HW6

PB17111614 王嵘晟

1、TCB可信计算基TCB，一个计算机系统中的保护机制的全体，共同负责实施一个安全策略。
TCB由在一个产品或系统上共同实施一个统一的安全策略的一个或多个组件构成。
成分：固件和硬件：CPU、内存、寄存器、I/O设备等，与安全策略相关的文件
负责安全管理的人员、安全核、具有特权的进程或命令

2、操作系统分层次结构，分层可以隔离运行域以起到保护作用。而运行之域可看作层次决定特权的同心圆，在越靠中心特权越高，使用等级之域机制以做到运行域保护。

3、最小特权：指在完成某种操作时授予每个主体（用户/进程）必不可少的特权。系统对给用户执行任务所需的最少特权，仅供完成当前任务。

4、①云存储平台安全机制是保护整个云存储平台系统自身的安全，主要两个技术：密码技术，加固技术
②云存储管控安全机制主要解决安全管理的问题，包括对云节点服务器密钥统一管理，密钥生命周期可控制性、云数据接口/云客户端密钥的自主性，
③云存储应用安全机制：存储加密，备份加密，交换加密，身份认证与访问控制，主机安全，手机安全，云端数据库

5、A. 首先建立信任根，可信性由物理安全、技术安全、管理安全共同确保
B. 再建立一条信任链，从信任根到硬件平台到操作系统再到应用。