Group Meeting - 6

Members: Yong Li, Depeng Liu, Weizhi Feng, Xie Li, Shizhen Yu, Yutian Zhu, Zongxin Liu

2021 年 6 月 2 日

内存安全工具开发

之前的问题：

- 符号执行在翻译时做的问题
- `malloc` 语句语义及验证的问题

进展情况：

- 打通了从 BoogieAST 到 CFG 的数据结构的初步转换，CFGState 上能够获取到基本块的数据结构。手动构造例子进行测试。（刘宗鑫）
- 之前实现的 SHSymbolicExecutor，能对部分语句进行符号执行，工具的基本框架。（李勰）

计划

内存相关文章调研

文章调研：

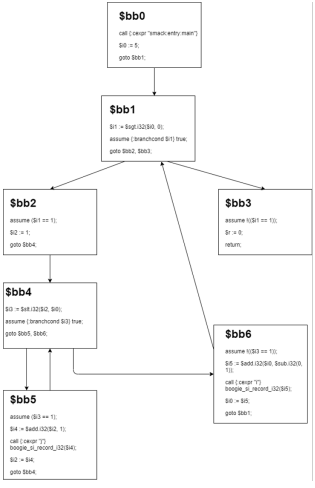
- 李勰：
  Dino Distefano et al. A Local Shape Analysis based on Separation Logic. TACAS'06
  Reinhard Wilheim et al. Shape Analysis. CC'00.
- 刘宗鑫：
  Josh Berdine, Cristiano Calcagno and Peter W.O'Hearn. Symbolic execution with separation logic. APLAS'05

冯维直：Progress

- 熟悉目前工具开发的 Smack 框架；
- 基于宗鑫写的 Boogie CFG 数据结构，实现了一个简单的 lasso sampling（遇到分支以 $1/2$ 概率选择后继），一次 sample 从原 Boogie 程序的 CFG 中得到一条路径，记录 lasso 的 stem 和 loop；
- 实验 Lasso Ranker 支持的 Boogie 程序，尝试集成到我们的工具中（目前在尝试作为黑盒直接调用）；
- 读 LTL2BA 文章，准备下周讲。

冯维直：Progress

- 基于宗鑫写的 Boogie CFG 数据结构，实现了一个简单的 lasso sampling（遇到分支以 $1/2$ 概率选择后继），一次 sample 从原 Boogie 程序的 CFG 中得到一条路径，记录 lasso 的 stem 和 loop；




```
Printing cfg of procedure main
$bb0 -> $bb1 -> $bb3
Found loop.
Standard: $bb0  Loop: $bb1 $bb2 $bb4 $bb6
Found loop.
Standard: $bb0 $bb1 $bb2  Loop: $bb4 $bb5
stem: $bb0 $bb1 $bb3  loop:
stem: $bb0 $bb1 $bb2  loop: $bb4 $bb5
stem: $bb0  loop: $bb1 $bb2 $bb4 $bb6
stem: $bb0  loop: $bb1 $bb2 $bb4 $bb6
stem: $bb0 $bb1 $bb3  loop:
```

冯维直：Plan

- 本周主要工作计划：将 Lasso Ranker 和 SVM Ranker 集成到工具中，使其能判断 sample 得到的一条 lasso 的终止性。

Differential Privacy

Currently:

- APLAS extension: complete the ePMC plugin, writing the tool description now;

Plan:

- Finish the description and polish the article(including Abstract, Introduction...);

Pufferfish Privacy

Currently:

- Pufferfish: Learning to write scripts of Sagemath to compute integrals for continuous noise. (The limit is with only finite inputs/outputs.)

Plan:

- Calculate more mechanisms..

```
sage: f
x |--> 0.250000000000000*e^(-0.500000000000000*abs(x))
sage: k1 = integral(f,x,-1,0)
sage: k2 = integral(f,x,-2,-1)
sage: k1
0.1967346701436833
sage: k2
0.11932560927059555
sage: k1<exp(0.5)*k2
0.1967346701436833 < 0.196734670143683
sage: k1<=exp(0.5)*k2
0.1967346701436833 <= 0.196734670143683
sage: k1==exp(0.5)*k2
0.1967346701436833 == 0.196734670143683
sage: 9<8
False
```