IRSB Recovery

前言

本项目来源于我正在进行的另一项目。本项目为辅助动态符号执行分析的工具和动态符号执行功能拓展工具。本项目初衷为编写angr分析器的plugin，但是angr没有提供所有满足条件的接口，并且考虑到学习和调试成本较高，因此改用moneypatch的方式实现替换分析块的功能。并且由于是辅助研究的工具，而且没有开发完毕，故而没有进行封装。

实现功能

1. 提供process(heavyvex\_mixin)/syscall/unicorn/heavy/failure/hooks/track/soot等模块（即所有的IR处理模块）及其子模块的修改接口。
2. 提供分析功能，配合功能1可以对angr的IR块分析速度进行精准测量。
3. 提供由IRSB.statements.\_\_str\_\_格式向IRSB格式转化的功能。（\*）这个功能需要根据格式微调才能使用。这个功能支持由GPT3.5/GPT4o产生的主要返回格式。
4. 提供简易访问器，只需将需要分析的文件置于工作目录，就可以批量读取和显示信息。

文件结构

Invert.py IRSBstr->IRSB转化程序

Measure4\_targetonly.py hook接口（\*）和测量程序

IRSBout\_multi.py 批量化读取程序

Test.py Invert.py调试程序