1. 研究背景

。

ROP（Return-Oriented Programming，面向返回编程）：是一种利用代码复用技术的攻击方法。攻击者扫描已有的动态链接库和可执行文件，提取出可以利用的指令片段（gadget），这些指令片段均已ret指令结尾，即用ret指令实现指令片段执行流的链接。操作系统通过栈来进行函数的调用和返回。函数的调用和返回就是通过压栈和出栈来实现的。每个程序都会维护一个程序运行栈，栈为所有函数共享，每次函数调用，系统会分配一个栈桢给当前被调用函数，用于参数的传递、局部变量的维护、返回地址的填入等。ROP攻击就是利用以ret结尾的程序片段，操作这些栈桢相关的寄存器，控制程序的流程，执行相应的gadget，实施攻击者预设的目标。

ROP攻击利用系统中可以利用的指令片段来完成，这些指令片段称为gadget。

CFI（Contro-Flow Integrity，控制流完整性）：通过限制控制流转移的目标来检测控制流劫持攻击。在控制流劫持攻击中，攻击者将程序的控制流重定向到不会到达正常执行的位置。CFI方法通过运行时监控程序的执行、并将其状态与预先设定好的CFG的路径对比来将程序的控制流限制到有效的执行轨迹中。如果检测到一种无效状态，就会发出警告，通常是终止程序的执行。CFG（Control-Flow Graph）通常通过源码分析、二进制分析或者执行剖析得到。

PMU（Performance Monitoring Unit，性能监控单元）：是Intel引入的用于记录处理器事件的功能单元。PMU事件有好几百个，包含了处理器在运行过程中可能遇到的所有情形，例如指令计数、浮点运算指令计数、L2缓存未命中的时钟周期、分支预测失败事件等。

BPU（Branch Processing Unit，分支处理单元）：是PMU中专门对分支事件进行处理的单元。分支指令通常是一个逻辑的指令，或者是一个循环的终点，常会伴随内存跳跃指令来执行。BPU会预测每个分支处理的结果。

PMI（Performance Monitoring Interrupt，性能监视器中断）：是性能监控单元PMU产生的中断。PMU中的计数器都是固定大小的(32位/64位取决于CPU的体系结构)，当计数器上溢时，就会产生性能监控中断。

LBR（Last Branch Record，最近分支记录）是Intel提供的一组用于记录和追踪程序最近的若干次跳转信息的循环寄存器组，这些寄存器的数量与Intel处理器的微架构相关，在早几年的Haswell架构中有16个这样的寄存器，也就是说可以记录程序最近的16条跳转指令的信息(包括从哪跳转过来的，将要跳转到哪去)，而在最新的Skylake架构中有32个。LBR寄存器的强大之处在于其定制性很强，能够过滤掉一些不重要的跳转指令，而保留需要重点关注的跳转指令。