理**，由专门的访问控制管理人员集中对访问控制进行设置和管理，这种方式：
  - ▶ 有利于执行统一、严格的安全政策；
  - ▶ 在访问需求变化较多的环境中访问控制管理的负担比较重，容易形成瓶颈；
- ▶ **目前主流的集中式认证服务**主要解决对各种网络设备进行访问时的认证（authentication）、授权（authorization）和记账（accounting）问题，所以又被称为AAA服务；
- ▶ **AAA服务的主要特点**包括：
  - ▶ 分布式（客户端/服务器）安全构架（distributed security model）；
  - ▶ 认证事务（authentication transaction）；
  - ▶ 灵活的认证机制（authentication mechanisms）；
  - ▶ 可扩充协议（extensible protocol）。
- ▶ **主流的AAA服务器**包括：
  - ▶ RADIUS；
  - ▶ TACACS；
  - ▶ DIAMETER。

# 目录



访问控制概念及模型

访问控制技术

访问控制实践

# 身份管理

- ▶ 身份管理(Identity Management ,IdM),包括使用不同产品对用户进行自动化身份标识、身份验证和授权。
- ▶ 身份管理的问题:
  - ▶ 每位用户应当能够访问哪些内容
  - ▶ 由谁批准和允许访问
  - ▶ 访问决策如何与策略相对应
  - ▶ 之前的员工是否仍然拥有访问权
  - ▶ 我们如何与动态的、不断变化的环境同步
  - ▶ 撤销访问的过程是怎样的
  - ▶ 如何对访问进行集中控制和监控
  - ▶ 为什么雇员需要记住8个密码?
  - ▶ 不同操作平台如何进行集中管理
  - ▶ 如何控制雇员、客户和合作伙伴的访问权限
  - ▶ 如何确保遵守必要的法规
  - ▶ 如何辞职

# 身份管理技术

- ▶ 目录
- ▶ Web访问管理
- ▶ 密码管理
- ▶ 单点登录
- ▶ 账户管理
- ▶ 配置文件更新



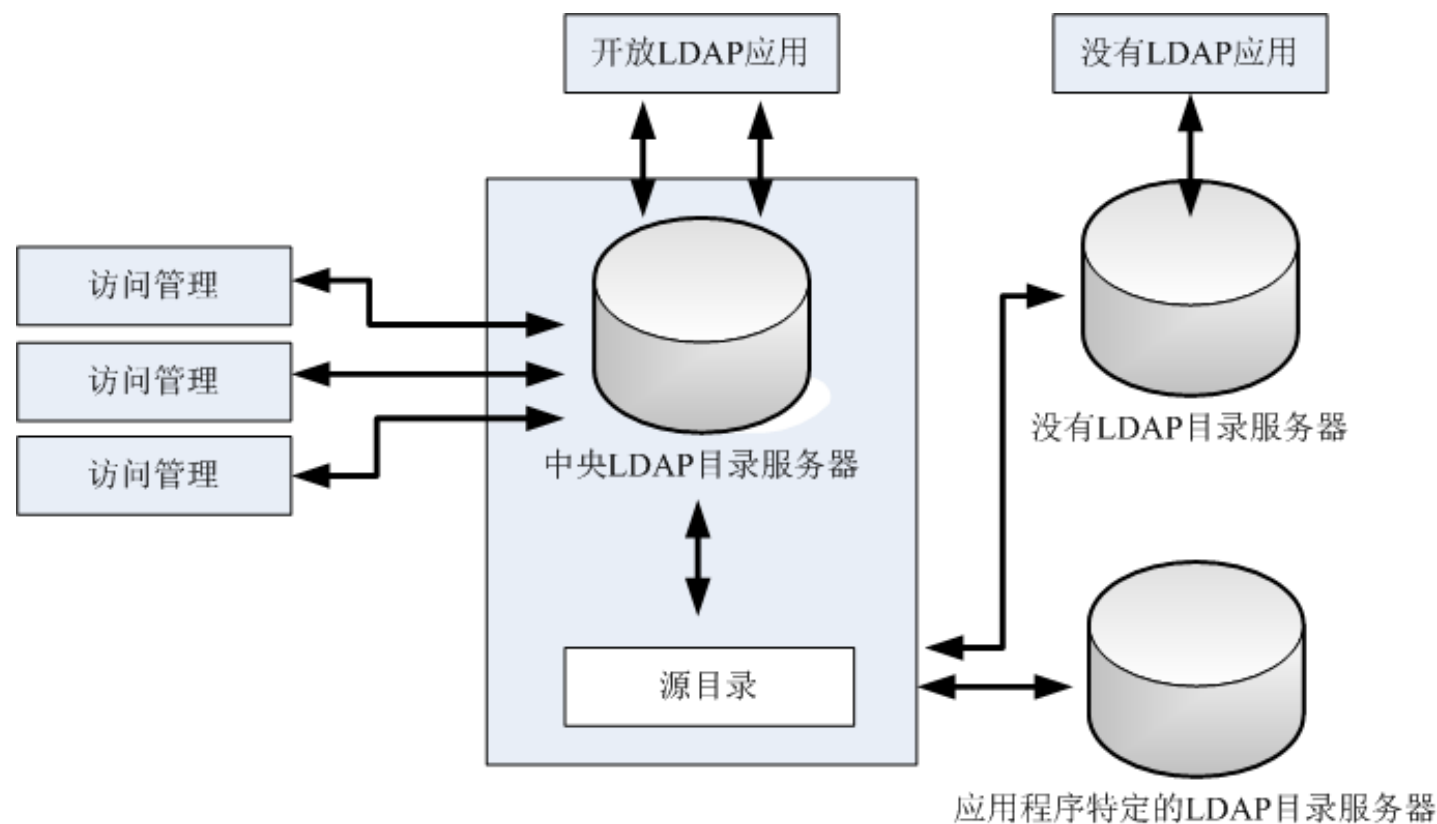
# 目录

## ▶ 目录

- ▶ 包含与公司网络资源和用户有关的信息
- ▶ 目录通过X.500标准和某种协议（轻量级目录访问协议（LDAP），允许主体和应用程序与目录进行交互
- ▶ 目录的客体由目录服务管理
- ▶ 用例：
  - ▶ Windows域管理

# 目录在身份管理中的角色

- 为读取和搜索操作而进行过优化的专用数据库软件，它是身份管理解决方案的主要组件

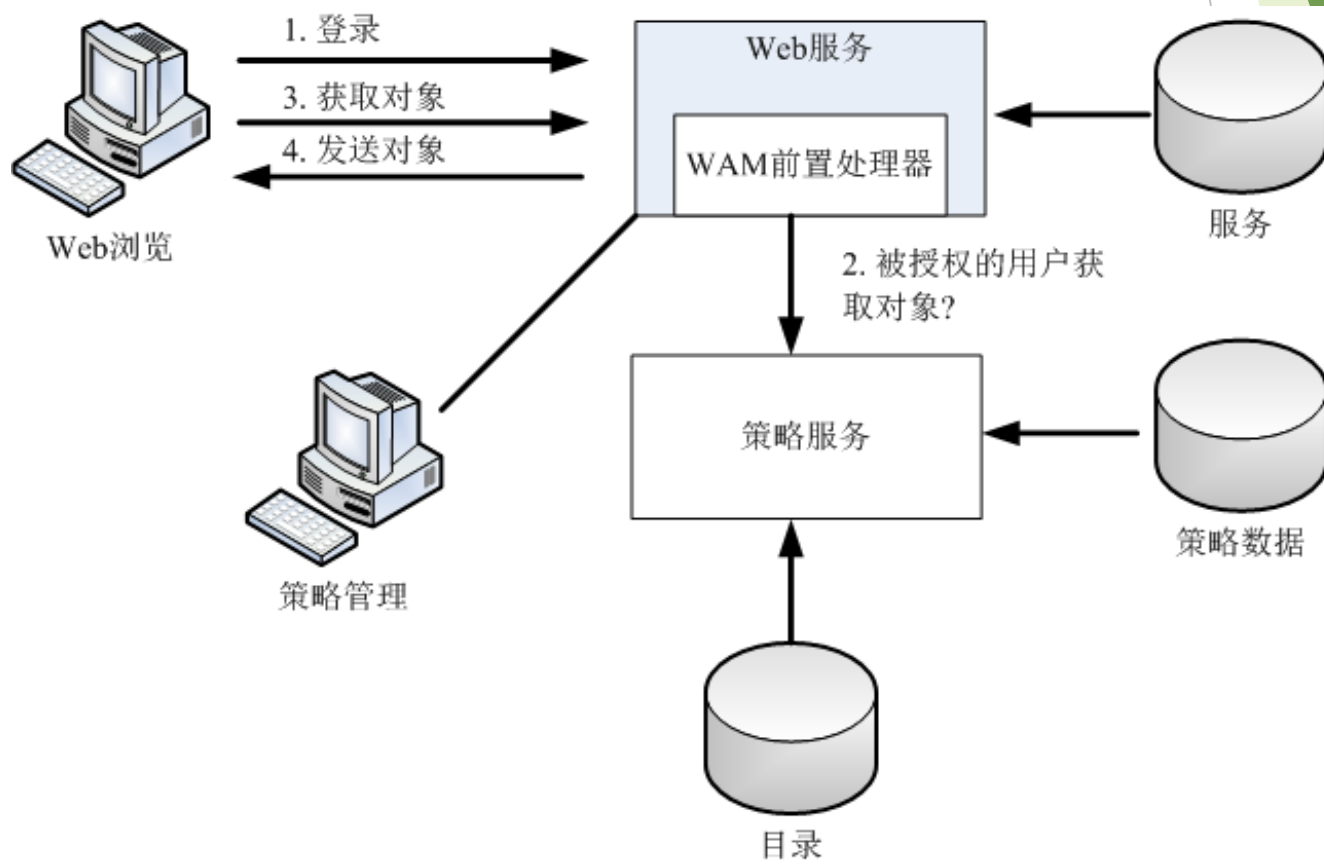


元目录从其他来源中提取数据以更新IdM目录

# Web访问管理

- Web访问管理（Web Access Management, WAM）软件控制用户在使用Web浏览器与基于Web的企业资产交互时能够访问哪些内容

- 1、用户向Web服务器送交凭证
- 2、Web服务器验证用户的凭证
- 3、用户请求一个资源（客体）
- 4、Web服务器使用安全策略进行验证以确定是否允许
- 5、Web服务器允许用户访问请求的资源



# 密码管理

## ▶ 密码同步

- ▶ 允许用户为多个系统维护一个密码，降低保留不同系统的不同密码的复杂性

## ▶ 自助式密码重设

- ▶ 通过允许用户重新设置密码，减少服务台人员受到的求助电话数量

## ▶ 辅助式密码重设

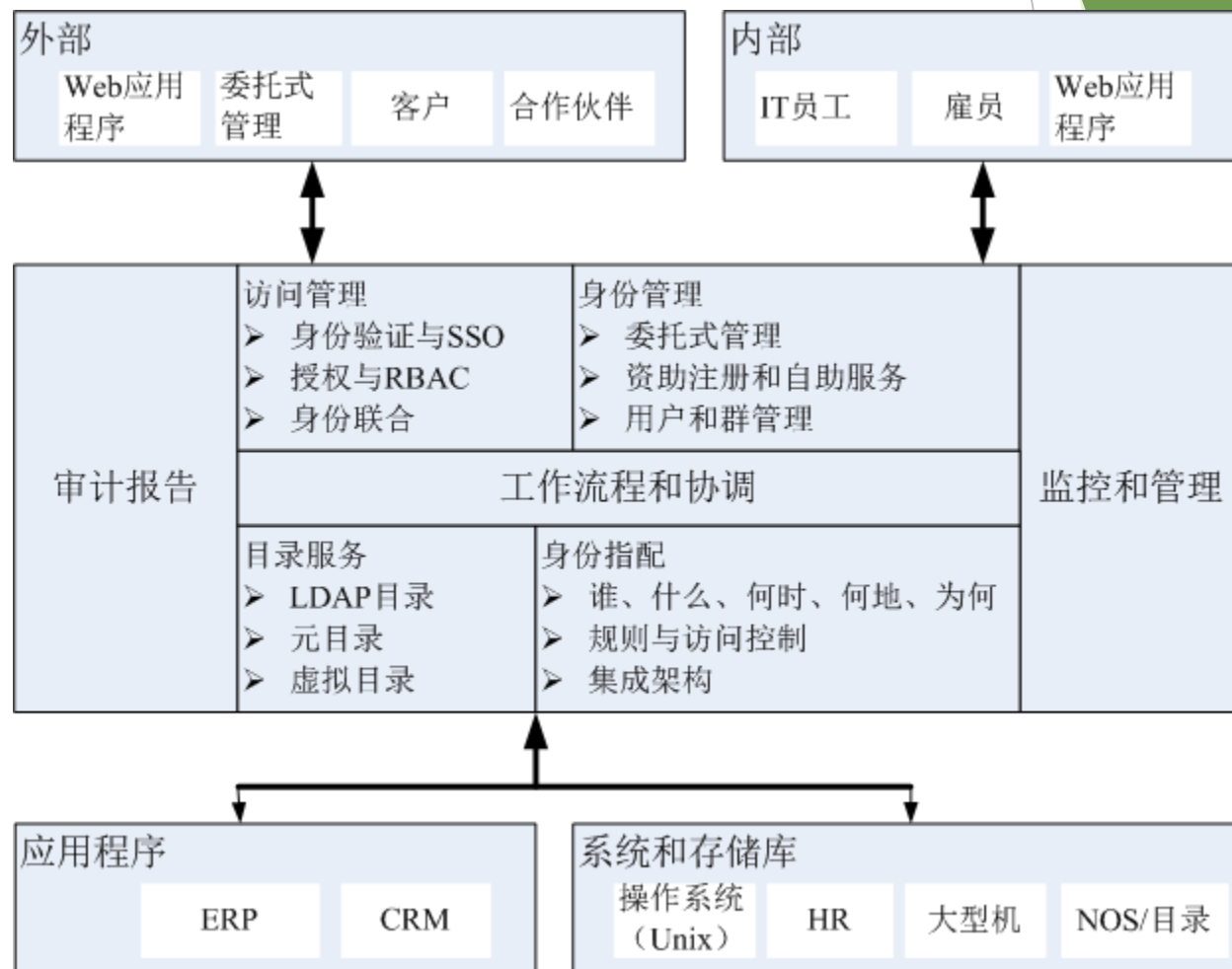
- ▶ 允许服务台工作人员在重设密码前对打入电话的用户进行身份验证。
- ▶ 减少有关密码问题的决策过程

# 单点登录

- ▶ 允许用户只须进行一次身份验证，随后不须再次身份验证就可以访问环境中的资源。
- ▶ 风险
  - ▶ 瓶颈问题或者单点故障
  - ▶ 风险集中

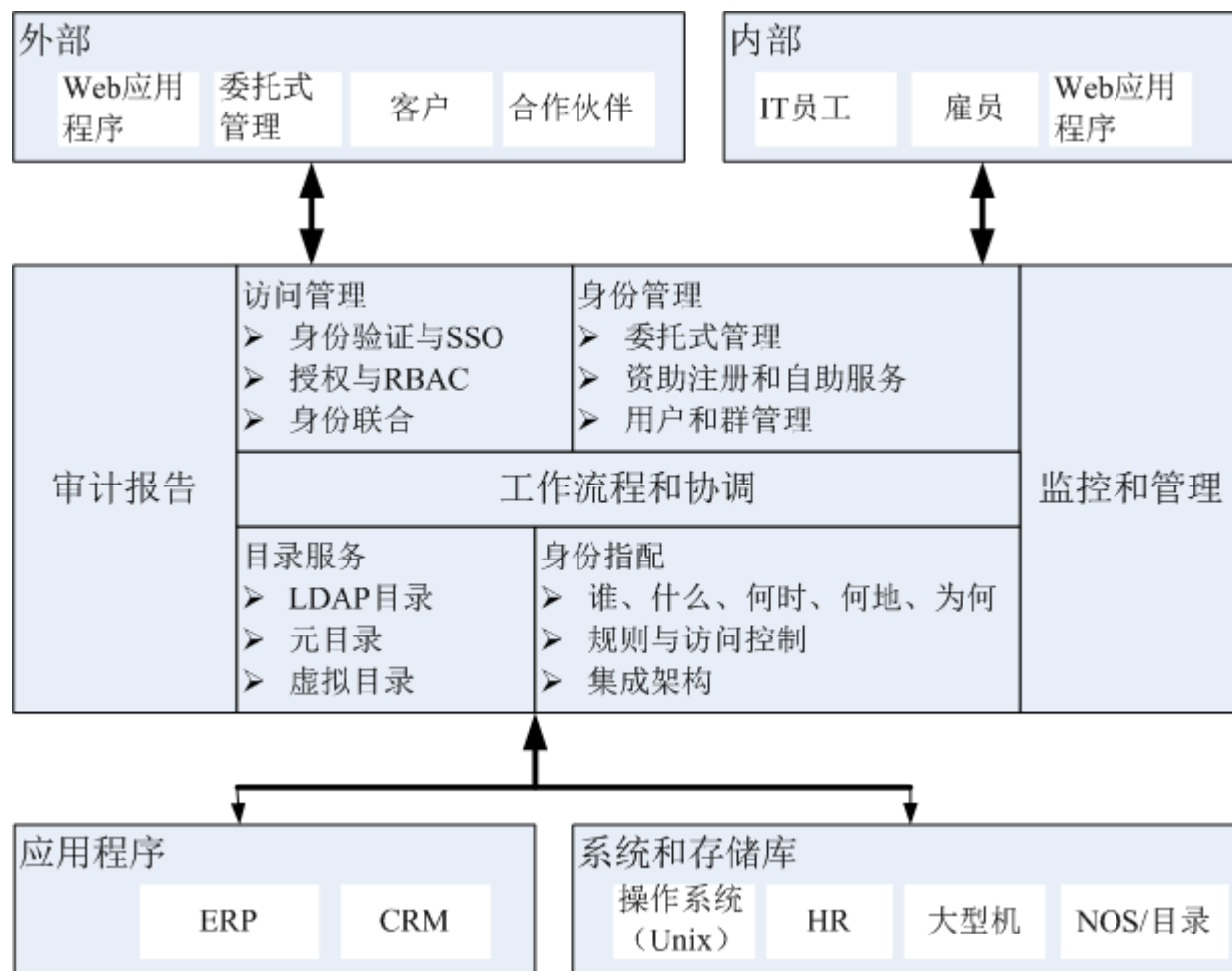
# 账户管理

- 负责创建所有系统中的用户账号，在必要时更改账户权限，并在不再需要时删除账户。



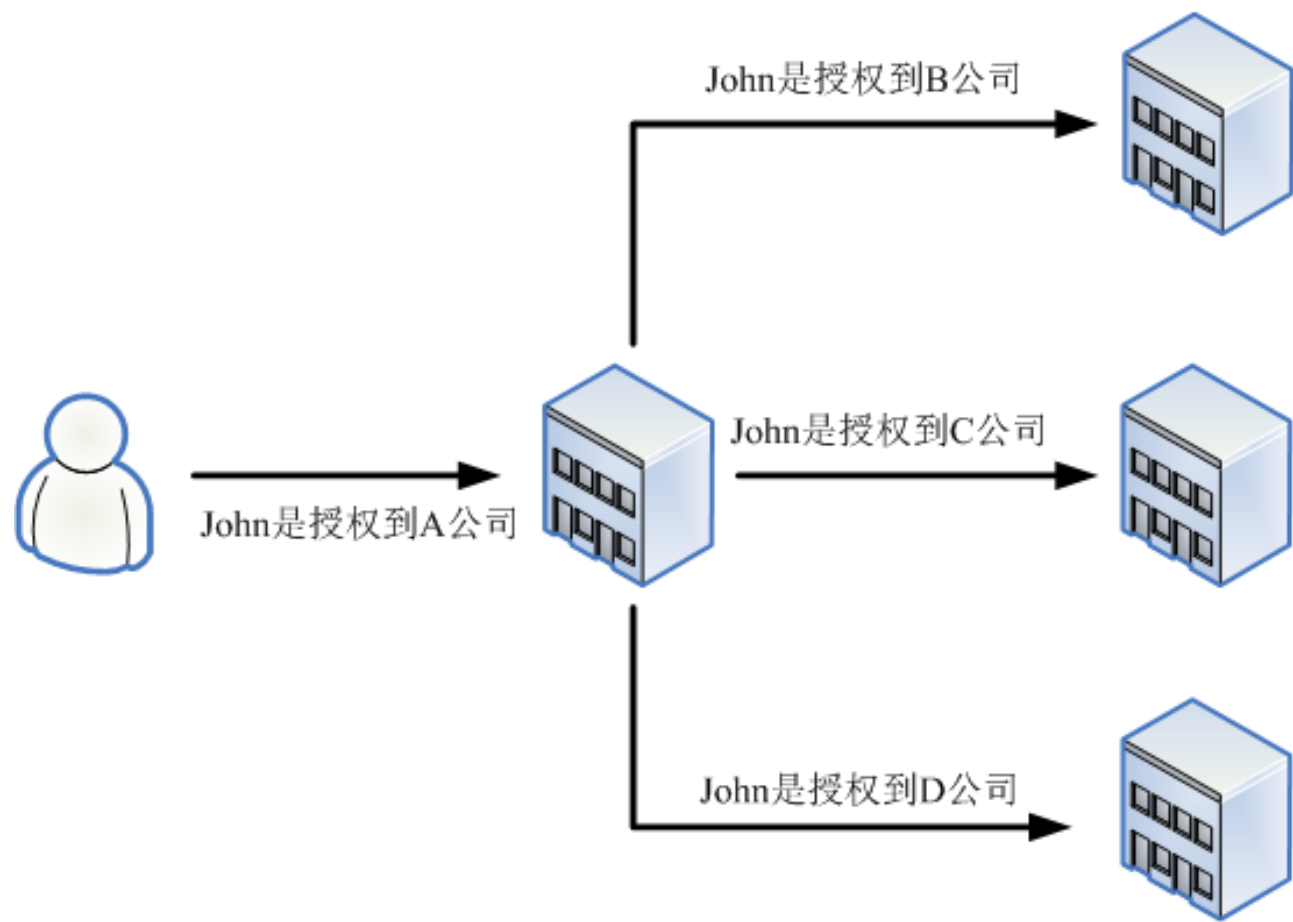
企业身份管理系统组件

# 指配



企业身份管理系统组件

# 联合





# 访问控制和标记语言

HTML: 超文本标记语言  
SGML: 标准通用标记语言  
GML: 通用标记语言

```
graph LR; OASIS[OASIS: 信息标准促进组织] --> HTML[HTML: 超文本标记语言]; OASIS --> SGML[SGML: 标准通用标记语言]; OASIS --> GML[GML: 通用标记语言]; OASIS --> XML[XML: 可扩展标记语言]; OASIS --> SPML[SPML: 服务供应标记语言]; OASIS --> XACML[XACML: 可扩展访问控制标记语言];
```

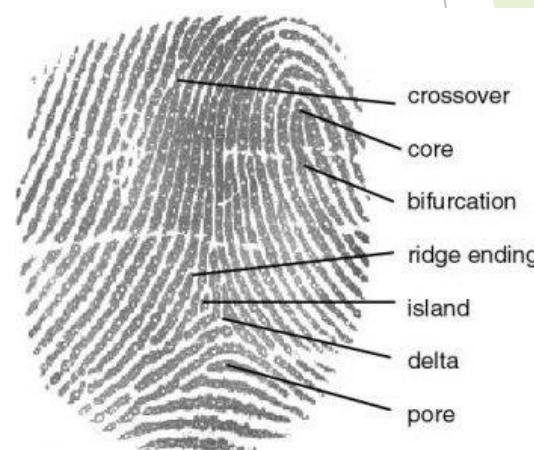
The diagram illustrates the relationship between OASIS and various XML-based languages. OASIS is shown as the parent organization, with arrows pointing to each of the listed languages. The languages are grouped into two boxes: the top box contains HTML, SGML, and GML, while the bottom box contains XML, SPML, and XACML. A curved arrow also points from SGML to GML, indicating a relationship between them.

XML: 可扩展标记语言  
SPML: 服务供应标记语言  
XACML: 可扩展访问控制标记语言

OASIS: 信息标准促进组织

# 生物识别技术的特点

- ▶ 生物识别技术在身份认证方面的优点包括：
  - ▶ 与生俱来、无需赋予；
  - ▶ 无需记忆、不会遗失；
  - ▶ 难以仿冒和复制；
  - ▶ 比其它认证信息具有更高的安全性；
- ▶ 身份认证技术的缺点有：
  - ▶ 需要专业设备，成本较高；
  - ▶ 识别精度还有待提高；
  - ▶ 接受度受到成本、性能、习惯、文化等因素制约。



# 生物识别技术的工作原理

- ▶ 选择生物学特征 (characteristic) 做为生物识别测量的目标;
- ▶ 对所选择生物学特征进行测量, 如采集图像或测量主体生命活动 (life sign) 信息, 并将其中被称为匹配点 (match point) 的关键信息记录在模板 (template) 中, 将模板存储在生物识别系统的数据库里, 这一过程被称为注册 (enrollment), 此过程一般耗时2分钟;
- ▶ 生物识别技术可用于认证, 也被称为正匹配 (positive matching) 或一对一匹配 (one-to-one matching), 或身份识别, 也被称为负匹配 (negative matching) 或一对多匹配 (on-to-many matching);
- ▶ 用户需要进行身份识别或认证时, 系统再次对主体的这些特征进行测量, 并将测量结果与数据库中的模板进行匹配, 并根据匹配结果确定认证或身份识别的结果, 此过程平均耗时6秒钟。

# 生物学特征 ( Biometric Traits )

- ▶ 由基因组成决定的遗传学型 (genotypic) 特征, 如:
  - ▶ 面容 (facial geometry) ;
  - ▶ 手形 (hand geometry) ;
  - ▶ DNA特征 (DNA patterns) ;
- ▶ 由胎儿发育期形成的随机型 (randotypic) 特征, 如:
  - ▶ 指纹 (fingerprints) ;
  - ▶ 虹膜特征 (iris patterns) ;
  - ▶ 手部血管特征 (hand-vein patterns);
- ▶ 人通过学习和训练形成的动作 (behavioral) 特征, 如:
  - ▶ 签名动力学 (signature dynamics) ;
  - ▶ 击键特征 (keyboard typing patterns) 。



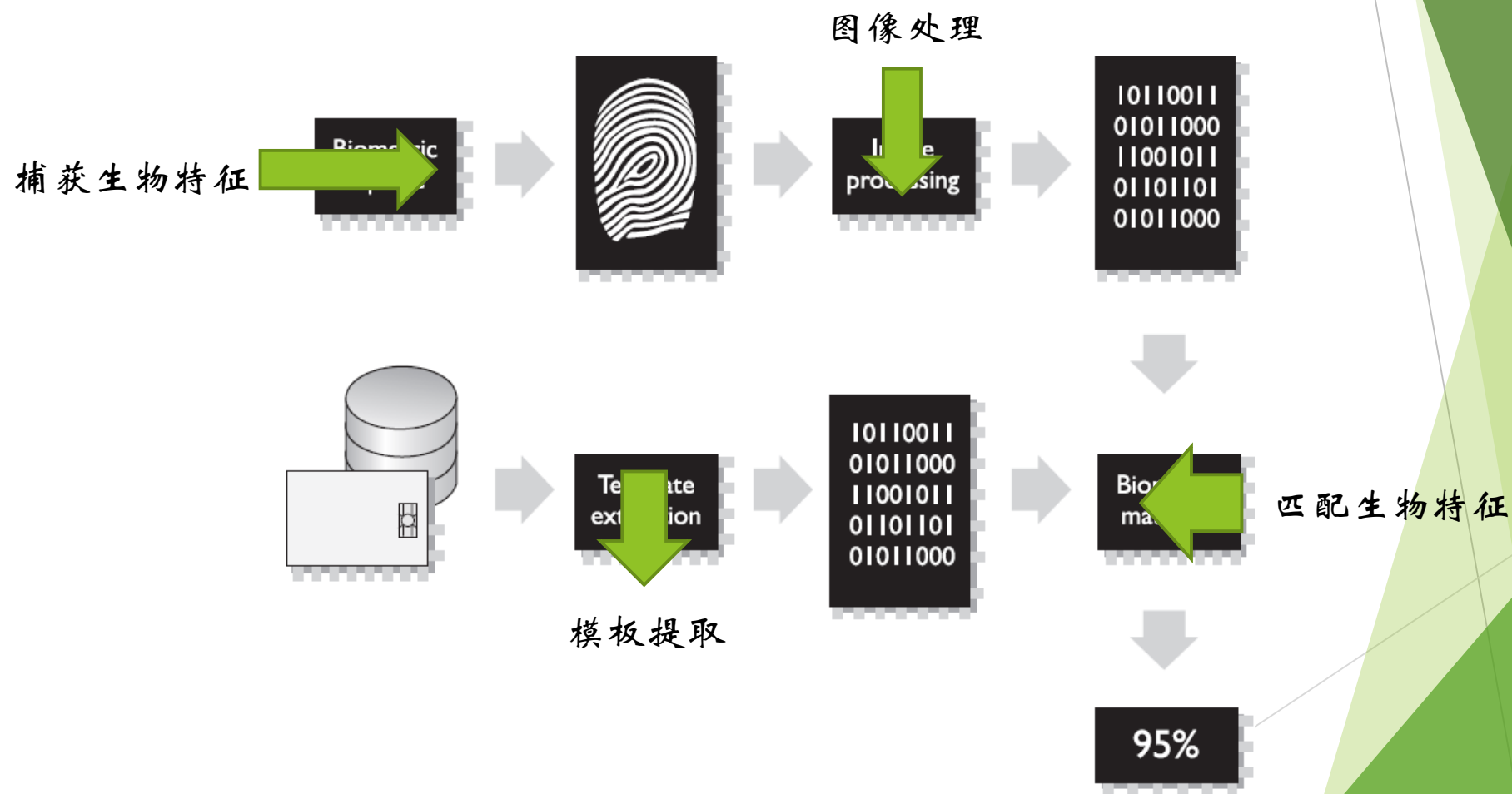
# 生物识别的错误率

- ▶ 表示合法用户被拒绝或被认为是非法用户的错误拒绝率 (false rejection rate, FRR)，也被称为I型错误 (type I error) 或错误否定 (false negative)；
- ▶ 表示非法用户被接受或被认为是合法用户错误接受率 (false acceptance rate, FAR)，也被称为II型错误 (type II error) 或错误肯定 (false positive)；
- ▶ 通过调整阈值等参数使系统错误拒绝率和错误接受率相等时，这个错误率被称为交叉错误率 (crossover error rate, CER)，也被称为相等错误率 (equal error rate, EER)，它是表示生物识别系统性能的重要参数；
- ▶ 系统无法注册用户的比率被称为注册故障率 (failure to enroll rate, FTE rate)。

# 影响用户接受生物识别的因素

- ▶ 侵犯性 (invasiveness)，有些生物测量方法（虹膜扫描和指纹读取）需要人体部位与测量设备密切接触，这会使一些用户感觉受到侵犯，声音识别和面容识别这方面相对要好一些；
- ▶ 舒适度 (psychological and physical comfort)，生物识别的目的（寻找嫌疑犯还是保护用户？），手段（指纹常用来辨别犯罪嫌疑人）、易用性（是否便捷？）都影响到用户的接受性；
- ▶ 隐私 (privacy)，生物特征是纯粹的个人信息，用户有理由担心这些信息的用途和安全性，如这些信息是否会被出售给第三方？这种信息是否会被用来监视用户的私人活动？信息是否会泄漏而造成他人假冒用户身份？
- ▶ 特征的替换 (characteristic replacement)，生物特征是难以替换的，如果这些特征信息泄漏可能造成无法挽回的影响。

# 生物测定学



生物测定学数据转换为二进制数，并与数据库中的对应数据进行比较以验证身份

# 生物测定学

- ▶ 指纹
- ▶ 手掌扫描
- ▶ 视网膜扫描
- ▶ 虹膜扫描
- ▶ 动态签名
- ▶ 动态击键
- ▶ 声纹
- ▶ 面部扫描
- ▶ 手形拓扑

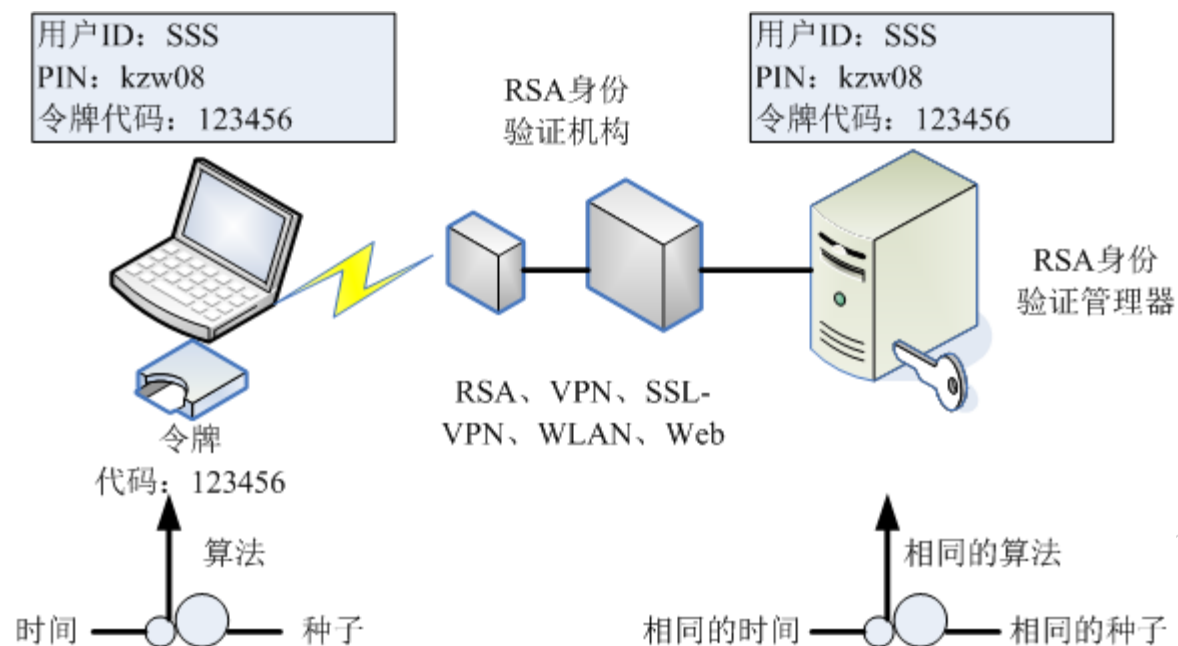


# 密码

- ▶ 密码管理
  - ▶ 密码获取技术
    - ▶ 电子监控
    - ▶ 访问密码文件
    - ▶ 蛮力攻击
    - ▶ 字典攻击
    - ▶ 社会工程
    - ▶ 彩虹表
- ▶ 密码检查器
- ▶ 密码散列与加密
- ▶ 密码生命周期
- ▶ 限制登录次数

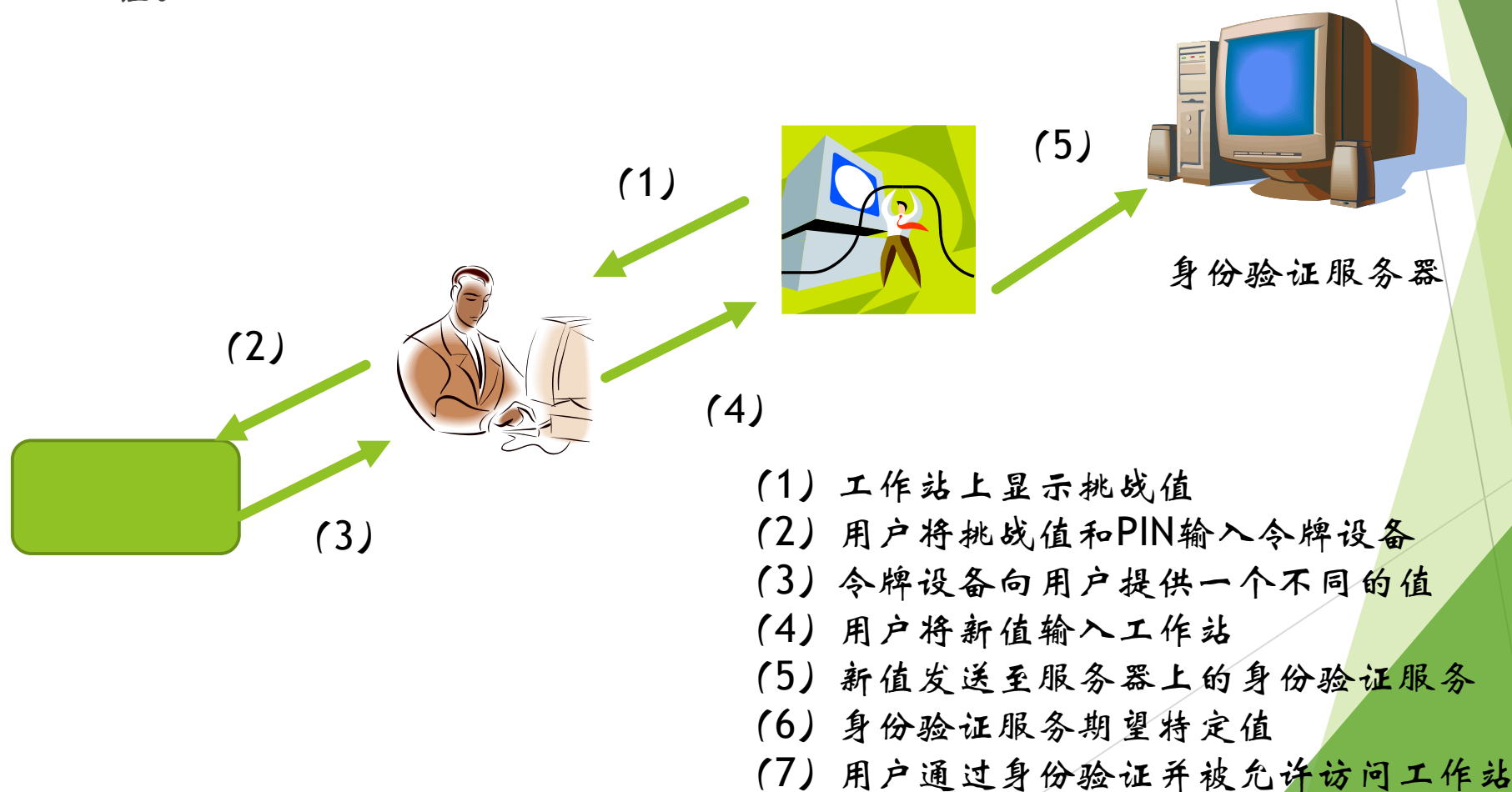
# 一次性密码

- 同步：通过使用时间或计数器作为身份验证过程的核心部分，同步令牌设备与身份验证服务能够同步



# 一次性密码

- 异步：使用异步令牌生成方式的令牌设备通过挑战/响应机制对用户进行身份验证。



# 身份验证

- ▶ 密钥
- ▶ 密码短语
- ▶ 存储卡

# 智能卡的安全特性

## ► 硬件

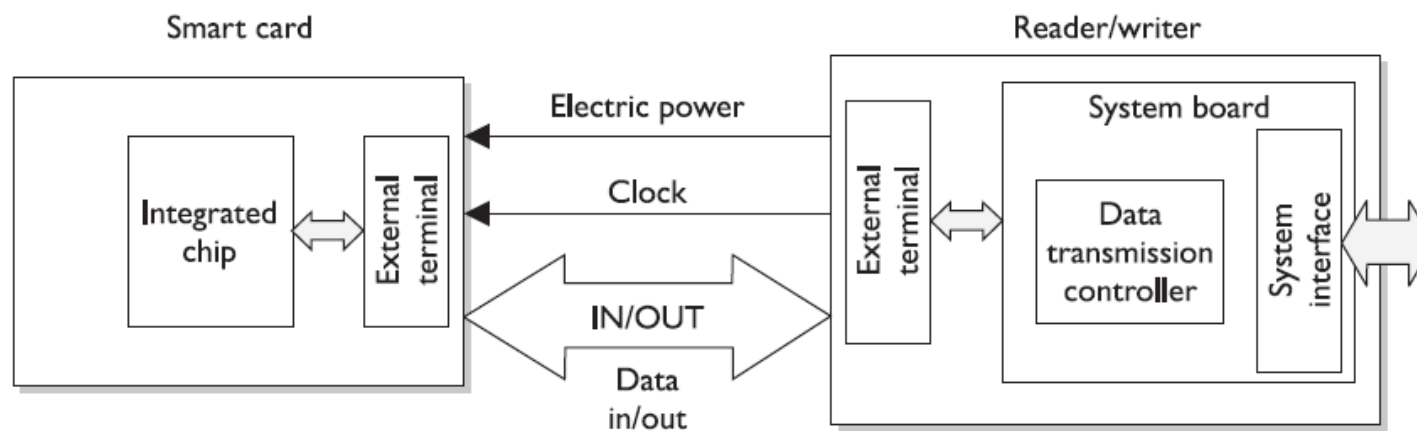
- 与外界通信前，先完成智能卡与终端间的认证
- 加入安全传感器，防止在数据被读出或写入时被修改
- 发生异常，智能卡复位，或者置标志位，使智能卡操作系统做出相应反应
- 存储器加密，不保存任何明文

## ► 软件

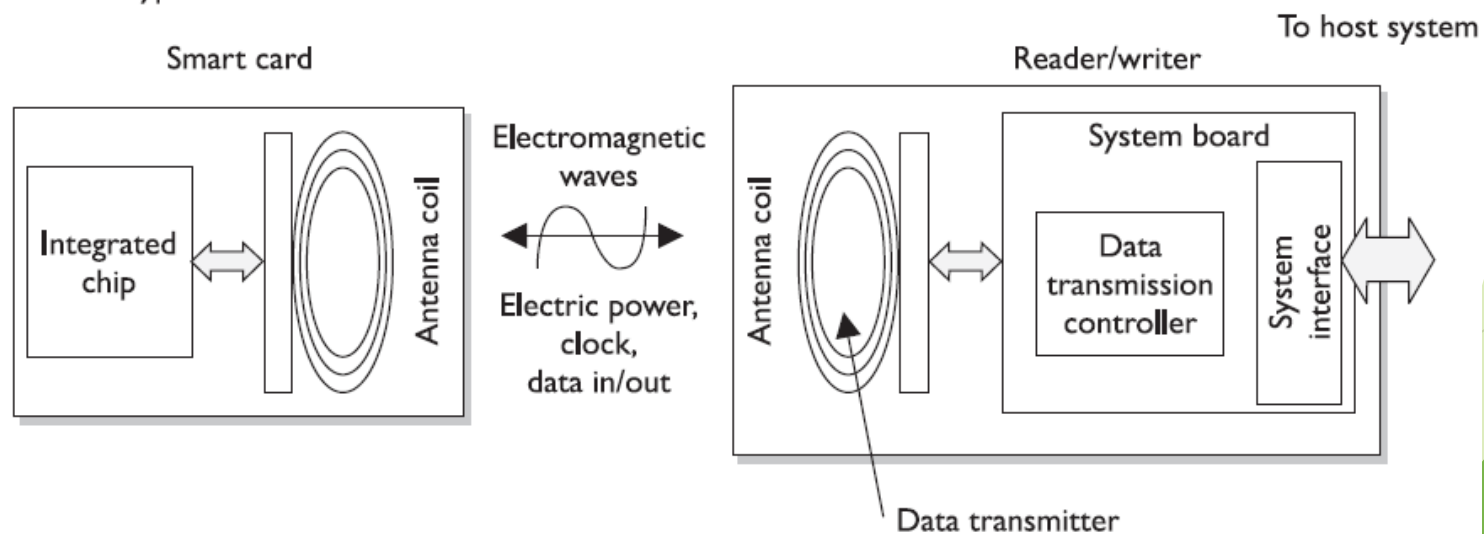
- 使用需要通过双因素认证，进入操作智能卡的安全状态
- 信息采用文件系统进行保存，依据类型或密钥的不同，提供不同的访问操作
- 支持DES、3DES和RSA等密码算法

# 智能卡的安全特性

Contact type



Contactless type



# 单点登录

## ▶ 单点登录 (SSO, Single Sign-on)

- ▶ 用户只需在登录时进行一次注册，就可以访问多个系统，不必重复输入用户名和密码来确定身份
- ▶ 实质是安全上下文 (Security Context) 或凭证 (Credential) 在多个应用系统之间的传递或共享

## ▶ 单点登录的优点

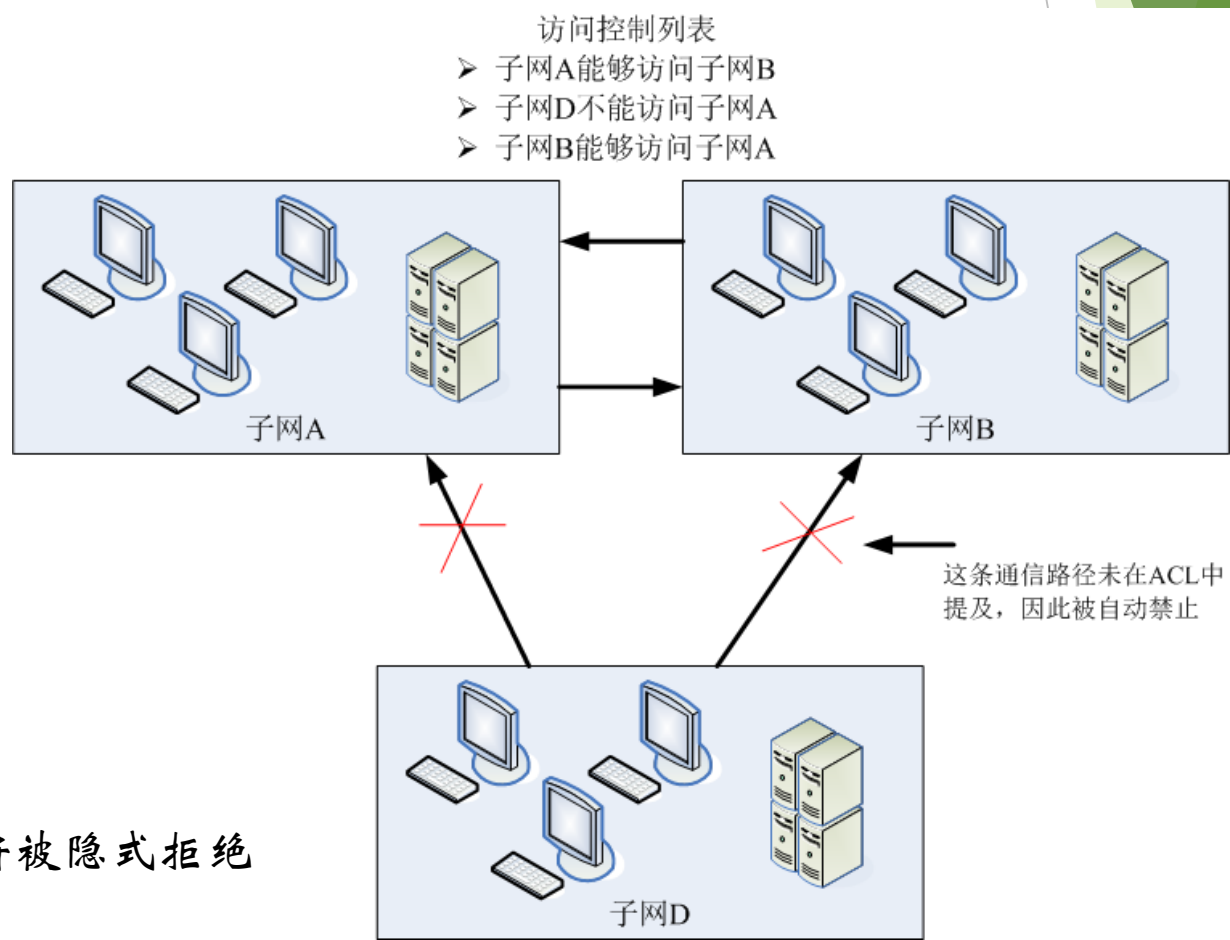
- ▶ 方便用户
- ▶ 方便管理员
- ▶ 简化应用系统开发

## ▶ 随着信息技术的广泛使用，机构员工为了完成工作通常需要访问多个不同（可能是异构的或远程）的系统，需要记住各个系统的不同账户和口令；

- ▶ 单次登录的缺点是同样给攻击者提供了便利，而且也可能是单一故障点 (single failure point)，在登录高峰期容易形成瓶颈。

# 授权

- ▶ 1、访问准则
- ▶ 2、默认为拒绝服务
- ▶ 3、知其所需

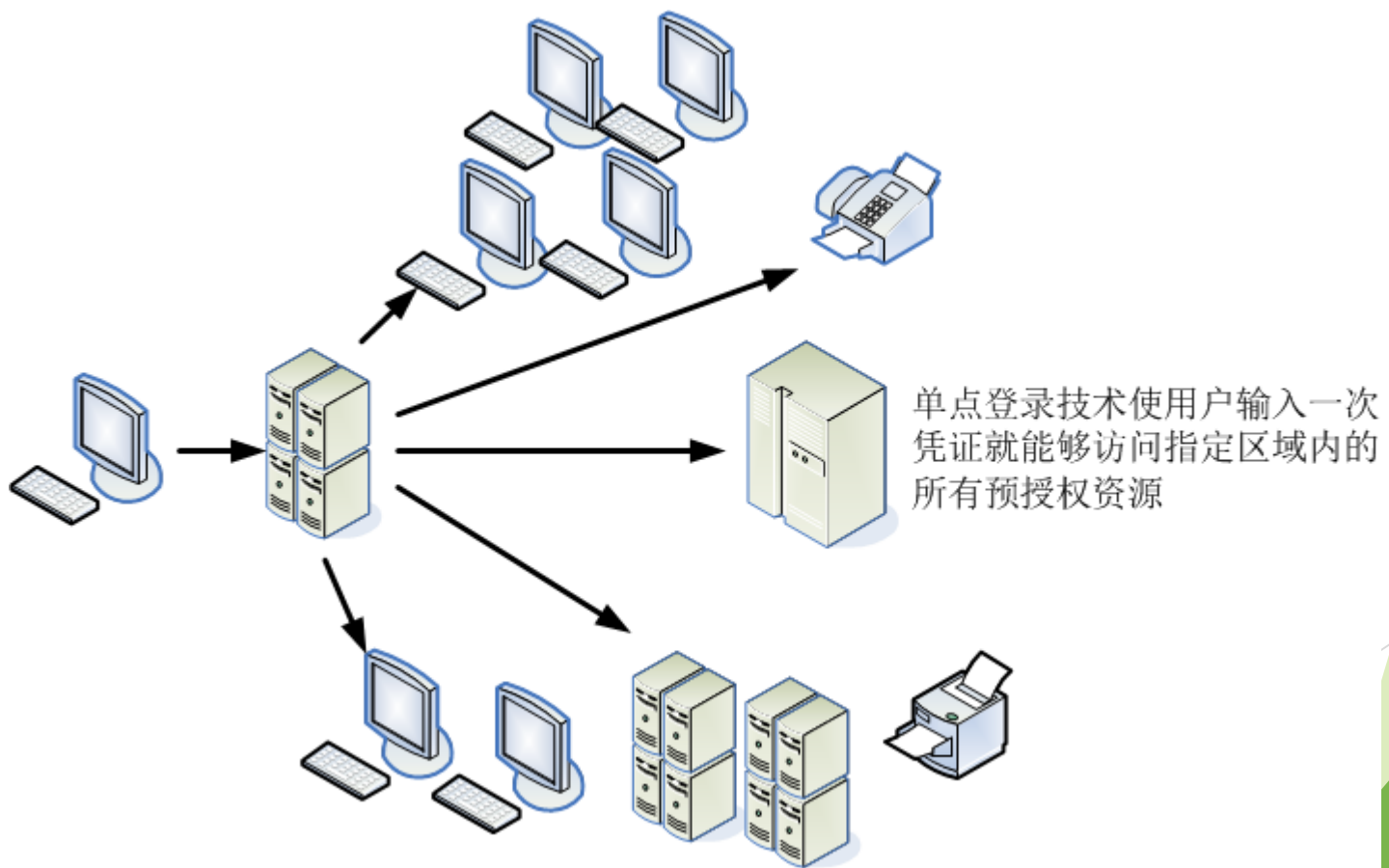


没有显示允许的访问将被隐式拒绝



# 授权

## ► 单点登录



# 访问控制部署原则

- ▶ 访问控制的目的是使适当的主体以适当的方式访问适当的客体，而阻止任何其它不适当的访问，访问的适当性主要遵循：
  - ▶ 最小特权（least privilege）原则；
  - ▶ 需知（need to know）原则；
- ▶ 不同的访问控制类型具有不同的特点，适合不同的应用环境，其特点主要表现在：
  - ▶ 控制的粒度（ fineness of granularity ）；
  - ▶ 管理的简便性（ management simplification ）。

# 分散式访问控制管理

- ▶ 域：一个信任范围，或者是共享共同安全策略的主体和客体的集合
- ▶ 每个域的访问控制与其它域保持独立
- ▶ 跨域访问必须建立信任关系，用户可以从一个域访问另一个域中的资源
- ▶ 信任可以是单向的，也可以是双向的

# 行政管理性控制

- ▶ 策略和措施

- ▶ 人员控制

- ▶ 规定雇员应当如何与安全机制交互以及处理与之相关的不服从行为

- ▶ 监管结构

- ▶ 管理层必须构造监管结构，使每位雇员都应当有一个能够汇报工作的上级，上级必须对该员工的行为负责，并形成关联关系

- ▶ 安全意识培训

- ▶ 人是最薄弱的环节

- ▶ 测试

- ▶ 所有的安全控制、机制和措施需要周期性进行测试，以确保它们合理地支持安全策略、目标和目的。

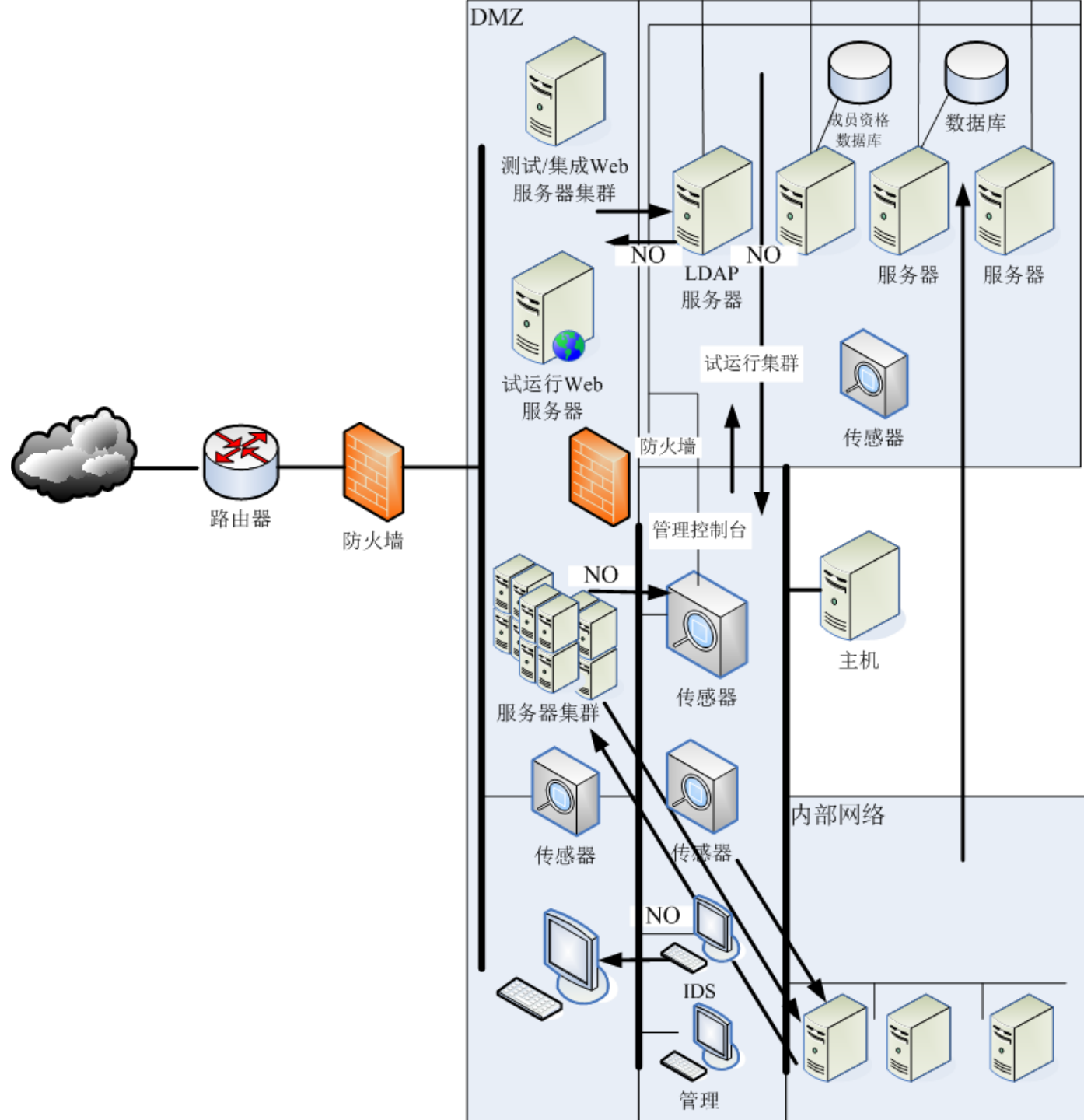
# 物理性控制

- ▶ 网络分段
  - ▶ 物理和逻辑手段
- ▶ 周边安全
  - ▶ 不同区域的访问控制
- ▶ 计算机控制
  - ▶ 计算机锁及其他物理保护手段
- ▶ 工作区分隔
  - ▶ 特定的人进入特定的区域
- ▶ 布线
  - ▶ 不同环境下的布线方式
- ▶ 控制区
  - ▶ 根据每个区域所发生活动的敏感程度分成不同的区域

# 技术性控制

- ▶ 系统访问
- ▶ 网络体系结构
- ▶ 网络访问
- ▶ 加密盒协议
- ▶ 审计

# 技术性控制



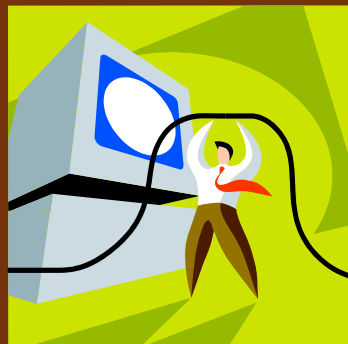
# 访问控制功能

周边安全

入侵检测系统

需要用户名和密码以进行身份验证

访问控制列表





# 访问控制功能

- ▶ 威慑：打消潜在攻击者的攻击意图
- ▶ 预防：避免事故的发生
- ▶ 纠正：在事故发生后修复组件或系统
- ▶ 恢复：将控制恢复回常规操作
- ▶ 检测：有助于标识事故和活动
- ▶ 补偿：提供备用控制措施
- ▶ 指令：根据法律或环境要求制定的强制型控制

# 物理访问控制服务

控制类型 控制类别	预防	检测	纠正	威慑	恢复	补偿
	避免意外事件的发生	标识已发生的意外事件	纠正已发生的意外事件	阻止安全违规行为	还原资源和功能	提供其他控制选择
栅栏				●		●
锁	●					●
证件系统	●					●
保安	●					●
生物测定学系统	●					●
陷阱门	●					●
照明				●		●
运动探测器		●				●
闭路电视		●				●
非现场设施					●	●

# 行政管理控制服务

控制类型 控制类别	预防	检测	纠正	威慑	恢复	补偿
	避免意外事件的发生	标识已发生的意外事件	纠正已发生的意外事件	阻止安全违规行为	还原资源 和功能	提供其他 控制选择
安全策略	●					●
监控和监督		●				●
任务分离	●					●
工作轮换		●				●
信息分类	●					●
人员措施	●					●
调查		●				●
测试	●					●
安全意识培训	●					●

# 技术方面控制服务

控制类型 控制类别	预防	检测	纠正	威慑	恢复	补偿
	避免意外事件的发生	标识已发生的意外事件	纠正已发生的意外事件	阻止安全违规行为	还原资源 和功能	提供其他 控制选择
ACL	●					●
路由器	●					●
加密	●					●
审计日志		●				●
IDS		●				●
防病毒软件	●		●			●
服务器镜像			●			●
智能卡	●					●
拨号回叫系统	●					●
数据备份					●	●

# 可问责性

## ▶ 审计要素

- ▶ 安全存储审计跟踪
- ▶ 使用适当的审计工具控制日志的大小
- ▶ 为了保护数据，日志必须不被未授权修改
- ▶ 培训合适的人员以合理方式检查数据
- ▶ 确保只有管理员才能删除日志
- ▶ 日志应当包含所有高权限帐户（根帐号、管理员）的活动

# 可问责性

## ► 事件类型

系统级事件	应用程序级事件	用户级事件
<ul style="list-style-type: none"><li>➤ 系统性能</li><li>➤ 登录尝试</li><li>➤ 登录ID</li><li>➤ 每次登录尝试的日期和时间</li><li>➤ 用户和终端的封锁</li><li>➤ 管理工具的使用</li><li>➤ 使用的设备</li><li>➤ 执行的功能</li><li>➤ 更改配置文件的请求</li></ul>	<ul style="list-style-type: none"><li>➤ 错误消息</li><li>➤ 打开和关闭的文件</li><li>➤ 文件的修改</li><li>➤ 应用程序内的安全违规</li></ul>	<ul style="list-style-type: none"><li>➤ 身份标识和身份验证尝试</li><li>➤ 使用的文件、服务和资源</li><li>➤ 运行的命令</li><li>➤ 安全违规</li></ul>

# 可问责性

- ▶ 审计信息的检查
  - ▶ 手动检查审计
  - ▶ 审计简约工具 (audit-reduction tool)，减少审计日志内信息的数量。
- ▶ 击键监控
  - ▶ 检查和记录用户在操作过程中的键盘输入的监控行为
  - ▶ 跟踪用户每次击键记录的审计过程
- ▶ 保护审计数据和日志信息
  - ▶ 只有特定的人才能查看、更改和删除审计跟踪信息

# 访问控制实践

## ► 任务计划表

- 拒绝未知用户或匿名帐户对系统的访问
- 限制和监控管理员以及其他高级帐户的访问
- 在登录尝试失败次数达到特定值后挂起或延迟访问功能
- 用户一离开公司，就立刻删除他的帐户
- 将不活动帐户挂起30-60天
- 实施严格的访问准则
- 实施“知其所需”和最小特权原则
- 禁止不必要的系统功能、服务和端口
- 更换为账户设置的默认密码
- 限制和监控全局访问规则
- 确保登录ID不是对工作职能的描述
- 删除帐户和组成员资格的多余访问规则
- 从资源访问列表中删除多余的用户ID、帐户和角色型帐户
- 实施密码轮换
- 实现密码需求（长度、内容、生命期、分发、存储和传输）
- 定期对系统、用户事件和活动进行审计，并检查相关报告
- 保护审计日志



# 信息的未授权泄露

- ▶ 客体重用

- ▶ 无意识泄露信息

- ▶ 将先前包含一个或多个客体的介质重新分配给主体。

- ▶ 敏感数据应当由数据所有者进行分类（秘密、绝密、机密、未分类等）

- ▶ 严格控制和审计数据的存储和访问方式

- ▶ 消磁

- ▶ 防止机密信息泄露的措施，它可以将介质恢复回原始状态

# 发射安全

- ▶ 电子设备中发射电子信号泄露造成的风险
  - TEMPEST 技术
    - TEMPEST (Transient Electromagnetic Pulse Emanation Surveillance Technology) 技术是电磁环境安全防护（电磁安防）的一部分，是包括了对电磁泄漏信号中所携带的敏感信息进行分析、测试、接收、还原以及防护的一系列技术，TEMPEST是一系列的构成信息安全保密领域的总称。
- ▶ 技术复杂、笨重和昂贵，因此只用于高度保护的高度敏感区域
  - ▶ 白噪声
    - ▶ 具有均匀频谱的随机电子信号
  - ▶ 控制区
    - ▶ 在某些环境的设备表面，使用特殊材料屏蔽电子信号

# 访问控制监控

网络型IDS	监控网络通信	配置为监控攻击行为、解析审计日志、终止连接、在攻击发生时向管理员报警、保护文件系统、揭示攻击者的方法、说明需要修复哪些脆弱性，甚至有助于追踪黑客
主机型IDS	分析特定计算机系统内部的活动	
知识型或特征型	特定的模型构成的示例，无法识别未知的攻击行为	检测已知攻击
状态型	在上下文中扫描攻击特征，而不仅仅是查看单个数据包 初始状态：攻击执行前的状态 侵入状态：成功渗透后的状态	
统计异常型	行为型系统 能够响应新的攻击，如：零日攻击 误报率高，容易在学习初被绕过检测	监视行为
协议异常型	基于协议异常过滤器 为每个数据包的建立和传输协议进行检测，通过过滤器整合入IDS分析网络行为	
流量异常型	通过环境基线建立监测流量异常过滤器 通过上限阈值调整减少误报和漏报，能够监测未知攻击	
规则型	IDS从传感器或日志中收集信息 推理引擎对数据应用预先编程的规则 规则匹配，IDS报警或者提供一个解决方案	
IDS传感器	分析引擎，过滤接收到的数据，抛弃无关的信息，以检测可疑的活动	
网络流量	流量超过IDS上限时攻击会被忽略	

谢谢！