

Статический анализ бинарных модулей z/OS

Леденева Екатерина Юрьевна, 344 группа
Научный руководитель: д.ф.-м.н., проф. А.Н. Терехов

27 апреля 2019 г.

Введение

Статический анализ кода – анализ программного обеспечения, производимый без реального выполнения исследуемых программ.

Основная задача — построение графа потока управления.

Основные проблемы

- динамические переходы
- побочные эффекты инструкций
- динамические по своей сути инструкции (EX)
- отсутствие разделения кода и данных

Постановка задачи

- Сравнение и выбор одного из существующих решений для других архитектур в качестве основы для реализации
- Разработка статического анализатора на выбранной основе
- Разработка графического интерфейса

Обзор существующих решений

Решения для архитектуры x86:

- **Jakstab** (Java toolkit for static analysis of binaries)
- **BAP** (Binary Analysis Platform)

Общая идея:

производится перевод машинного кода в некоторый промежуточный язык и на этой основе строится граф потока управления.

Выбор основы для реализации

ВАР



Выбор основы для реализации

Jakstab



Графический интерфейс

The screenshot displays the Jakstab GUI interface, which is divided into several sections for configuration and visualization.

Input: Source: paper\jakstab_git\jakstab\my_tests\bctrloop

Jakstab folder: Source: D:\SPbSU\Term paper\jakstab_git\jakstab

Disassembly: Source: stab_git\jakstab\my_tests\bctrloop_jak.asm

Graph settings: Source: b_git\jakstab\my_tests\bctrloop_asmcfg.dot

Autofill properties: Generate path based on input

File format: .dot .graphml

Buttons: Graph, Stop, Run!

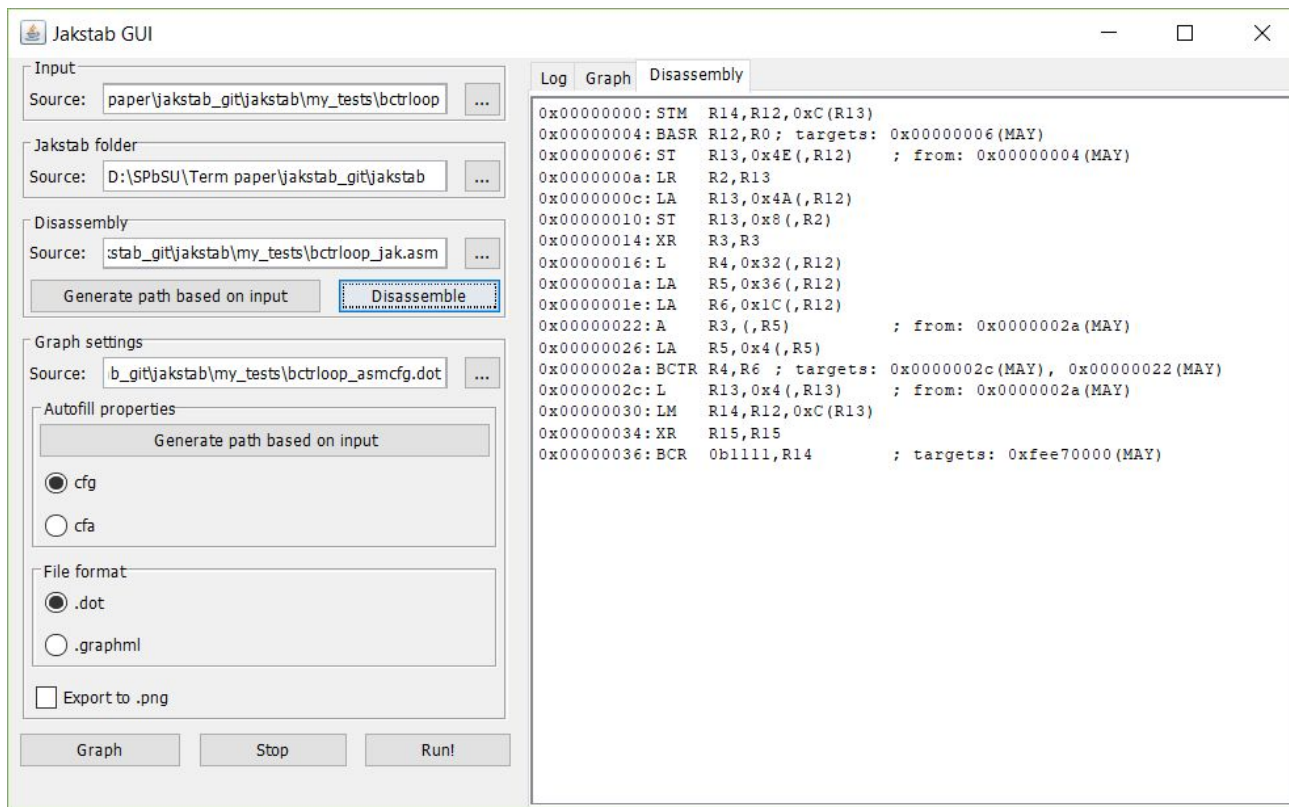
Log Graph Disassembly: Jakstab v0.8.4-devel Tue Apr 09 00:41:59 MSK 2019\n-m D:\SPbSU\Term paper\jakstab_git\jakstab\my_tests\bctrloop

Control Flow Graph:

- Address: 0xface0000
- Address: 0x00000000
STM R14,R12,0xC(R13)
BASR R12,R0
ST R13,0x4E(,R12)
LR R2,R13
LA R13,0x4A(,R12)
ST R13,0x8(,R2)
XR R3,R3
L R4,0x32(,R12)
LA R5,0x36(,R12)
LA R6,0x1C(,R12)
- Address: 0x00000022
A R3,(,R5)
LA R5,0x4(,R5)
BCTR R4,R6
- Address: 0x0000002c
L R13,0x4(,R13)
LM R14,R12,0xC(R13)

Flow control: True (T) and False (F) branches are indicated.

Графический интерфейс



Развитие статического анализатора

- Обработка входных форматов
- Исправление анализа инструкций перехода по регистру
- Исправление сообщений об ошибках

Ограничения статического анализатора

- Реализованы не все инструкции
- Не поддерживается инструкция EXECUTE

Результаты

- Произведено детальное сравнение существующих решений
- В качестве основы выбрана платформа Jakstab
- Разработан графический интерфейс
- Развитие существующего прототипа модуля статического анализа