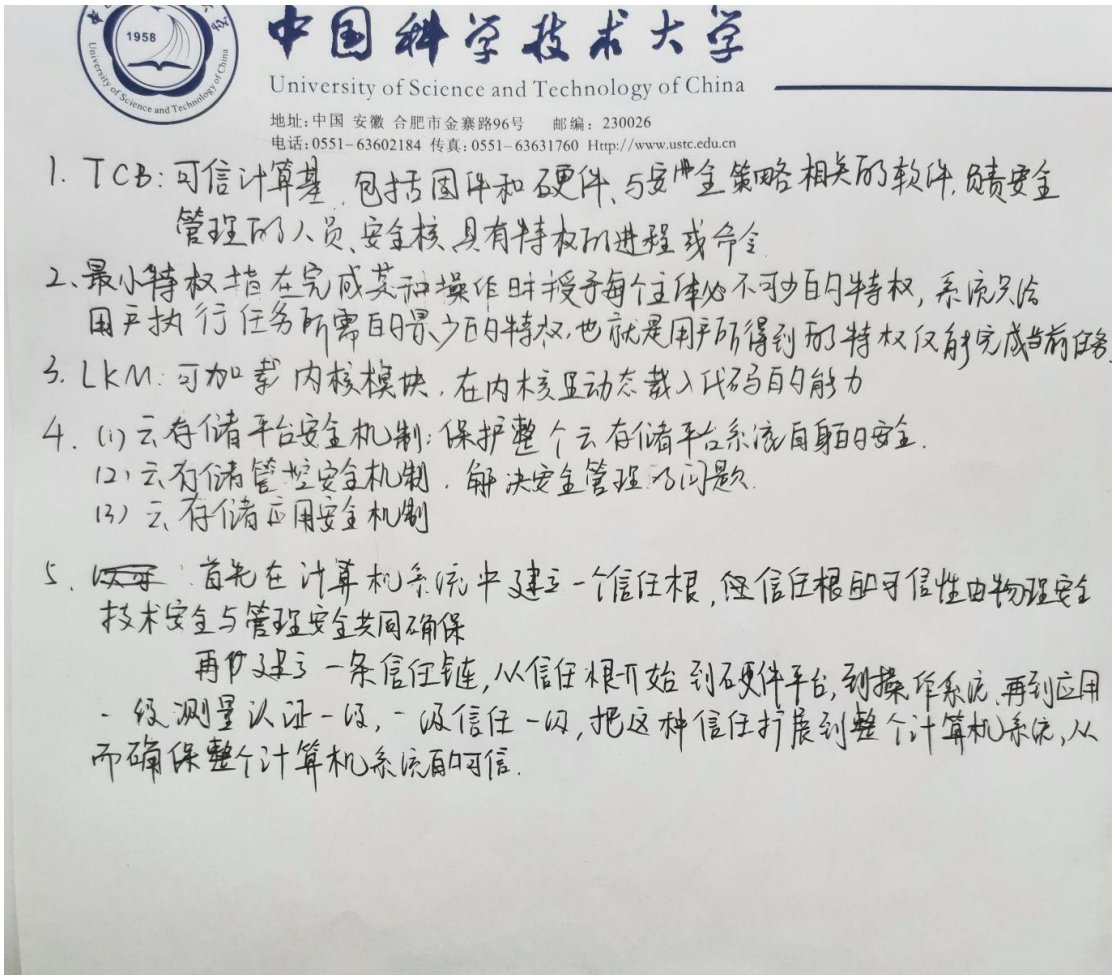
作业六

PB19111708 杨云皓



中国科学技术大学
University of Science and Technology of China
地址：中国 安徽 合肥市金寨路96号 邮编：230026
电话：0551-63602184 传真：0551-63631760 Http://www.ustc.edu.cn

1. TCB：可信计算基，包括固件和硬件、与安全策略相关的软件，负责安全管理的人员、安全核，具有特权的进程或命令。
2. 最小特权指在完成某种操作时授予每个主体必不可少的特权，系统允许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。
3. LKM：可加载内核模块，在内核里动态载入代码的能力
4. (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。
   (2) 云存储管控安全机制，解决安全管理的问题。
   (3) 云存储应用安全机制
5. ~~以太~~ 首先在计算机系统中建立一个信任根，此信任根的可信性由物理安全技术安全与管理安全共同确保
   再构建起一条信任链，从信任根开始到硬件平台，到操作系统，再到应用，一级测量认证一级，一级信任一级，把这种信任扩展到整个计算机系统，从而确保整个计算机系统的可信。