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

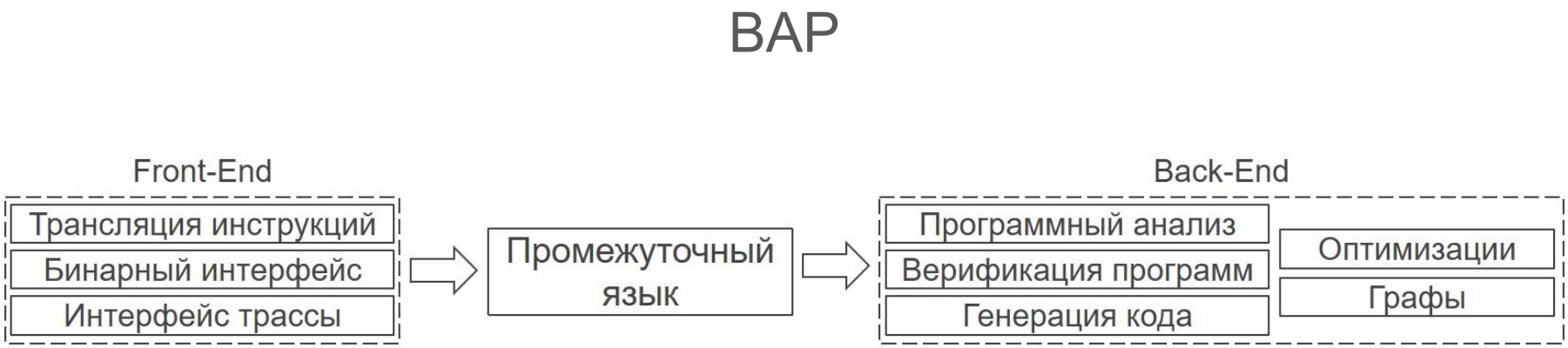
Решения для архитектуры x86:

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

Общая идея:

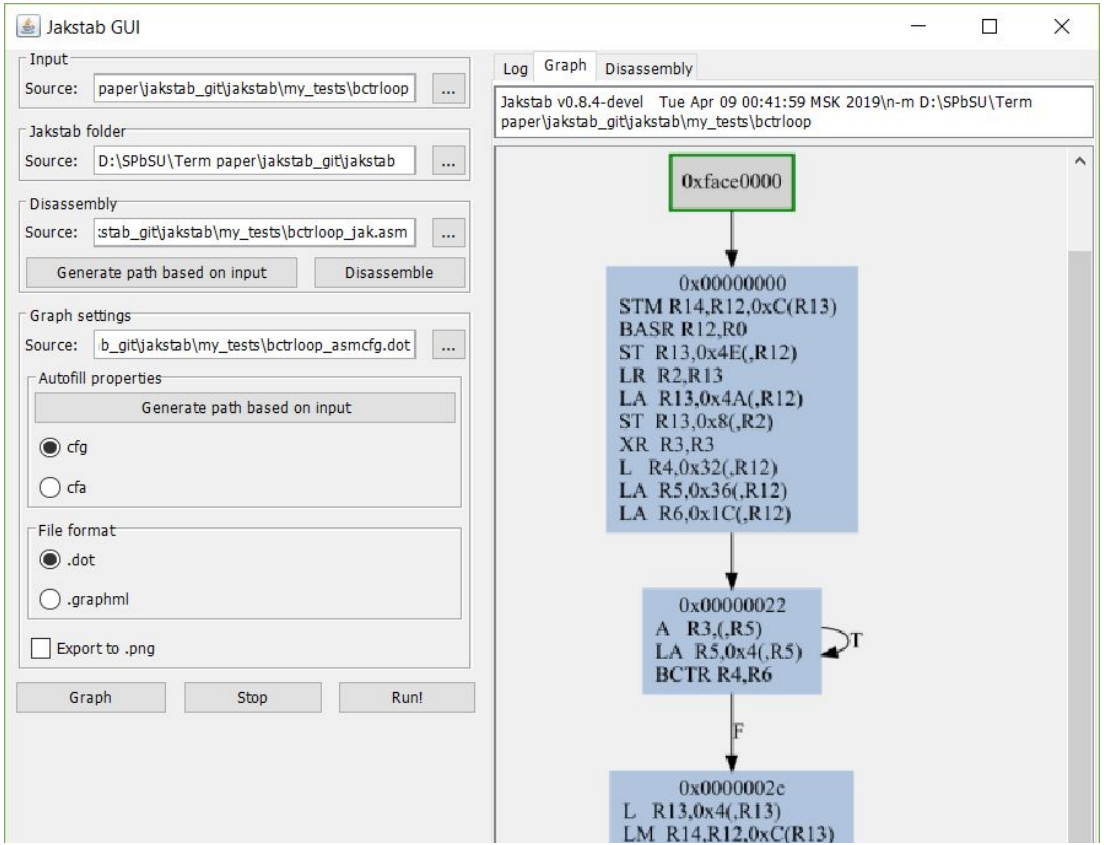
производится перевод машинного кода в некоторый промежуточный язык и на этой основе строится граф потока управления.

Выбор основы для реализации

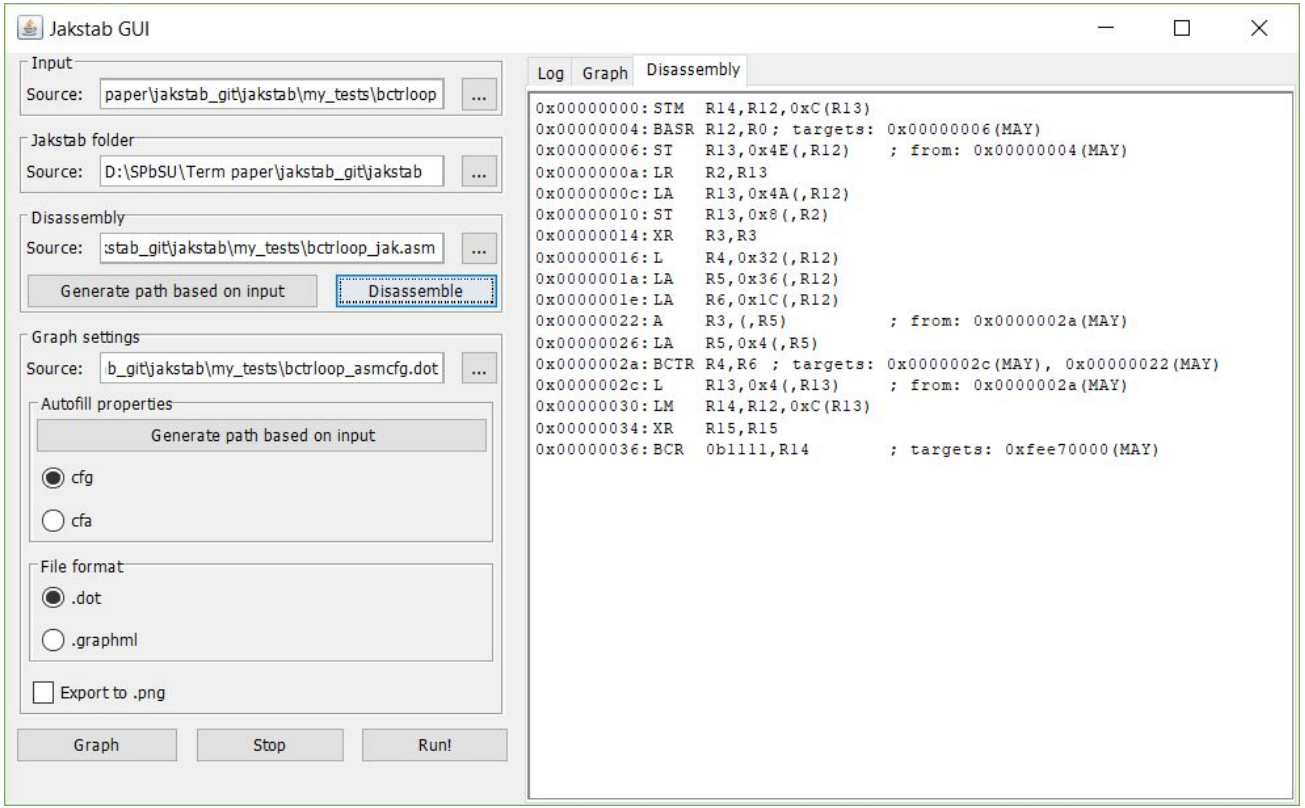


Выбор основы для реализации

Графический интерфейс



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