

## Group Meeting - 9

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

2021 年 7 月 14 日

# 差分隐私

这周:

- Aplus 期刊: 已用 PRISM 求解差分隐私问题; 针对部分问题, 为了防止出现计算  $P_{\min}=0$  的情况, 加入公平性性质求得更精确的隐私参数; 文章再和老师一起加工一下准备这两天投稿;
- 读 formal testing 的文章, 准备和蓝牙协议的黑盒模型学习一起报告。

计划:

- Aplus 期刊: 计划完成;
- 报告讨论一下文章, 讨论后续差分隐私模型的学习问题;
- 准备几个报告 (包括学习、这周五和下周三组会)。

# 内存安全工具开发

上周目标和进展情况：

由于开会和协助写项目书，花在内存工具安全上的时间较少，没有实质性进展。

- 过程间分析的调研和实现

（目前正在阅读 Principles of Program Analysis 的教材、熊英飞老师的课件）

- 一些 Debug 的工作：昨天的问题..

TODOs:

- 继续完成上周目标，需要注意以下问题
  - 对于栈上基本类型变量的 alloc 处理。
  - 过程间分析的函数调用图如何利用的问题，以及递归调用的问题。
  - 栈上内容的在函数中的上下文信息。

# 内存安全工具的开发

```
int a = 10;
int* j = malloc(4);
if(a > 10){
    free(j);
}

for(int i = 0; i < 15; i ++){
    int *j = (int*)malloc
        (sizeof(int));
    if(i < 10){
        free(j);
    }
}
```

```
TData data;
TData* pdata = &data;

TData c;
pdata->lo = malloc(16);
pdata->hi = malloc(24);
void *lo = pdata->lo;
void *hi = pdata->hi;
if(lo == hi){
    free(lo);
    free(hi);
}
```

# 内存安全工具的开发

```
n = 128;
a = malloc (n * sizeof(*a));
b = malloc (n * sizeof(*b));
*b++ = 0;
int i;
for (i = 0; i < n; i++)
    a[i] = -1;
for (i = 0; i < 128 - 1; i++)
    b[i] = -1;
if (b[-2]) /* invalid deref */
{ free(a); free(b-1); }
else
{ free(a); free(b-1); }
```

## 进展:

- 代码实现:
  - 上周已经实现了 GandALF 文章中的 NCB 算法（一种对 unambiguous Büchi automata 取补的 slice-based 的算法）。
  - 上周提到在实现李老师提出的 semi-deterministic automata 取补新算法时（NSBC 算法）发现有些样例不对，本周已经将 bug 修复。
  - 读李老师博士论文中介绍 pldi 文章对 semi-deterministic 取补算法的改进，和李老师讨论了他的改进算法。
  - 目前在用 seminator 自带的公式和李老师给的几百个例子进行实验。

## 计划:

- 目前的实验结果显示实现的 NSBC 算法优势不明显，需要进行优化或者找其他 benchmark.
- 调研硬件验证的内容.
  - 问题，验证方法，难点，工具框架。

- Compositional Shape Analysis by means of Bi-Abduction - 整理完成
- VeriSolid Correct-by-Design Smart Contracts for Ethereum FC2019 - 读完
- Static Automated Program Repair for Heap Properties - 在读
- 学习 Ocaml