软件调试学习笔记

CPU的操作模式：

1. 保护模式：段的保护机制和页的保护机制。
2. 实模式：可以直接访问物理内存和I/O空间。
3. 虚拟8086模式：保护模式下用于执行8086程序的准模式， 通过该模式可以将8086程序当做保护模式的一项任务来执行。
4. 系统管理模式：用于系统固件指向电源管理，安全检查和平台相关的特殊任务，当CPU的系统管理终端管脚(SMI#)被激活，处理器将上下文保存，然后切换到另一个单独的地址空间中执行专门的SMM例程，SMM例程通过RSM指令是处理器退出SMM模式并恢复到系统管理中断前的状态。感觉与VT技术有点像。
5. IA-32e模式：应用程序可以是32位也可以是64位，内核和驱动程序必须是64位，也就是说如果为32位应用程序，在进入系统内核时会从32位切换到64位，从内核返回时再从64位切换回32位。

CPU模式之前的转换：

//todo

处理器通电开始运行或复位后处于实模式，CR0控制寄存器的PE(Protection Enable)标志用来控制处理器是处于实模式还是保护模式。EFLAGS标志寄存器的VM标志用来控制是在虚拟8086模式还是保护模式(之前在逆向函数过程中, 会经常看见对应标志位)，EFER寄存器(Extend Feature Register)的LME(Long Mode Enable)用来启用IA-32e模式.

进程资源：

1. 虚拟地址空间
2. 进程ID
3. 可执行文件镜像
4. EPROCESS结构体
5. 一个或者多个线程
6. 进程句柄表
7. CR3页目录基地址
8. PEB
9. 访问令牌

使用命令：

.process PID(代表所有进程) 0(代表要显示进程的属性) + [过滤条件]

ex: .process 0 0 notepad.exe

进程Session ID, 是指该进程所在的windows会话(session id)的ID号，当有多个用户同时登录时，windows会为每个登录用户建立一个会话，每个会话有自己的Work Station和 Desktop。

windows XP, 当只有一个用户登录时，用户启动的程序和系统服务程序都运行在session 0。当切换到另一个用户后，系统会建立session 1。从Vista之后(server 2003, windows 7及之后)，

系统服务运行在session 0，当用户登录后，会创建另一个会话session 1, 在任务管理器可以看到两个CSRSS进程在运行。特殊的系统进程不属于任何会话。

CR3(页目录基地址), X86(XP, 7, 8, 10等)下使用2-9-9-12(32位)分页模式，X64下使用9-9-9-9-12分页模式(48位)，如图所示：