### 访问控制

访问控制 ： 授予或拒绝下列特定要求的过程

1 . 获得并使用信息及相关信息处理服务

2 . 进入特定物理设施

访问控制基本安全要求

|  |
| --- |
| 限制信息系统对授权用户，代表授权用户的进程或设备的访问 |
| 限制信息系统对各种类型的事务和授权用户允许执行的功能的访问 |

|  |
| --- |
| 根据批准的授权控制CUI流 |
| 分离个人职责以减少不共谋的恶意活动的风险 |
| 采用最小权限原则 |
| 访问非安全功能的时候，使用特权账号 |
| 阻止非特权用户执行特权功能 |
| 限制不成功的登录 |
| 提供与合适的CUI规则一致的隐私和安全注意事项 |
| 使用带有模式隐藏显示的会话锁 以防止在为活动期间访问和查看数据 |
| 在定义的条件后自动终止一个用户会话 |
| .... |
| .... |

访问控制策略

1 . 自主访问控制 ：基于请求者的身份和访问规则控制访问 一个实体基于自己的抑制授予另一个实体访问某些资源的权限

2 . 强制访问控制 ：通过比较具有安全许可的安全标记控制访问 ，具有访问某种资源的许可的实体不能按其意志访问那些资源的权限

3 . 基于角色的访问控制

4 . 基于属性的访问控制

访问控制的基本元素 主体 客体 访问权

主体 ： 所有者 组 世界

客体 ： 外界对其访问受到控制的资源

访问权 ：读 写 执行 删除 创建 搜索

访问矩阵

按列分解 生成访问控制表 提供了一个指定资源的信息

按行分解 生成能力权证 指定一个用户的授权客体和操作

4.3.1 一个访问控制模型

4.5 基于角色的访问控制

传统的DAC（自动访问控制）定义了单独用户和用户组的访问权。然而基于角色的访问控制规定了不同的角色 为不同的角色分配不同的访问权 然后为用户和用户组分配角色

用户与角色是多对多的，动态的

RBAC0 -- 基本模型

RBAC1 -- 角色层次 ：角色层次提供了一种反映组织中角色层次结构的方式 下级岗位的访问权可能是上级岗位访问权的一个子集

约束 -- RBAC2 ：对安全策略一些细节的调整

|  |  |
| --- | --- |
| 互斥角色 | 一个用户只能被分配给集合中的一个角色 |
| 基数 | 约束用户的最大角色数，角色的最大用户数 |
| 先决条件 |  |