Архитектура и функциональные возможности инструмента ИСП Фаззер

Докладчик: Мишечкин Максим Владимирович
Акользин Виталий Владимирович
Курмангалеев Шамиль Фаимович

11.12.2020

ИСП РАН

Требования к современному фаззеру:

- Анализ программ через различные входы.
- Обратная связь по покрытию.
- Статическая и динамическая инструментации.
- Качественная фильтрация аварийных завершений.
- Интеграция с различными средствами динамического анализа.
- Отображение достигаемого покрытия.
- Удобное отображение найденных аварийных завершений.
- Фаззинга приложений принимающие на вход контейнеры.
- Фаззинг сетевых протоколов и сложных форматов данных.
- Возможность создания пользовательских мутаций.
- Интеграция с инструментами динамического символьного выполнения.
- Масштабируемость.
- Система управления многопоточного фаззинга.
- Наличие генератора входных данных на основе грамматик.
- Учет покрытия модуля и библиотек, используемых в программном обеспечении.

Сравнение фаззеров

	AFL	AFL++	AFL Smart	Peach	aggroArgs	ИСП Фаззер
Обратная связь по покрытию	+	+	+	-	-	+
Фаззинг файлов	+	+	+	+	-	+
Фаззинг сети	-	-	-	+	-	+
Фаззинг аргументов командной строки	-	-	-	-	+	+
Фаззинг stdin	+	+	+	-	-	+
Отображение покрытого бинарного кода	-	-	-	-	-	+
Описание формата данных(в т.ч. Peach)	-	-	+	+	-	+
Фаззинг контейнеров	-	-	-	-	-	+
Генератор на основе грамматик	-	-	-	-	-	+

ИСП РАН

Сравнение фаззеров

	AFL	AFL++	AFLSmart	Peach	aggroArgs	ИСП Фаззер
Интеграция с средствами динамического анализа	-	+	-	-	-	+
Пользовательские мутации	-	+	-	+	-	+
Символьное выполнение	-	-	-	-	-	+
Система управления многопоточного фаззинга	-	-	-	-	-	+
Качественная фильтрация аварийных завершений	-	-	-	-	-	+
Масштабируемость	+/-	+/-	+/-	-	-	+
Планировщики выбора данных на мутацию	-	+	-	-	-	-

ИСП РАН

Архитектура системы управления ИСП Фаззер

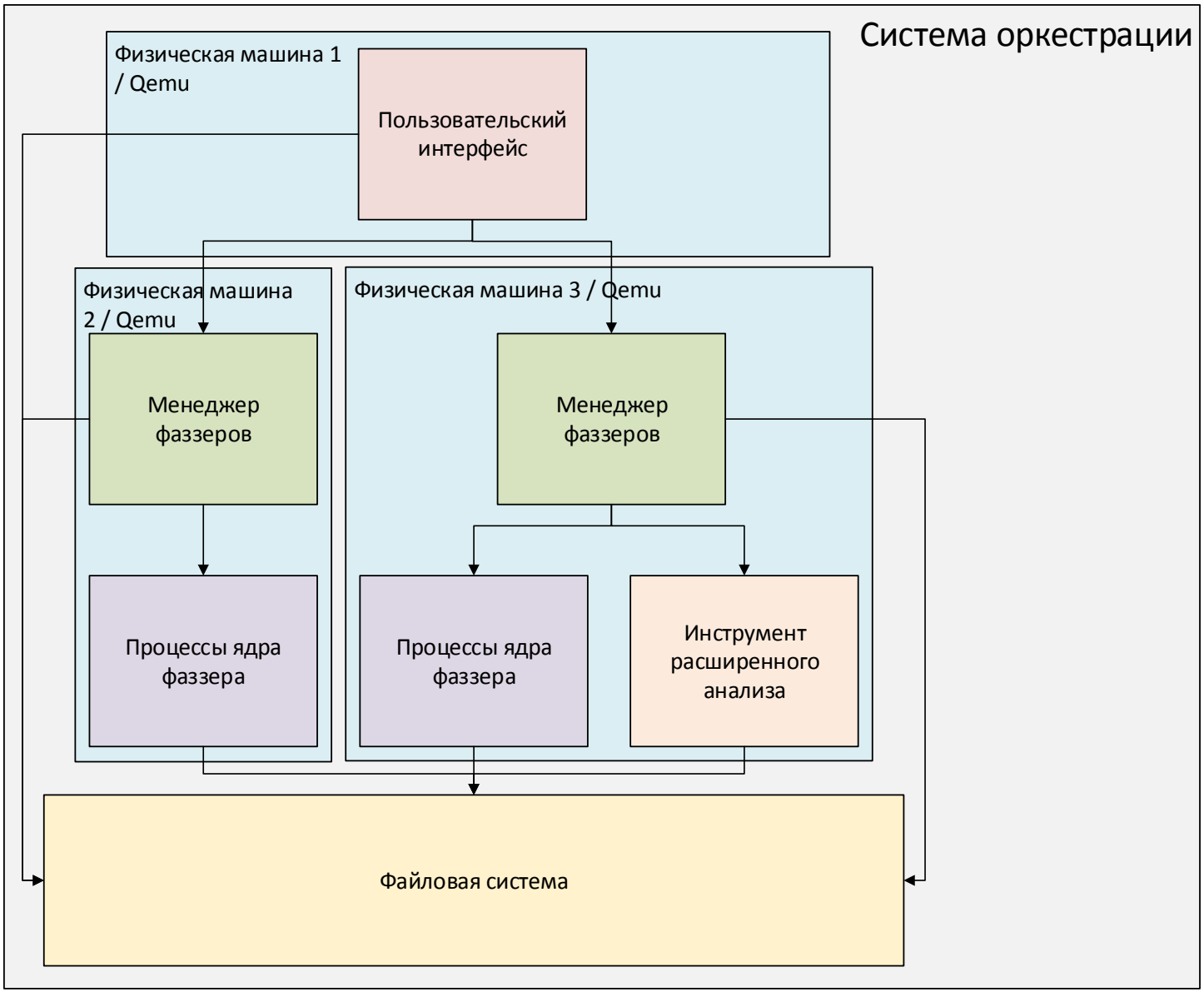
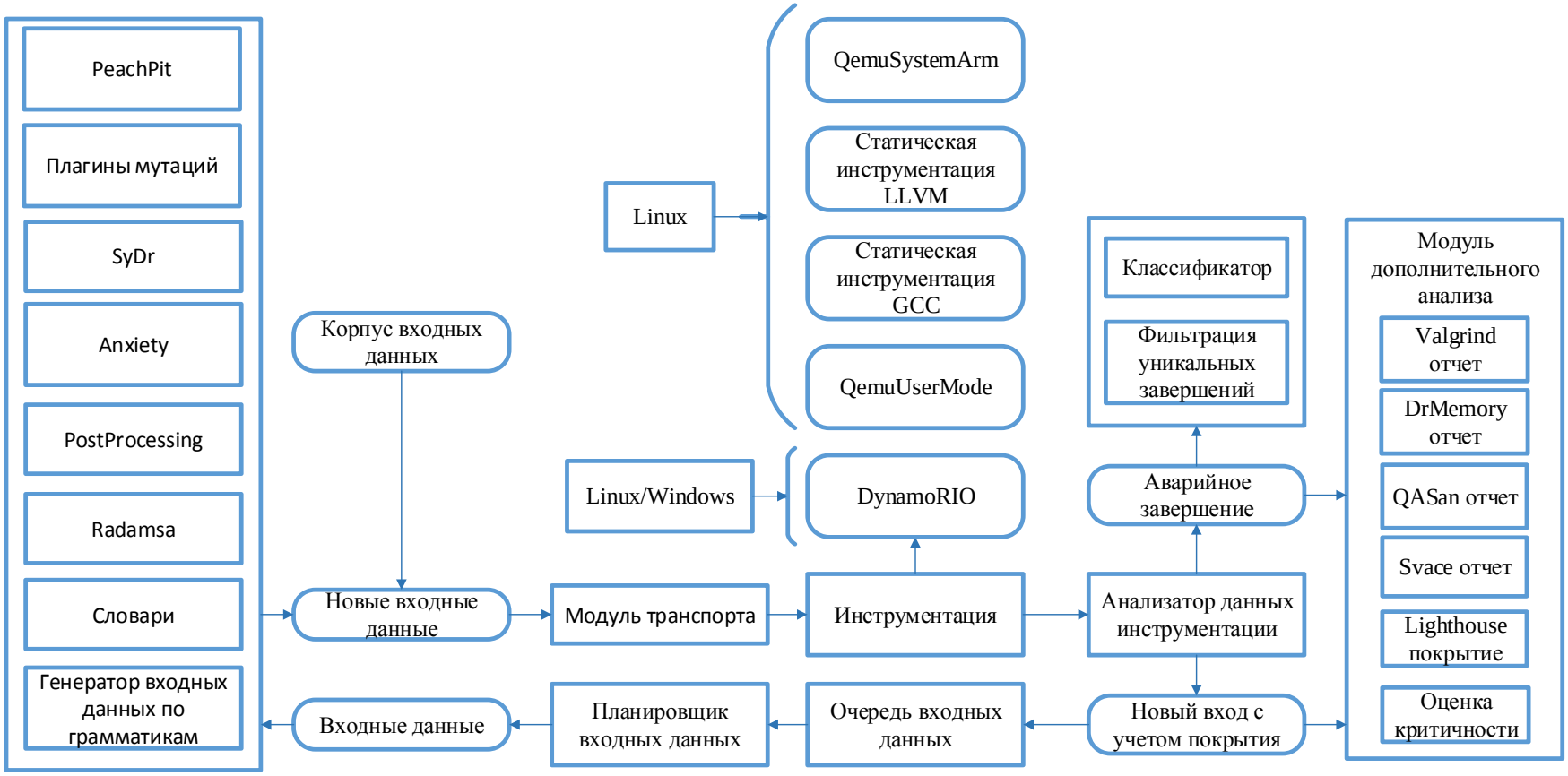


Схема ИСП Фаззера



ИСП РАН

Инструментации ИСП Фаззер

- Статическая инструментация :
  - GCC/G++
  - LLVM mode
- Динамическая инструментация:
  - QemuUserMode
  - DynamoRio
  - На основе LuaQemu
    - QemuSystemARM
    - QemuSystemX86
    - QemuSystemX64
    - …

ИСП РАН

Функциональные возможности

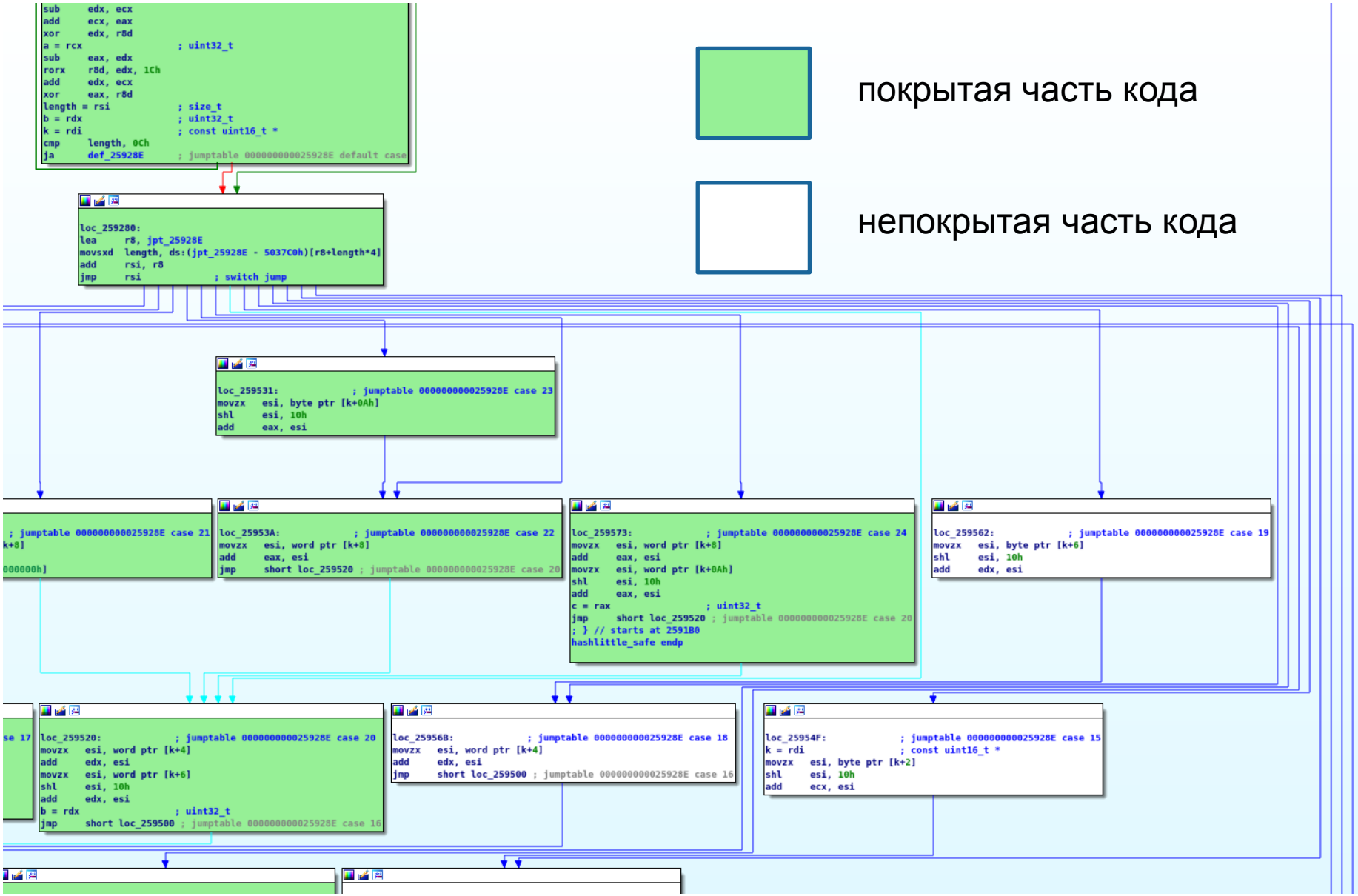
- Анализ драйверов и приложений операционных систем Windows/Linux, встраиваемого ПО («прошивок») с использованием полносистемного эмулятора на основе LuaQemu.
- Анализ сетевых протоколов с использованием Peach описаний формата и пользовательских скриптов отправки данных.
- Возможность пост и пред обработки для анализа ПО принимающего на вход контейнеры и сложные форматы данных.

Инструмент расширенного анализа

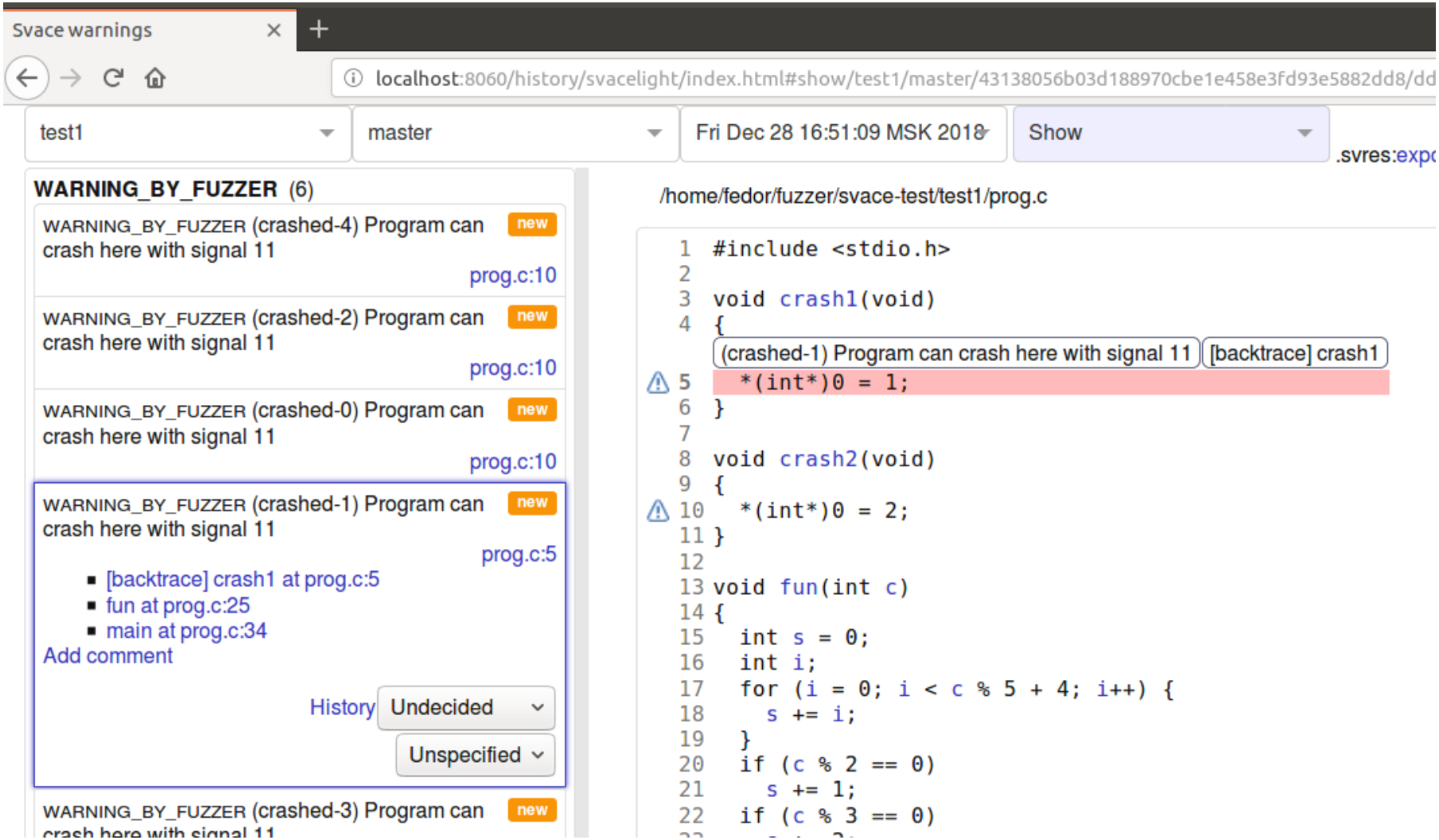
- Покрытие по базовым блокам в формате Lighthouse.
- Отчеты Valgrind.
- Отчеты DrMemory.
- Отчеты QSan.
- Отчет аварийного завершения в формате svres, который можно загрузить в проект Svace.

ИСП РАН

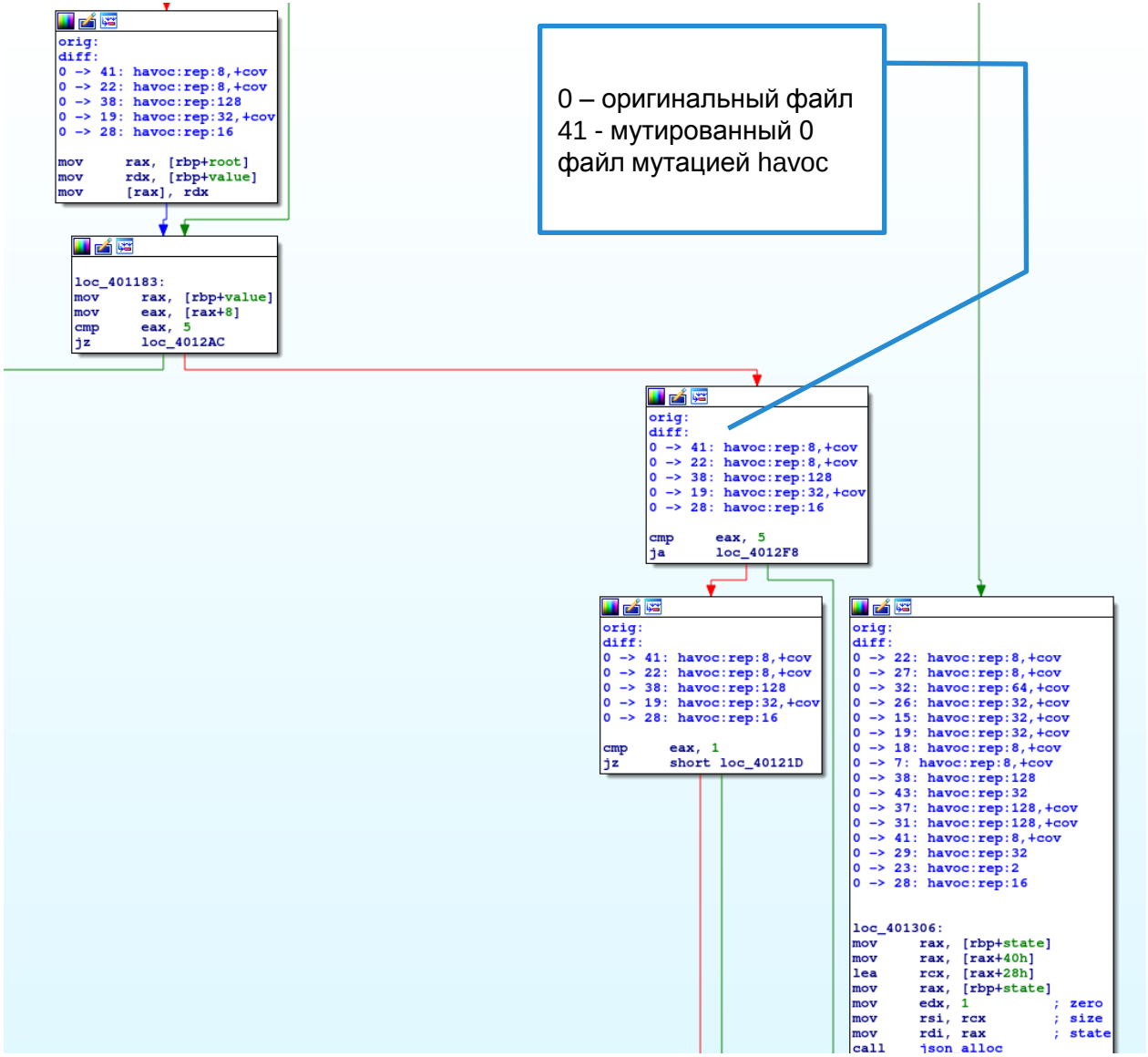
Пример Lighthouse покрытия



Отчет аварийного завершения в Svace



Технология MIA



Применение ИСП Фаззера

Результаты фаззинга popler Release 20.12.1 :

- Число путей: 4571
- Утечек памяти: 2
- Использование неинициализированной переменной: 4

Результаты фаззинга mupdf-1.18.0:

- Переполнение буфера на куче: 1

Результаты фаззинга wavpack 5.3.2:

- Найдено 10 уникальных аварийных завершений.

ИСП РАН

Применение ИСП Фаззера

Фаззинг DXE драйверов UEFI BIOS без наличия исходного кода методами:

- Частичной эмуляции LuaQemu.
- Пересборки DXE драйверов PE32+ формата в ELF с заменой UEFI специфичного кода.

Обнаруженные дефекты:

- Разыменование нулевого указателя.
- Деление на ноль.
- Выход драйвера из строя(DoS).
- Переполнение буфера на куче.

Результаты были получены с использованием:

- Покрытия в формате Lighthouse.
- Символьного выполнения Sydr.
- Отчетов Valgrind.

ИСП РАН

Спасибо за внимание

Мишечкин Максим
mish.max@ispras.ru