Security Checking Android Apps with Silicon

2014/6/14

Agenda

- Problem
- Architecture
- Detailed Design
- Test Data

Problem

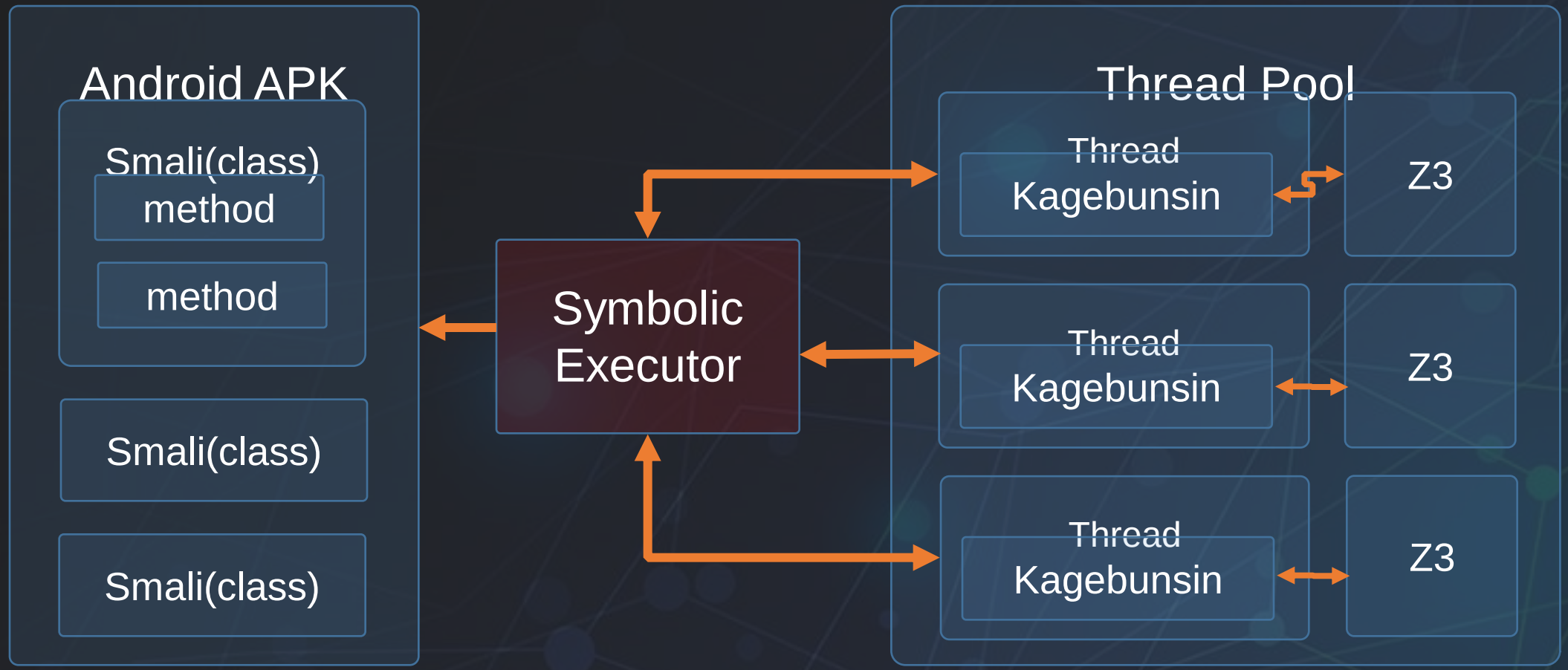
- 安全业界对产品安全分析研究逆向工程的挑战
- 从事移动应用开发的公司对产品开发测试的需求

Solution

- Symbolic execution, or symbolic execution

  run the program statically

Big Picture

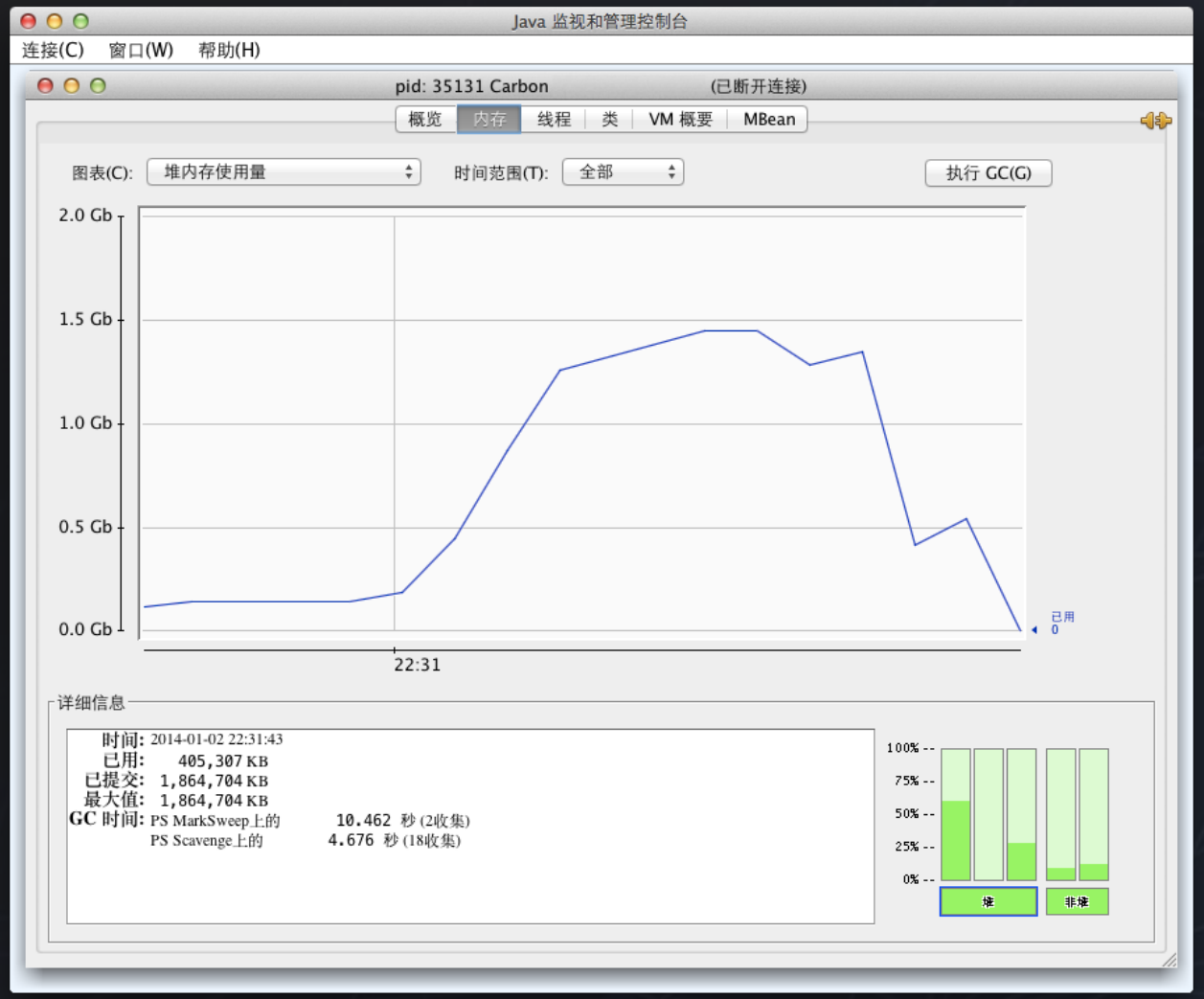

Android APK
Smali(class)
method
method
Smali(class)
Smali(class)
Symbolic Executor
Thread Pool
Thread
Kagebunsin
Z3
Thread
Kagebunsin
Z3
Thread
Kagebunsin
Z3

Detailed Design

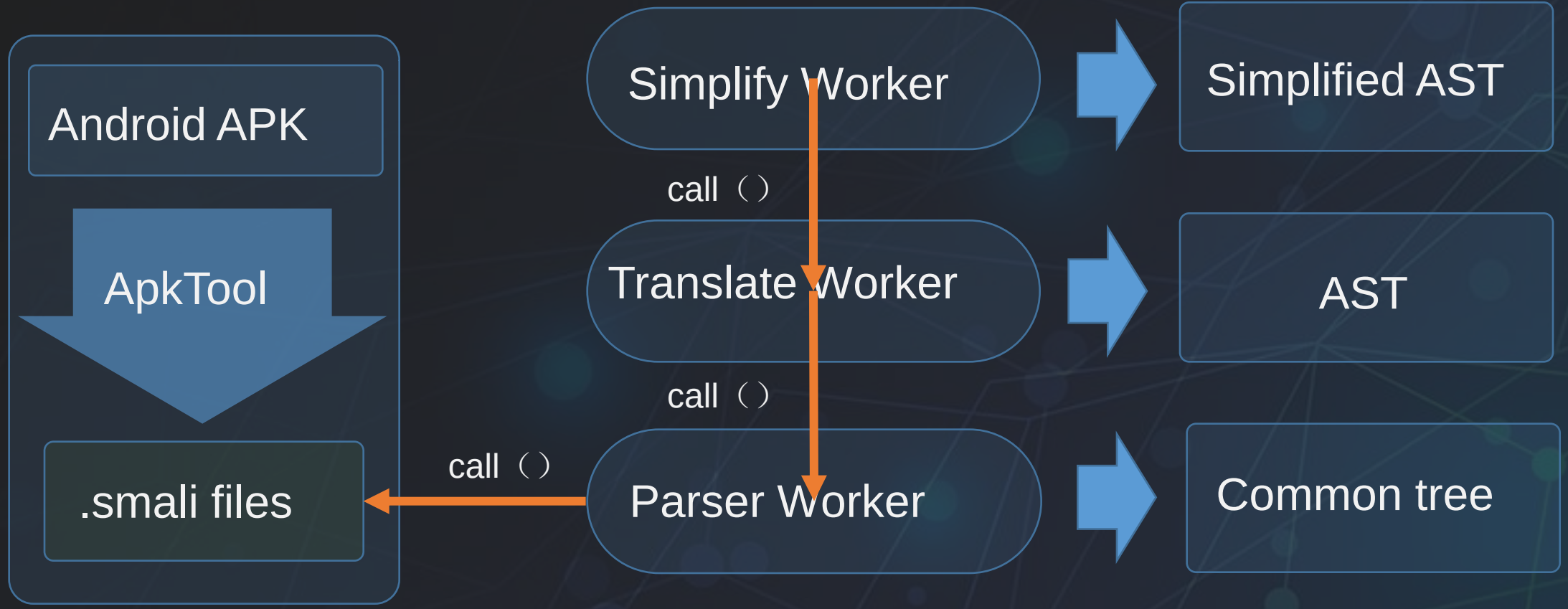
- AST Generation
- Kagebunsin
  - Operator
  - Predicate
- Symbolic Executor
- Theorem Prover

Compiler：Native

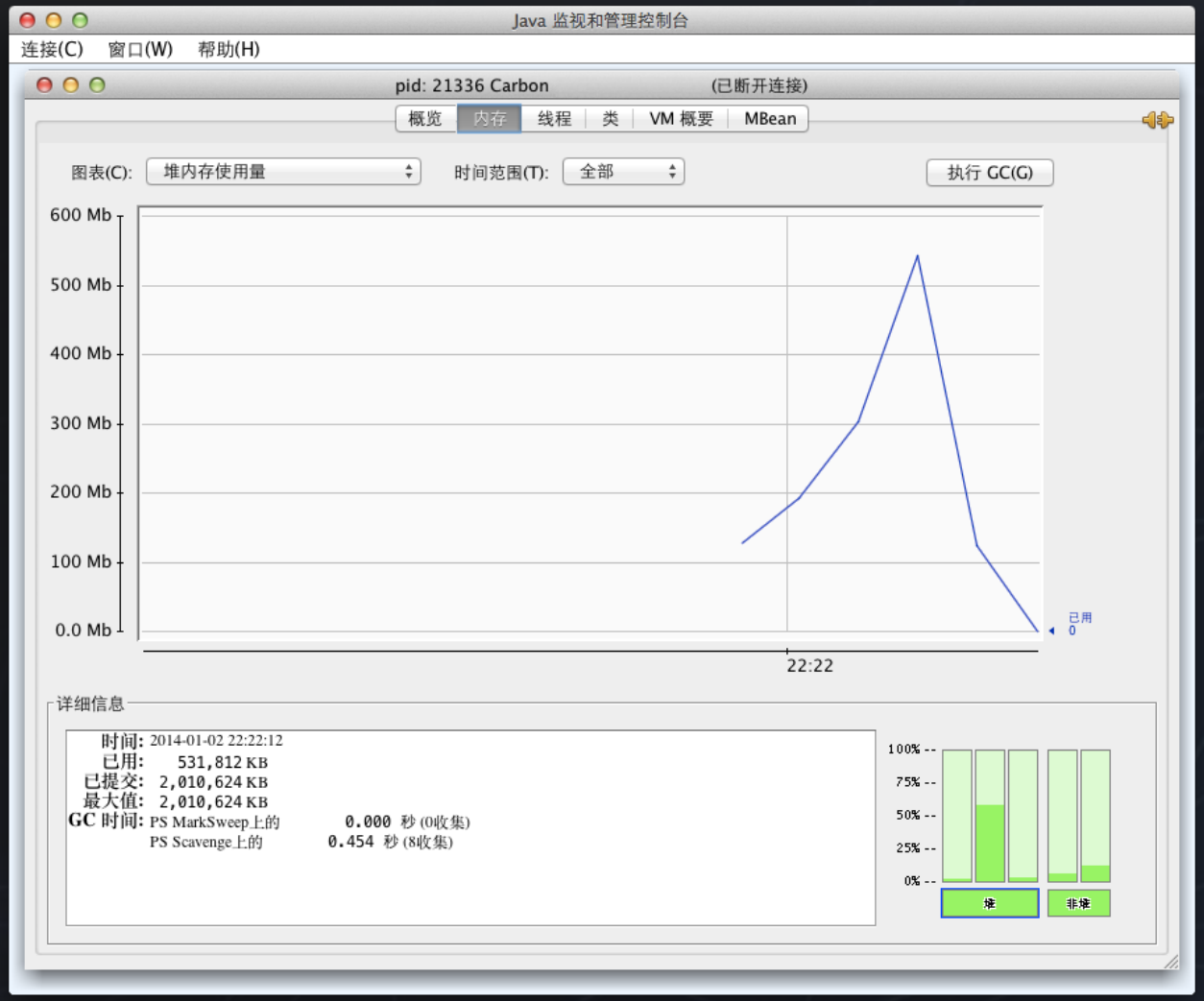
Native : Performance



Compiler：Laziness

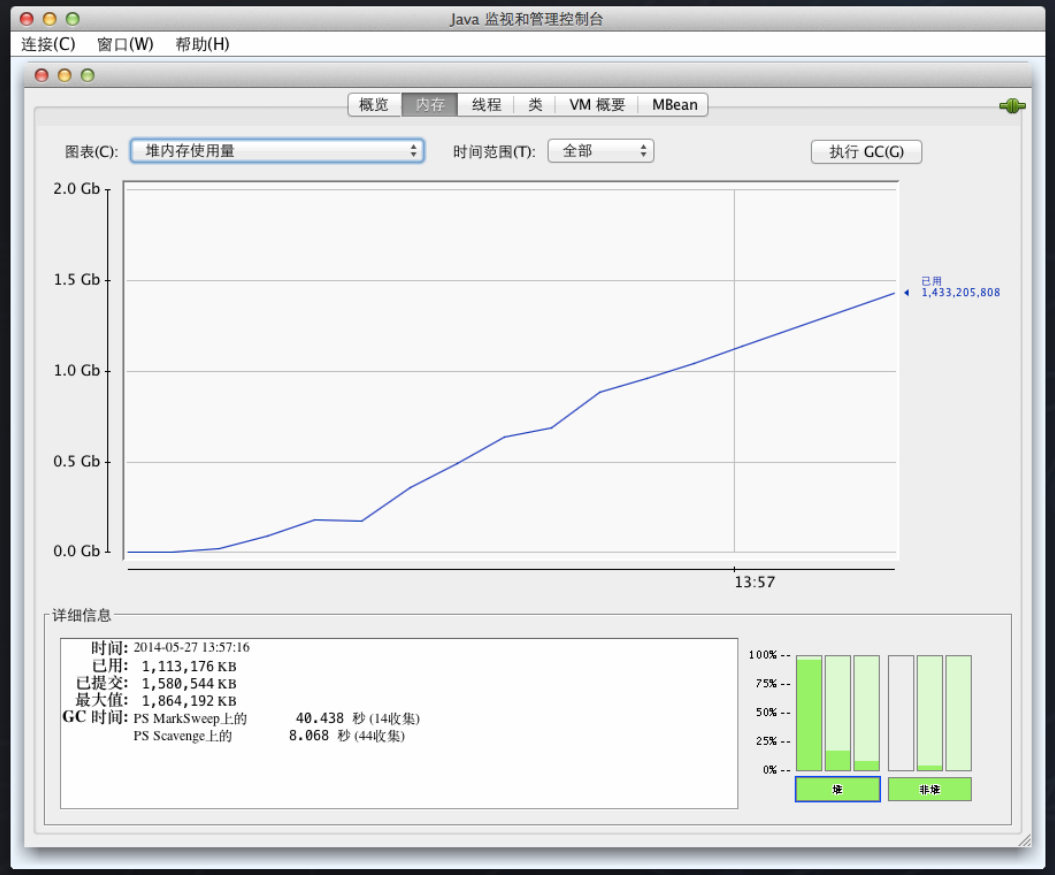


Laziness : Performance



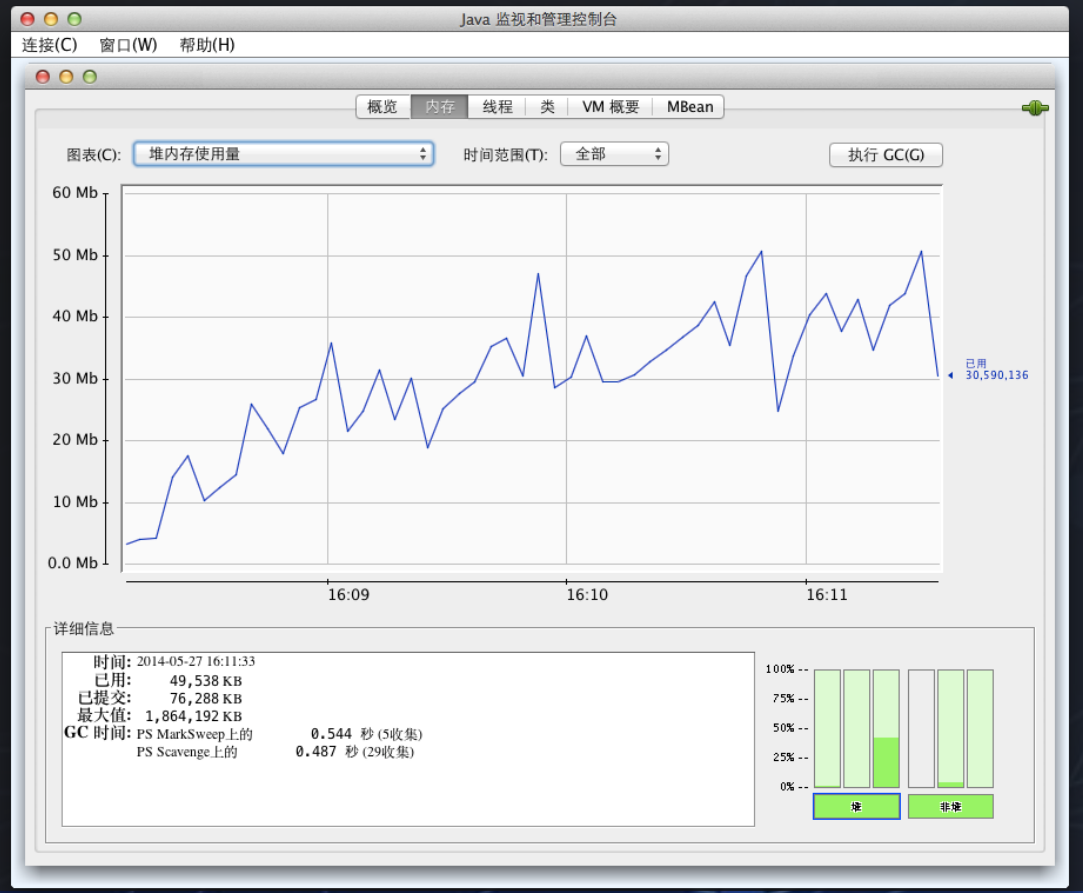
SwapMap

由于AST过大，所以在符号执行的过程中会在内存中占用越来越多的内存，但是很多AST只会被用一次，所以可以使用类似操作系统中的方法——将不用的数据结构Swap out到磁盘上，如果下次仍然需要则再Swap in到内存即可。优化效果十分明显。



SwapMap

由于AST过大，所以在符号执行的过程中会在内存中占用越来越多的内存，但是很多AST只会被用一次，所以可以使用类似操作系统中的方法——将不用的数据结构Swap out到磁盘上，如果下次仍然需要则再Swap in到内存即可。优化效果十分明显。



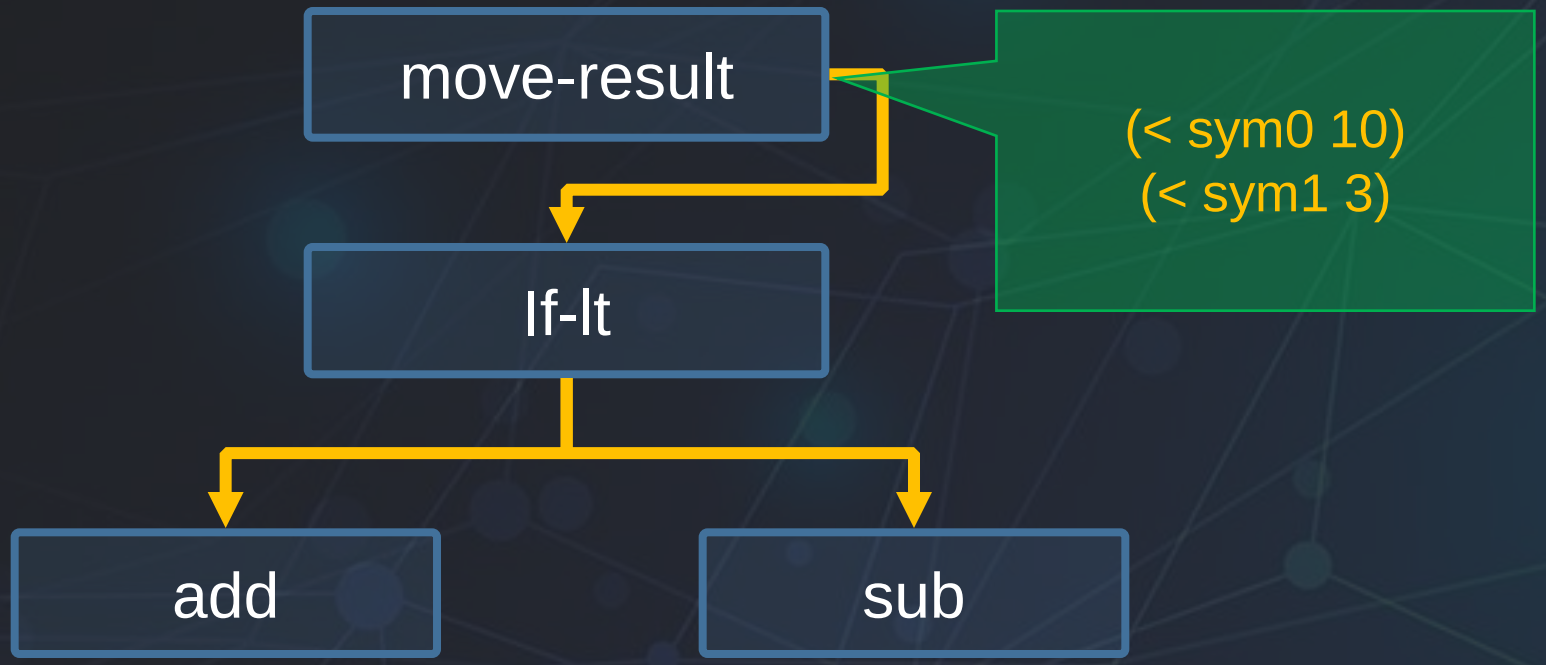
Kagebunsin

- 分身（**Kagebunsin**）是基本的符号执行单位，本质上是一个大的循环，循环中对方法内的指令进行符号执行。
- 遇到分支进行定理证明，如果两条路径都能够执行则自己执行一个路径并启动另一个分身去执行另一个可执行的路径。

Kagebunsin: Data Sharing

- 问题：为什么需要数据共享？

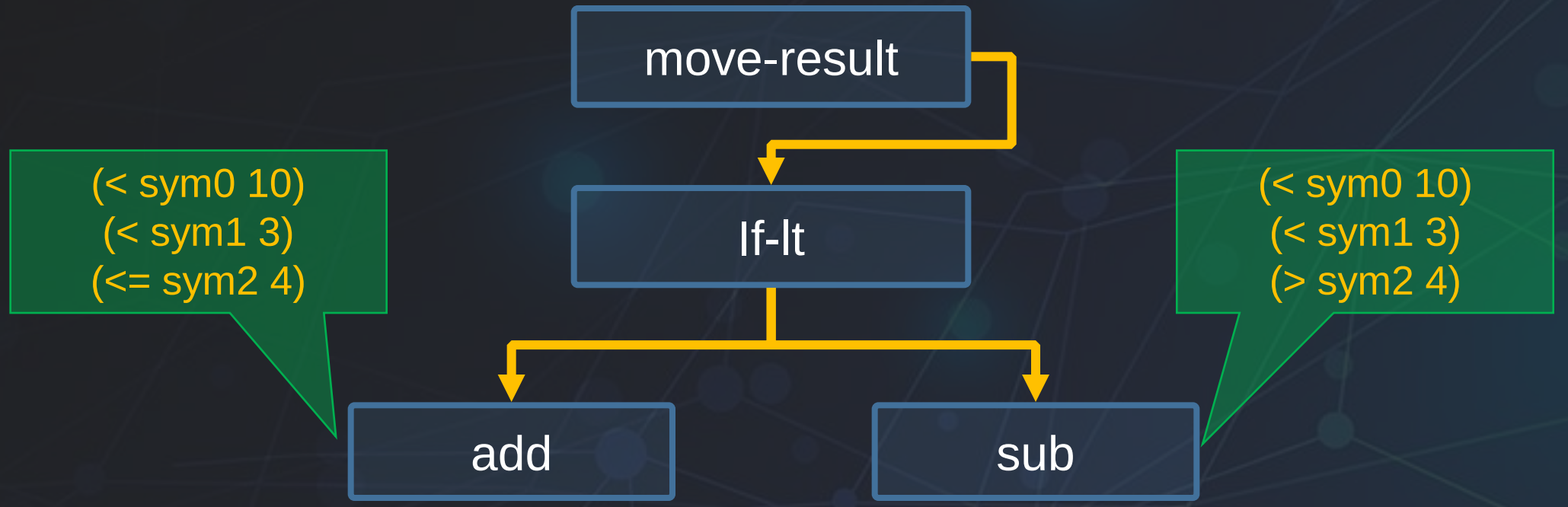
由于分身遇到分支条件就会进行一个分身，而且之前积累的所有路径条件以及寄存器状态都需要整个复制一份让两个分身使用。



Kagebunsin: Data Sharing

- 问题：为什么需要数据共享？

由于分身遇到分支条件就会进行一个分身，而且之前积累的所有路径条件以及寄存器状态都需要整个复制一份让两个分身使用。



Operator and Predicate

- 使用一阶逻辑作为逻辑公式
- 谓词和操作符都是符号执行的辅助数据结构，谓词即分身所积累的路径条件，形如：

  (and (> sym0 1) (< sym0 10))

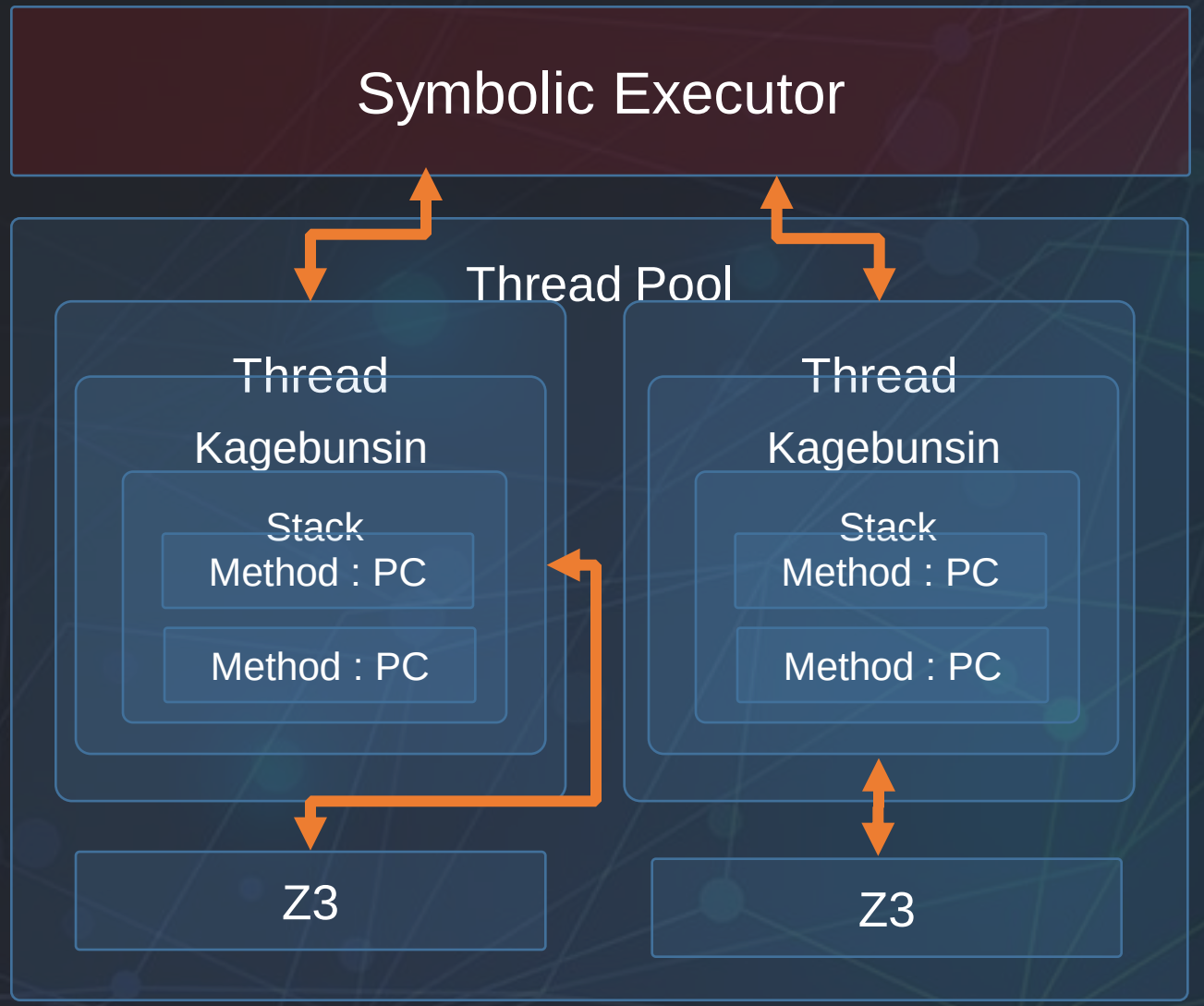
- 操作符则是模拟虚拟机进行操作的数据结构，比如当前寄存器的值有{“p0” -> (+ sym0 1), “v1” -> (/ sym1 (+ sym0 1))}

  那么执行 add p0, v1

  就会得到 (+ (+ sym0 1) (/ sym1 (+ sym0 1)))

Symbolic Executor

- 符号执行器是整个符号执行系统的管理者。
- 符号执行器负责：
  - 启动整个符号执行的进程
  - 提供API
  - 同步输出的诊断信息到文件
  - 并在符号执行系统启动时开启计时防止符号执行的时间超过所允许的执行时间。



Theorem Prover

- 选用微软开发的Z3定理证明器
  - Z3在业界比较成熟
  - 定理证明能力能够满足项目需求

Z3接口的选择	优势	劣势
Python库	成熟、文档齐全	需要跨语言
Java库	不需要自己解析输出	Unstable、文档稀少
命令行	成熟	需要自己解析输出

Test Data

- 程序 Benchmark 包括 864 个APK
- 包括 16 个类别 每个类别 54 个APK，类型数据如表：
- 所有Benchmark APK 是利用爬虫从热门应用网站按类别以下载数量为基准进行下载
- 大部分APK都会有数组越界的错误

动态壁纸
通话通讯
浏览器
影音播放
系统工具
输入法
社交网络
便捷生活
主题插件
学习办公
图书阅读
游戏
拍摄美化
网购支付
新闻资讯
金融理财

Thank You!