一、调研资料的准备

目前的ROP攻击防御机制可粗略分为5种：控制流完整性检测；动态/静态指令检测；用户输入扫描；指令重构；内存随机化。我所设计的题目属于第二类中的动态指令检测，即：在程序运行时动态地检测指令，并根据获取的信息判断程序行为是否为ROP攻击。

二、设计目的

本题目中采取了基于二进制插桩框架的动态检测方法，目的在于检测并防御所有类型的ROP攻击，并在程序遭到ROP攻击时及时关闭程序，防止损失。此外，由于动态检测的缘故，必然会导致程序运行放缓，因此本题目设计的另外一个目的是尽可能的减小这种副作用。

三、设计要求

检测现有的各种ROP攻击及其变种

检测到攻击后，采取防御措施

无误报

四、设计思路

静态收集程序所用的函数地址，即合法地址集合，记为setF，程序运行时，动态检测ret,jmp,call的目标地址，若不在setF中，即不是正常函数入口，则判定为gadget。

五、预期成果

实现上述系统，并取得尽可能小的系统开销。

六、任务完成的阶段内容及时间安排

寒假：查阅资料，了解ROP攻击及其变种，并归纳总结其特点，了解现有的ROP攻击及其变种的检测方法。

三月：熟悉动态插桩工具PIN的使用方法，初步系统实现。

四月：调试、优化，完成原型系统。

七、完成设计（论文）所具备的条件因素

实验所需的环境，可以通过搭建虚拟机实现。检测工具可在PIN框架下运行。演示ROP攻防御效果，需要准备攻击素材，我在本科期间曾参加过信息安全类的竞赛，专攻二进制安全，在此期间，我积累了丰富的ROP攻击案例，可作为展示素材。