虚拟机保护技术就是将基于x86汇编系统的可执行代码转换为字节码指令系统的代码，以达到保护原有指令不被轻易逆向和篡改。

目标，设计软件，通过添加一个vm section，修改软件中注册部分就调用这个section的函数进行处理，达到加密的目的

初步构思：

第一期:设计好VM

1.初步设计

Vm的过程还比较简单，先设计start\_vm->vm\_dispatch->vm\_handler

先设计下start\_vm

再设计vm\_dispatch

最后设计对应的指令解析vm\_handler

2.重点是vm指令设计

vm的核心就是这些指令翻译了

vm\_handler,要实现尽可能多的指令设计

常见的汇编指令add/sub，jmp，ja，jae，jb等等一系列都要进行指令设计，还有异常的模拟，这是比较有难度的，避免直接出现这些指令，尽可能达到注册机制的保护

指令按功能可以分为4类:

3.反汇编引擎的使用

还必须把80x86指令转换为字节码，需要用到反汇编引擎，初步设定为使用OD里头的开源反汇编引擎

以上这几三部分先开始，需要用到3个周的时候

第二期:设计VM section，构思中

理解软件中section如何合理安排使用

第三期:beta软件的设计，构思中

实际添加这个section并将能够对软件进行保护