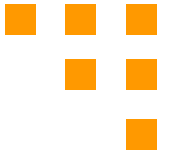
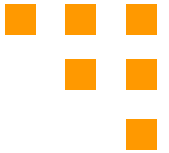


16 安全



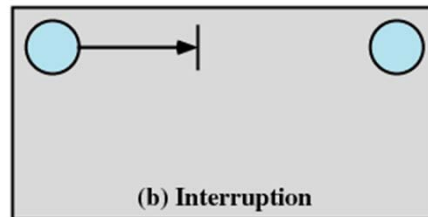
- 计算机和网络安全要求
 - 机密性;
 - 完整性;
 - 可用性;
 - 可靠性;

16 安全

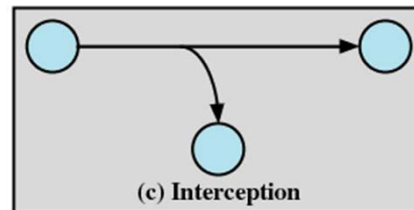


■ 威胁的类型

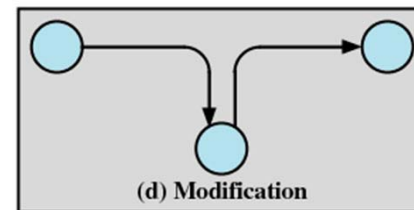
■ 中断;



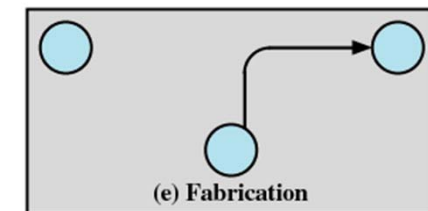
■ 侦听;



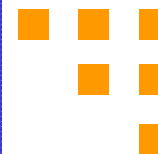
■ 更改;



■ 伪造;



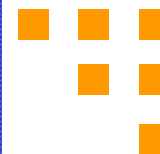
16 安全



计算机系统资源面临的威胁

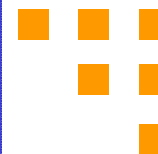
	可 用 性	机 密 性	完整性/ 可靠性
硬件	设备被偷或破坏，故拒绝服务		
软件	程序被删除，故拒绝用户访问	非授权的软件拷贝	工作程序被更改，导致在执行期间出现故障，或执行一些非预期的任务
数据	文件被删除，故拒绝用户访问	非授权读数据。通过对统计数据 的分析揭示了潜在的数据	现有的文件被修改，或伪造新的文件
通讯 线路	消息被破坏或删除，通讯线路 或网络不可用	读消息；观察消息的流向规律	消息被更改、延迟、重排序，伪造假消息

16 安全



- 被动攻击是对传输过程进行窃听或截取，目的是非法获得正在传输的信息，了解其内容和数据性质。包括两种威胁：释放消息内容和通信分析。
- 主动攻击不但截获数据，还冒充用户对系统中的数据进行修改、删除或生成伪造数据，可分为伪装、重放、更改信息和拒绝服务。

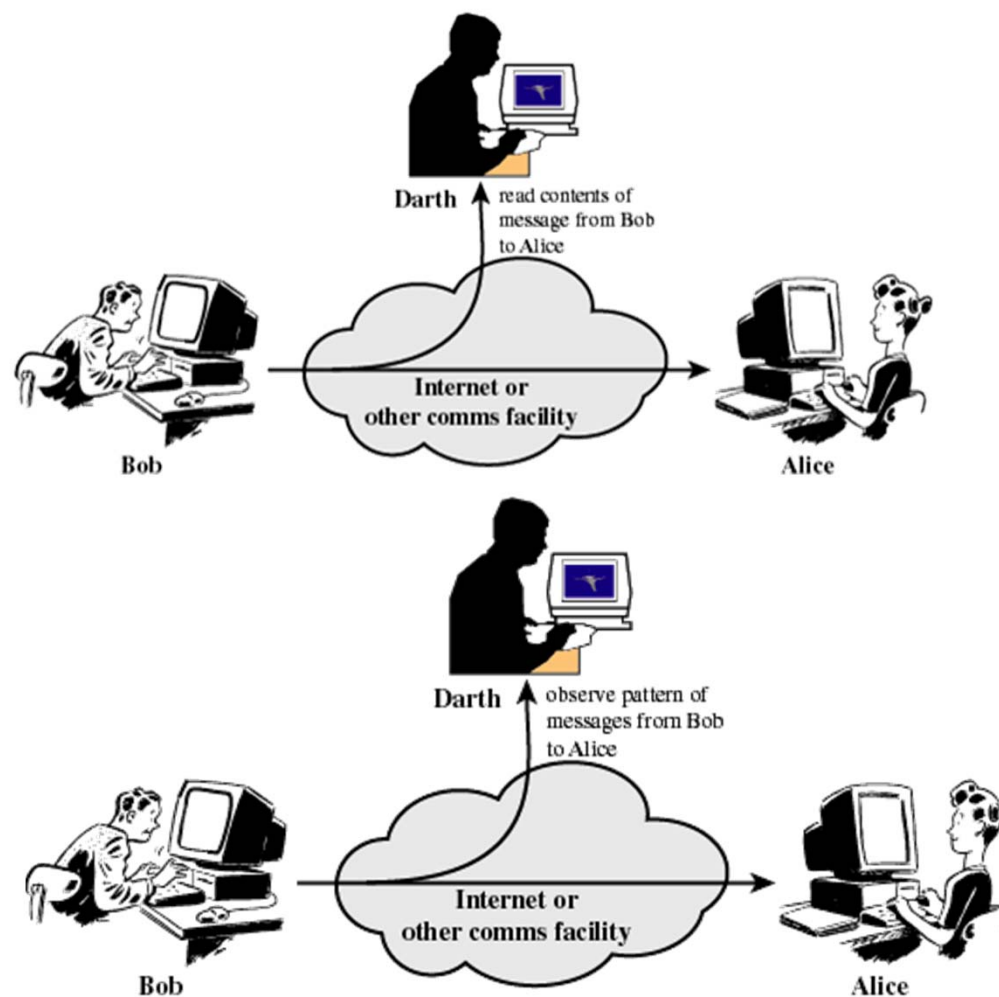
16 安全



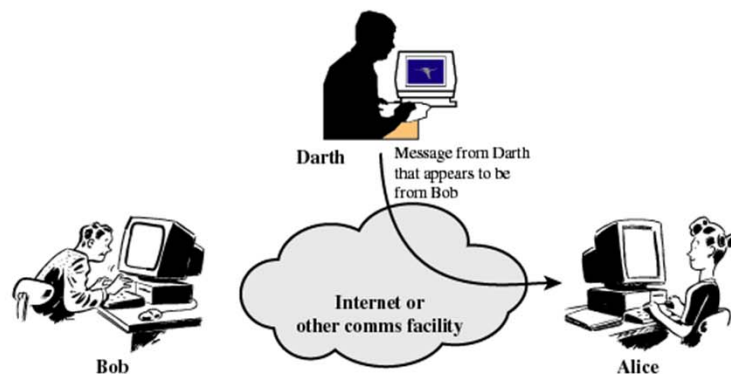
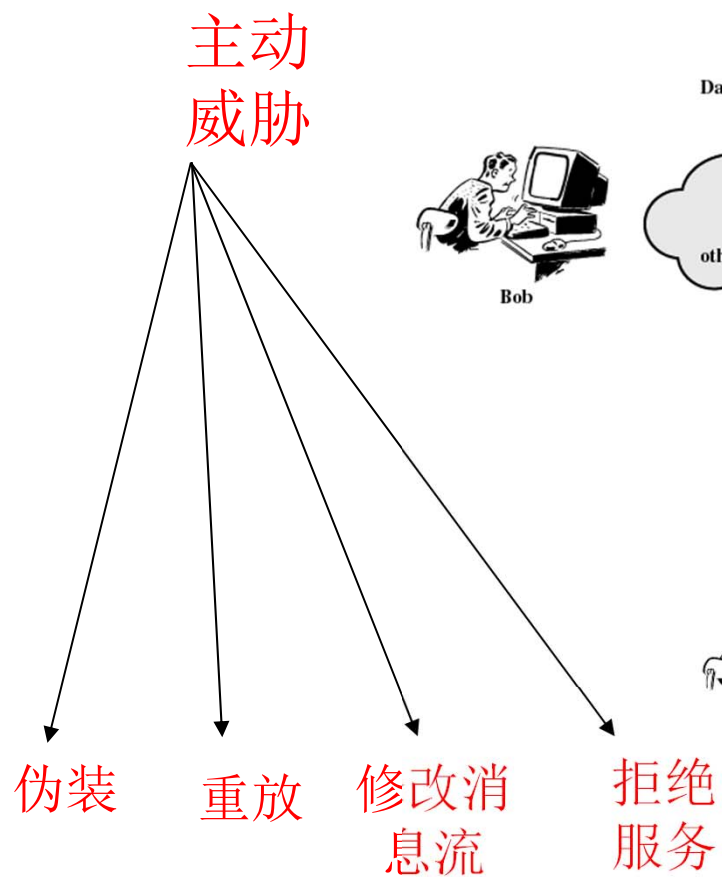
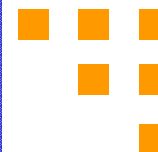
被动
威胁

消息内
容泄漏

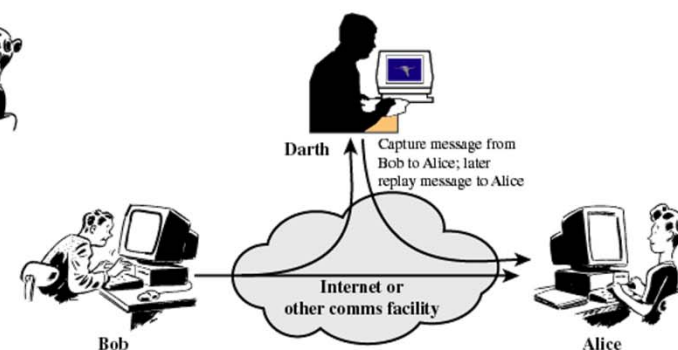
消息流
量分析



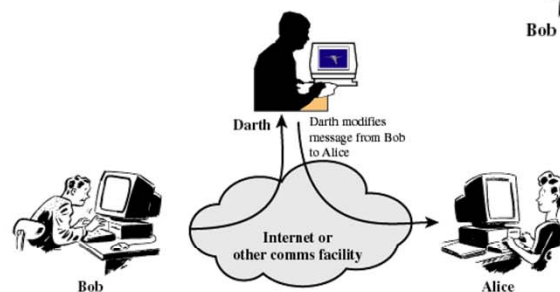
16 安全



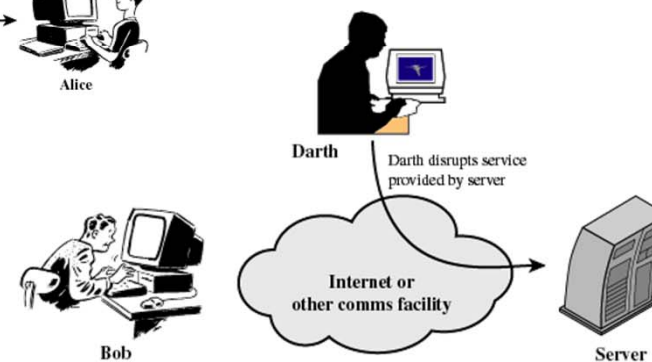
(a) Masquerade



(b) Replay

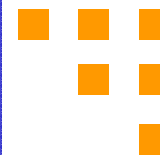


(c) Modification of messages



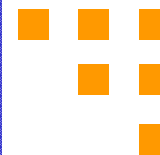
(d) Denial of service

保 护



1. 操作系统保护层次
2. 内存储器的保护
3. 面向用户的访问控制
4. 面向数据的访问控制

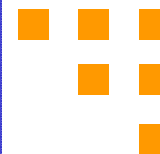
操作系统保护层次



多道程序设计技术共享资源引起资源保护的需
要和保护层次：

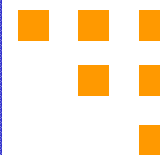
- 无保护：
- 隔离：
- 全部共享或不共享：
- 通过访问控制的共享：
- 通过权能的共享：
- 限制对象的使用：

内存存储器的保护



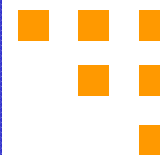
- 多道程序设计环境中，主存储器保护的重要性。
- 进程的存储空间分离可通过虚存方法来实现，分段、分页，或两者的结合，提供了管理主存的一种有效的方法。

面向用户的访问控制(1)



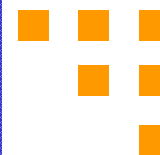
- 在数据处理系统中访问控制所采取的方法有两类：与用户有关的和与数据有关的。
- 用户访问控制普遍技术是用户登录，需要一个用户标识符（ID）和一个口令。
- ID/口令文件容易遭到攻击。

面向用户的访问控制(2)



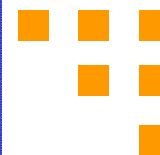
- 通信网络中的用户存取控制问题
- 分布式环境中的用户访问控制问题
- 网络中使用两级访问控制

面向数据的访问控制(1)



- 成功登录后，对数据库中机密数据的访问，通过用户访问控制过程进行验证。
- 一个权限表与每个用户相关，指明用户被许可的合法操作和文件访问，系统基于用户权限表进行访问控制。
- 数据库管理系统必须控制对特定的记录甚至记录的某些部分的存取，这个问题需要更多细节层次。

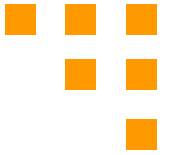
面向数据的访问控制(2)



访问控制的通用模型是访问矩阵，模型的基本要素：

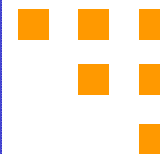
- 主体(Subject):
- 客体(Object):
- 访问权(Access Authority):

入侵者



1. 入侵技术
2. 口令保护
3. 入侵检测

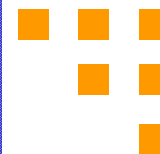
入侵技术(1)



Anderson标识了三种类型的入侵者：

- 伪装者（masquerader）：
- 违法行为者（misfeasor）：
- 秘密的用户（clandestine user）：

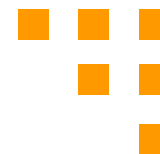
入侵技术(2)



口令文件的保护可采取下列方式之一：

- 单向加密：系统存储的仅仅是加密形式的用户口令。
- 访问控制：对口令文件的访问被局限于一个或非常少的几个账号。

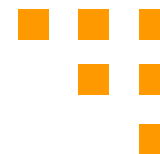
入侵技术(3) 入侵者获悉口令的技术



1. 尝试标准描述使用的缺省口令试猜。
2. 试遍所有短口令（1到3个字符）。
3. 尝试系统联机字典中的单词或可能的口令表中的词试猜。
4. 收集用户信息
5. 尝试用户的电话号码，身份证号和房间号。
6. 尝试该地区的所有合法牌照号码。
7. 使用特洛伊木马绕过对访问的限制。
8. 窃听远程用户和主机系统间的线路。

两种主要对策：预防与检测

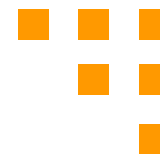
口令保护



系统的第一条防线是口令系统，ID在下列情况中提供安全性：

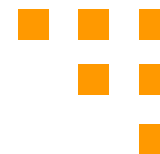
- ID用来确定用户是否有权获得访问系统。
- ID确定用户权限。
- ID可用于自由决定的访问控制。

UNIX口令方案(1)



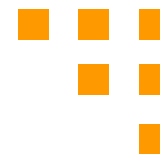
- 加密例程crypt(3) 基于DES算法，
- 使用12位的“salt”值修改，这个值与将口令分派给用户的时间有关。
- 算法的输出作为下一次加密的输入，过程重复共进行25次。
- 64位输出转化为11个字符的序列。密文口令与salt的明文副本一起被存在口令文件中，用作相应的用户ID。

口令文件访问控制



阻止口令攻击的一个方法是**不让对手访问口令文件**，如果口令文件中的口令密文只能被特权用户访问，那么，攻击者不知道特权用户的口令就不能读口令文件。

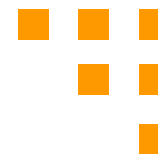
口令选择策略



用户选择口令可使用4种基本方法：

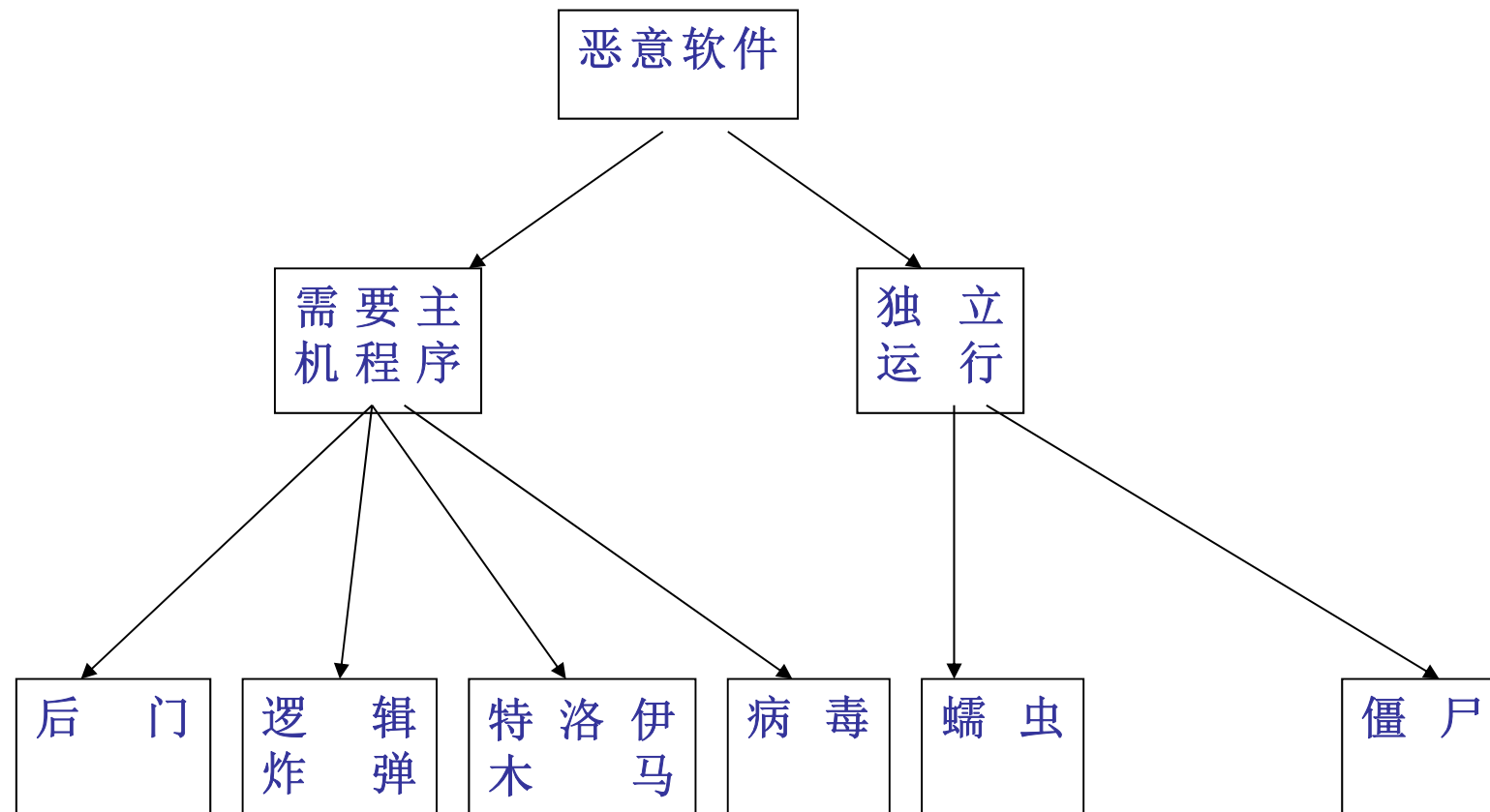
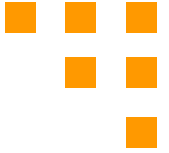
- a. 用户教育
- b. 计算机生成的口令
- c. 口令生效后检测
- d. 口令生效前检测

恶意软件

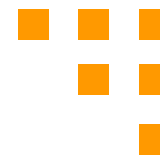


- a. 病毒及其威胁
- b. 病毒的特性
- c. 病毒的类型
- d. 反病毒的方法
- e. 电子邮件病毒

恶意软件分类



病毒的本质

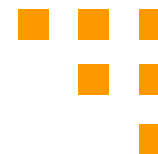


a. 病毒的执行过程:

b. 病毒的生命周期:

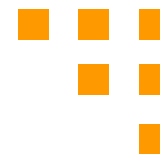
- 潜伏阶段
- 传播阶段
- 触发阶段
- 执行阶段

病毒的类型



- 寄生病毒：
- 常驻内存病毒：
- 引导扇区病毒：
- 隐蔽的病毒：
- 多态病毒：
- 宏病毒：

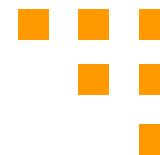
反病毒的方法(1)



解决病毒威胁的办法:

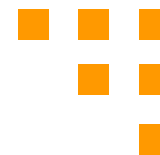
- 预防。
- 另一个方法是:
 - 检测:
 - 识别:
 - 删除:

反病毒的方法



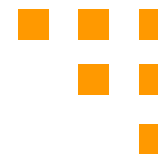
- a. 数字免疫系统原理:
- b. 数字免疫系统系统结构:
- c. 数字免疫系统操作步骤:

电子邮件病毒



- 新一代恶意软件通过电子邮件到达，或者使用电子邮件软件特征在Internet上复制自己。只要通过打开电子邮件附件，或者通过打开电子邮件激活病毒，就开始把自身传播到被感染的主机所知道的所有电子邮件地址中去。

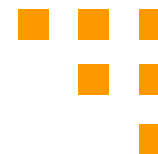
Windows 2000的安全



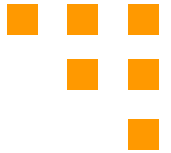
提供全面、可配置的C2级安全性服务。1995年，两个独立配置的Windows NT Server和Windows NT Workstation 3.5得到美国国家计算机安全中心NCSC的C2级认证。

安全级别	各商用操作系统的安全级别
D级，最低安全性；	DOS
C1级，主存取控制；	
C2级，较完善的自主存取控制（DAC）、审计；	sco open server 、 windows NT、 solaris、 hp-ux、 aix
B1级，强制存取控制（MAC）；	osf/1
B2级，良好的结构化设计、形式化安全模型；	
B3级，全面的访问控制、可信恢复；	
A1级，形式化认证。	

访问控制方案(1)



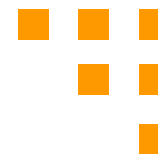
- 用户登录时，使用名字/口令来验证。如果可接受登录，则为该用户创建一个进程，同时有一个访问令牌与这个进程对象相关联。
- 访问令牌包括安全ID（SID），它是基于安全目的，系统所知道的这个用户的标识符。
- 用户进程派生出任何一个额外进程时，新的进程对象继承了同一个访问令牌。



访问控制方案(2) 访问令牌两种用途

- 负责协调所有必需的安全信息，加速访问确定。当一个用户进程试图访问时，安全子系统使用与该进程相关联的访问令牌来确定用户的访问特权。
- 允许每个进程以受限的方式修改自己的安全特性，而不会影响代表用户运行的其他进程。

访问令牌



WINDOWS 2000安全结构

安全ID
组ID
特权
默认所有者
默认ACL

(a) 访问令牌

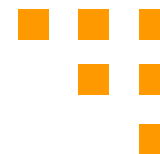
标记
所有者
系统访问控制表 (SACL)
自由访问控制表 (DACL)

(b) 安全描述符

ACL头
ACE头
访问掩码
SID
ACL头
ACE头
访问掩码
SID
.
.

(c) 访问控制表

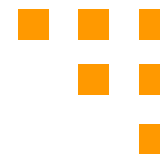
安全描述符(1)



安全描述符的一般结构

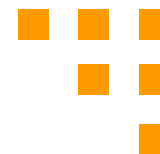
- 标记:
- 所有者:
- 系统访问控制表 (SACL):
- 自由访问控制表 (DACL)

安全描述符(2)

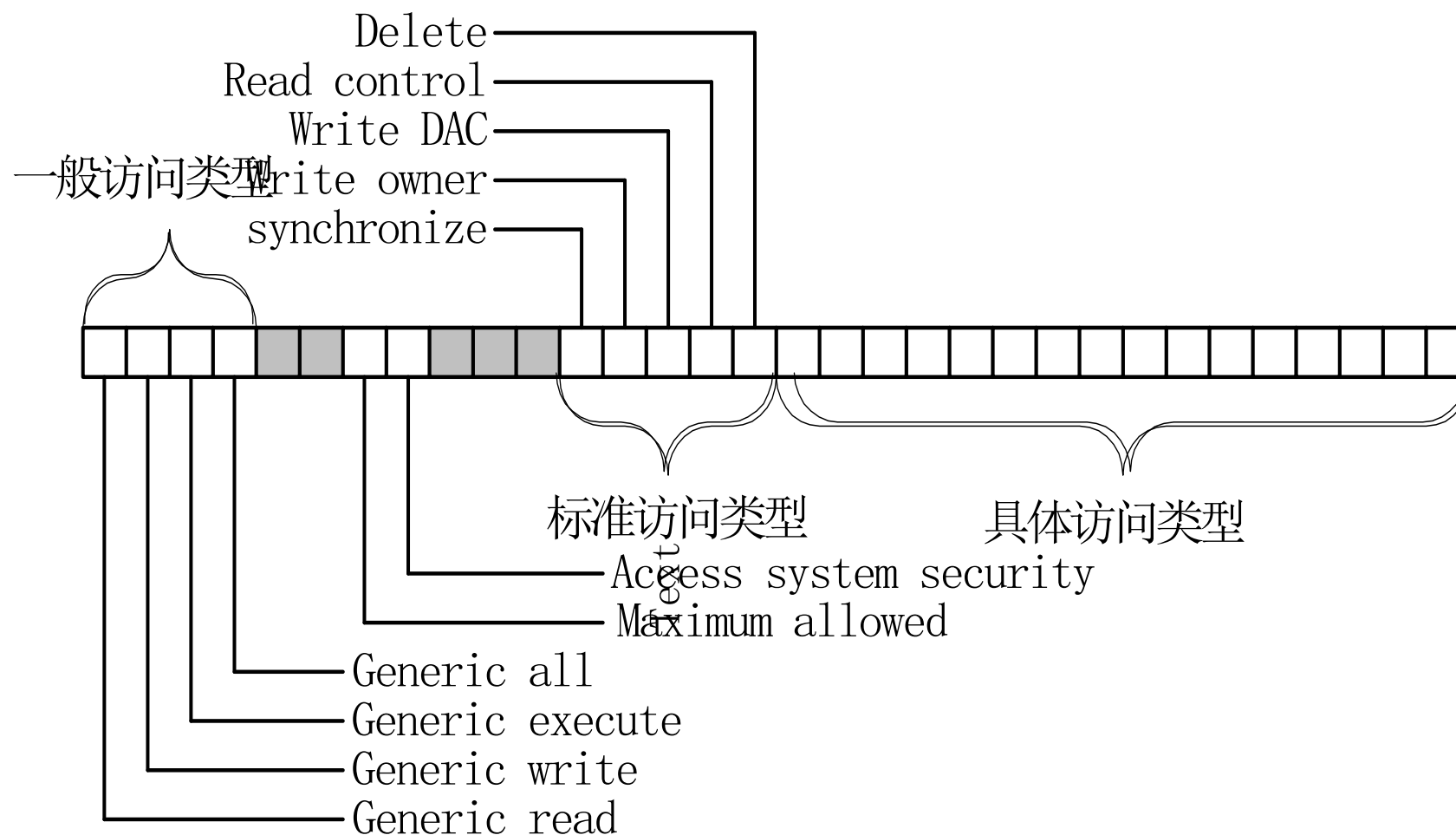


- 访问控制表是访问控制机制的核心。每个表由表头和许多访问控制项组成。每项定义一个个人SID或组SID，访问掩码定义了该SID被授予的权限。
- 当进程访问对象时，对象管理程序从访问令牌中读取SID和组SID，扫描该对象的DACL。如果发现有匹配项，即找到一个ACE，它的SID与访问令牌中的某SID匹配，该进程具有该ACE的访问掩码所确定的访问权限。

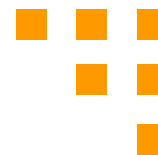
安全描述符(3)



访问掩码的内容

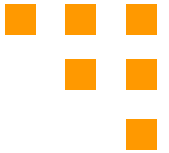


安全描述符(4)



- 安全机制的重要特征是应用程序可以为用
户定义的对象使用安全框架，例如，数据
库服务器可以创建自己的安全描述符，并
把它们附加在数据库的某一部分。
- 除普通的读/写访问约束，服务器还可设置
数据库专用的安全机制，如在一个结果集
合中滚动或执行连接操作。服务器负责定
义具体权限的含义，并执行访问检查。

小结



- 各种类型的安全威胁;
- 安全保护
 - 内存保护
 - 访问控制
- 恶意软件
- 可信系统