信息安全导论第六次作业

PB17151767 焦培淇

1. TCB(可信计算基)是一个计算机系统中的保护机制的全体,它们共同负责实施一个安全策略,包括硬件,固件和软件。

构成:①固件与硬件:包括CPU,内存,寄存器和I/O设备等;

②与安全策略相关的文件,比如安全策略库,标识与鉴别库等;

③负责安全管理的人员;

④安全核:为整个操作系统提供安全基础机制;

⑤具有特权的进程或命令。

2. 运行域是进程运行的区域,运行域保护的思想是对整个系统空间进行分层设计,隔离不同进程的运行域,通过一个进程与中心的接近程度来决定是其可访问与访问权限,从而达到运行域保护的目的。

3. 最小特权原则指的是系统只给用户执行任务所需的最少的特权,也就是用户所得到的特权仅能完成当前任务。

4. 云存储安全机制可以简单归纳为3方面

①云存储平台安全机制:保护整个云存储平台系统自身的安全,其中主要有密码技术与加固技术;

②云存储管控安全机制:包括云节点服务器密钥的统一管理、密钥周期的可控性、云数据接口/云客户端密钥的周期性自主性等;

③云存储应用安全机制

5. 可信计算的基本思想是通过提高主机的安全性，以从终端源头控制绝大多数不安全因素。对于计算机系统来说，包括芯片、主板、操作系统开始，综合采取措施，才能提高其安全性。