Lab3 解题报告

冯友和、赵培宇、李越洋

1 团队分工

冯友和：提供思路并代码实现。赵培宇，李越洋：负责代码的调试以及效率测试。

2 基本思路

先通过完全随机变异 fuzzer 找到若干覆盖率较高的输入，对这些输入通过静态分析的方法寻找出若干最具变异价值的字节，并尽可能对每个字节分析最有效率的变异策略。

然后优化 Mutate 函数的机制，把完全随机变异替换为对若干关键字节的策略性变异，以获得较高的稳定性和高效率。

3 Mutate

采取随机变异与定向性变异相结合的变异策略。

随机变异策略为：记录上一次变异的位置，每次有 50% 的概率继续对这个字节进行变异，50% 的概率重新随机选择一个字节进行变异，将选中的字节赋值为 [0,255] 的随机值。

定向性变异策略为：通过静态分析筛选出若干关键字节（取值对 coverage 有影响的），将他们分为两类，一类是该字节对 coverage 的影响基本只与取值是否为零有关，另一类是该字节的不同取值会大大影响 coverage。

对第一类字节，每次进行随机重构且限制它们的取值只能是 0/1。

对第二类字节，对每个字节以 50% 的概率进行指向性随机重构。指向性通过每次等概率随机 +16 或 +1 来实现。

4 Select & Observe

Select 函数的机制是完全随机地选择队列中的任意一个测试用例。

这种做法具有效率的前提是队列中的元素不能过多，于是就需要一种限制队列大小的策略。

Observe 函数的机制是只保留覆盖了**从未覆盖**的边或**从未访问**的 BB 块的新用例。这就需要一个去重机制。通过新建立 coverage-0, state-0 这两个文件并实时更新已访问的边和 BB 块即可实现。

经过测试该策略可以有效地限制队列大小，并且队列中的元素具有变异的效率。