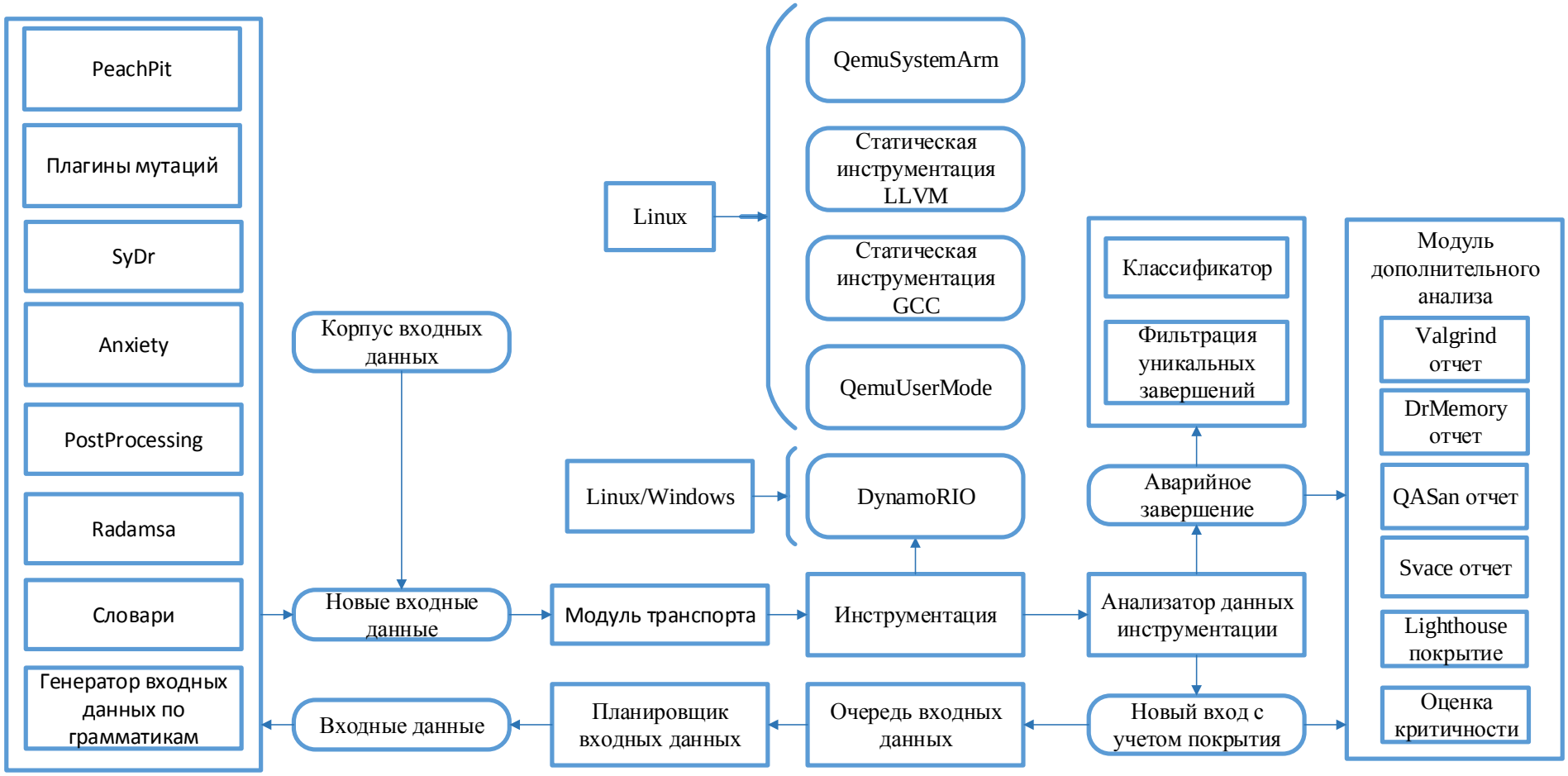
ISP Fuzzer



ИСП РАН

Ключевые возможности

- Работа в операционных системах Linux/Windows.
- Обратная связь по покрытию.
- Пользовательские мутационные преобразования.
- Модули пред и пост обработки входных данных.
- Фаззинг серверного и клиентского ПО.
- Фаззинг драйверов операционных систем Linux/Windows и встраиваемого ПО («прошивок»).
- Фаззинг на основе описания формата пакета
- Фаззинг сервисов (служб) и COM объектов
- Покрытие кода в формате Lighthouse.

ИСП РАН

Ключевые возможности

- Процент покрытых базовых блоков в ПО
- Масштабируемость до 1000 ядер.
- Пользовательские плагины отправки данных по сети.
- Интеграция с SVACE.
- Фильтрация аварийных завершений.
- Получение входных данных, на которых проявляется ошибка, размеченная в инструменте статического анализа BINSIDE.
- Использование инструмента динамического символьного выполнения Anxiety (Crusher).
- Использование инструмента динамического символьного выполнения Sydr (Crusher).

ИСП РАН

Ключевые возможности

- Наличие генератора входных данных на основе грамматик ANTLR.
- Качественная фильтрация аварийных завершений.
- Статическая и динамическая инструментации.
- Интеграция с различными средствами динамического анализа:
  - Valgrind.
  - Qsan.
  - DrMemory.

ИСП РАН

Поддерживаемые входы

- Файл
- Параметры командной строки
- Стандартный поток ввода
- Аргументы переменных окружений
- Сеть (клиент/сервер)
- Установка контекста выполнения
- Пользовательские плагины отправки данных

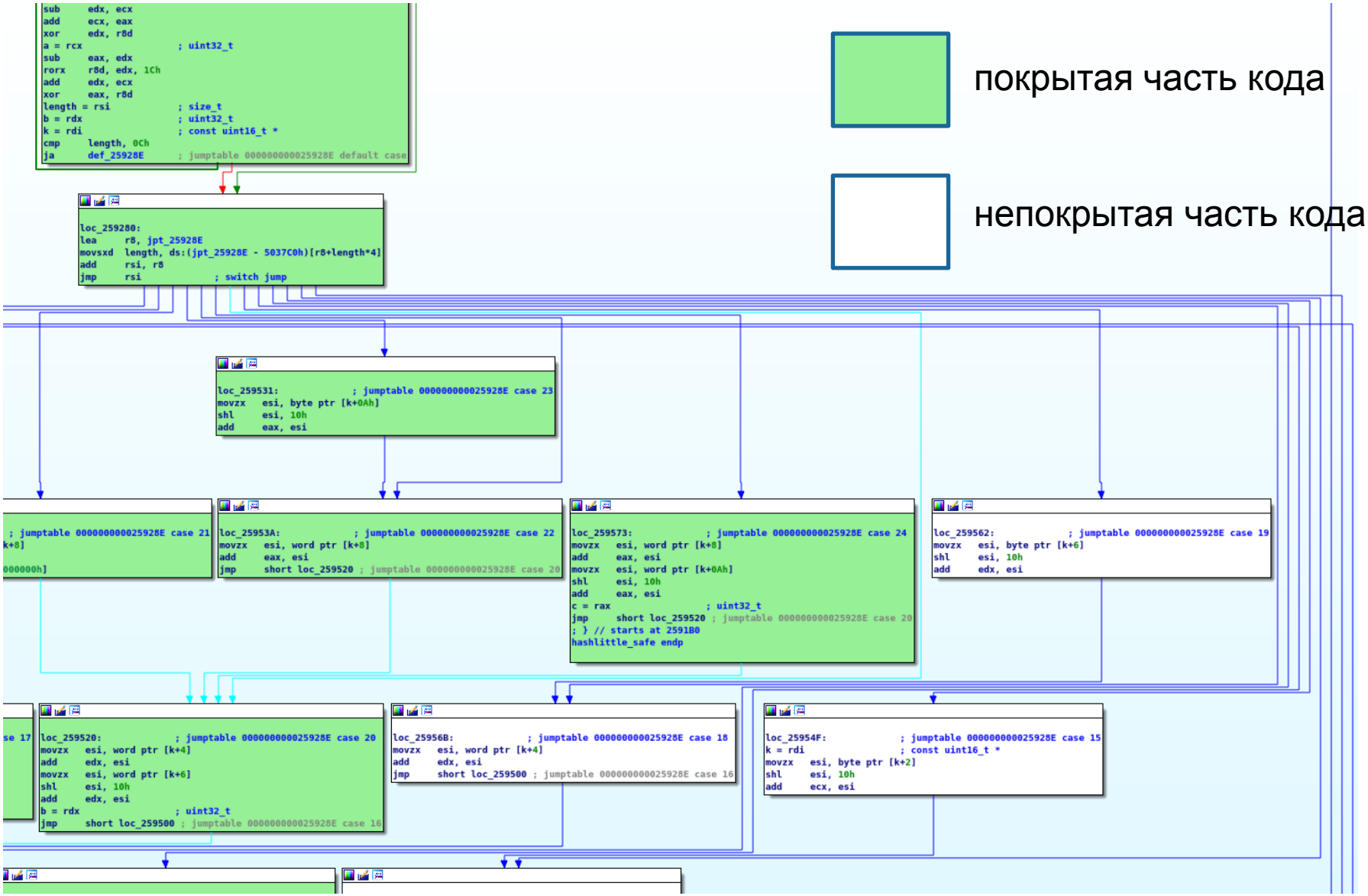
ИСП РАН

Поддерживаемые инструментации

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

ИСП РАН

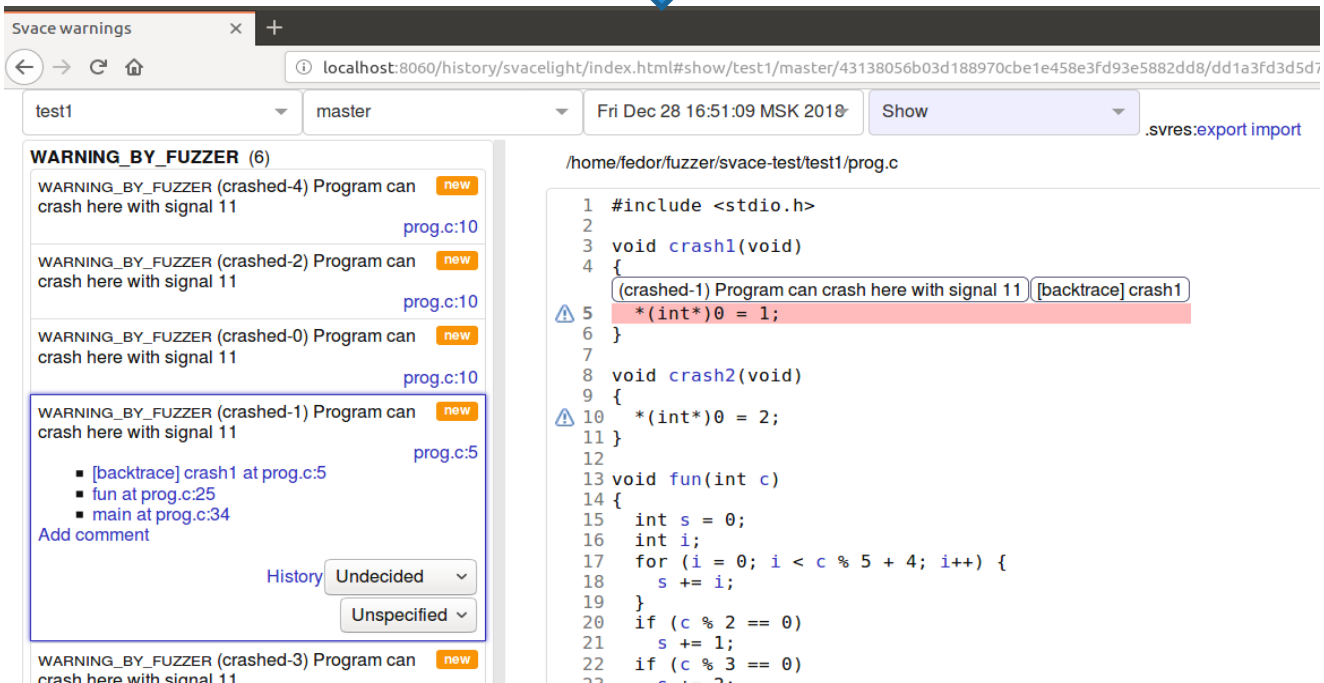
LIGHTHOUSE покрытие



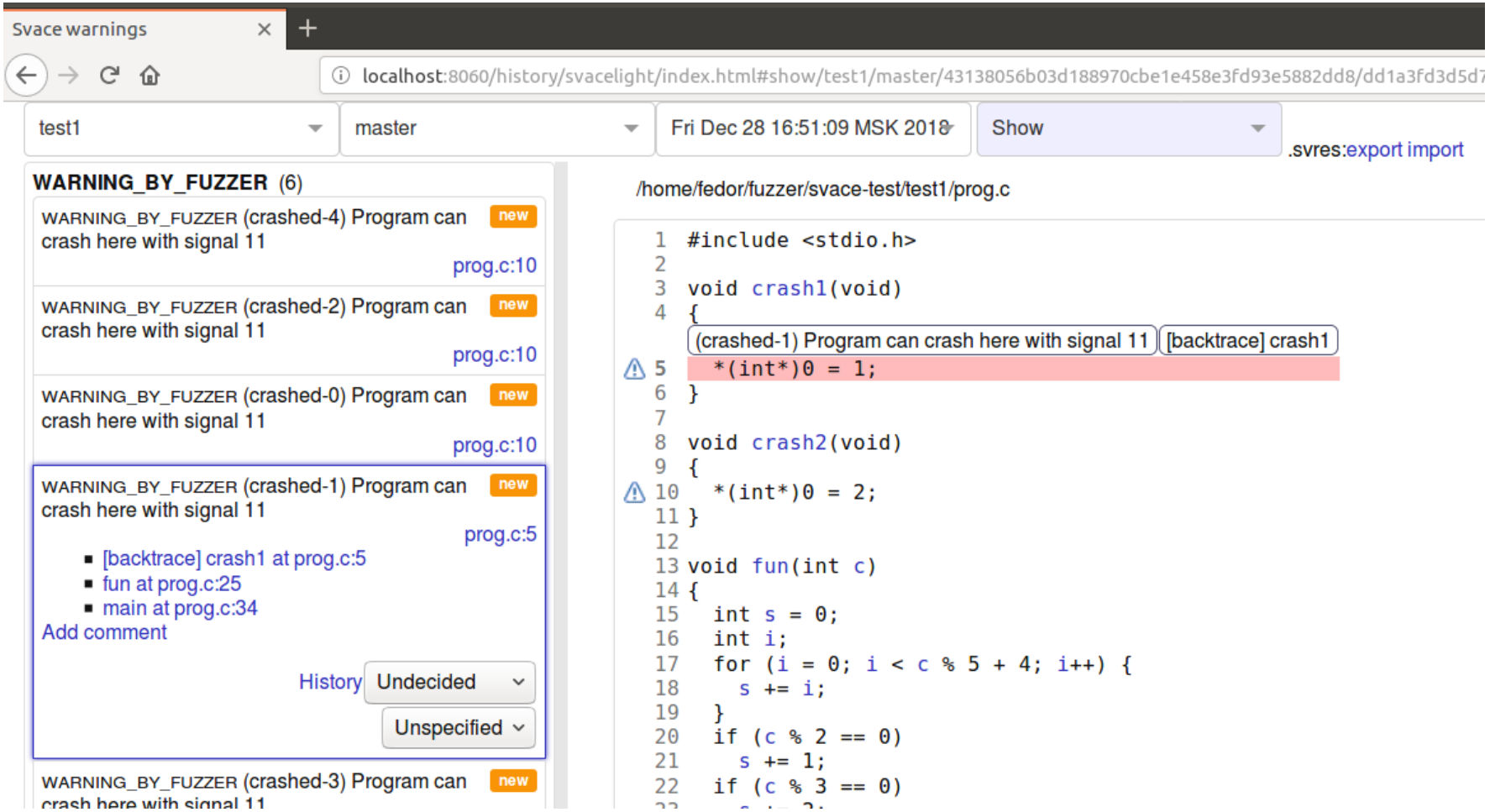
Анализ аварийного завершения

```
Starting program: /home/jenkins/projects/jasper-1.900.1/src/appl/jasper -f out/crashes/id_
crash_dse_0 -t mif -F Out_tmp -T mif

Program received signal SIGABRT, Aborted.
0x00007ffff7739428 in __GI_raise (sig=sig@entry=6)
    at ../sysdeps/unix/sysv/linux/raise.c:54
54      ../sysdeps/unix/sysv/linux/raise.c: Нет такого файла или каталога.
(gdb) bt
#0  0x00007ffff7739428 in __GI_raise (sig=sig@entry=6)
    at ../sysdeps/unix/sysv/linux/raise.c:54
#1  0x00007ffff773b02a in __GI_abort () at abort.c:89
#2  0x000000000041a5e4 in mif_hdr_get (in=in@entry=0x64f4b0) at mif_cod.c:491
#3  0x000000000041a648 in mif_decode (in=0x64f4b0, optstr=0x0) at mif_cod.c:166
#4  0x0000000000403341 in jas_image_decode (in=in@entry=0x64f4b0, fmt=<optimized out>,
    optstr=<optimized out>) at jas_image.c:372
#5  0x00000000004014a1 in main (argc=9, argv=<optimized out>) at jasper.c:229
```



Интеграция с SVACE



ИСП РАН

Peach описание.

```
<Peach>
    <DataModel name="FuzzDataModel">
        <Blob name="ContentType" valueType="hex" value="16" mutable="false"/>
        <Blob name="Version" valueType="hex" value="03 01" mutable="false"/>
        <Blob name="LengthHandshakeMessage" valueType="hex" value="40 00" mutable="false"/>
        <Blob name="LengthOfChallenge" valueType="hex" value="01 00" mutable="false"/>

        <Number name="DataLength" size="16" signed="false" endian="big" mutable="false">
            <Relation type="size" of="Data"/>
        </Number>

        <Blob name="Data" valueType="hex" value="00" mutators="blob_mutator;bit_flipper_mutator"/>

    </DataModel>
</Peach>
```

ИСП РАН