1.DAC是以用户或者用户组为主体来访问客体的，每个用户或用户组有一定的权限来访问特定的客体，且可以自主地把拥有的访问权限授予其他用户。

而MAC是为主体和客体分配了不同的安全级别属性，通过设置的访问规则如向下读、向上写来控制主体对客体的访问操作，故权限没办法从一个主体转移到另一个主体。

2.组一般是由有某些相同特质的用户组成集合，可以为一个组赋予权限从而使得组内的成员获得该组的权限。

而角色是一个行为和责任的集合，代表了一定的权限，实现了权限和用户分离，所以可以将角色分配给用户或者组，使得用户或组内的用户获得该角色拥有的能力和责任。

组主要指用户的集合，而角色代表了责任和能力。

3.Windows系统的安全体系结构包括用户认证、访问控制和加密、管理和审计、安全策略。

Windows系统安全开始于用户认证。加密保证了系统与用户之间的通信及数据存储的机密性。访问控制则维护了用户访问的授权原则。

审计和管理处于系统的内核层。审计可以发现系统是否曾经遭受过攻击或正在遭受攻击，并进行追查；管理则是为用户有效控制系统提供功能接口。