ИСП РАН

Повышение эффективности гибридного фаззинга с помощью метода поиска перспективных условных переходов

Новиков Александр Андреевич

a.novikov@ispras.ru

Курмангалеев Шамиль Фаимович

kursh@ispras.ru

22 июня 2023

Динамический анализ

Фаззинг:

- ИСП Fuzzer
- AFL
- AFL++

Динамическое символьное выполнение:

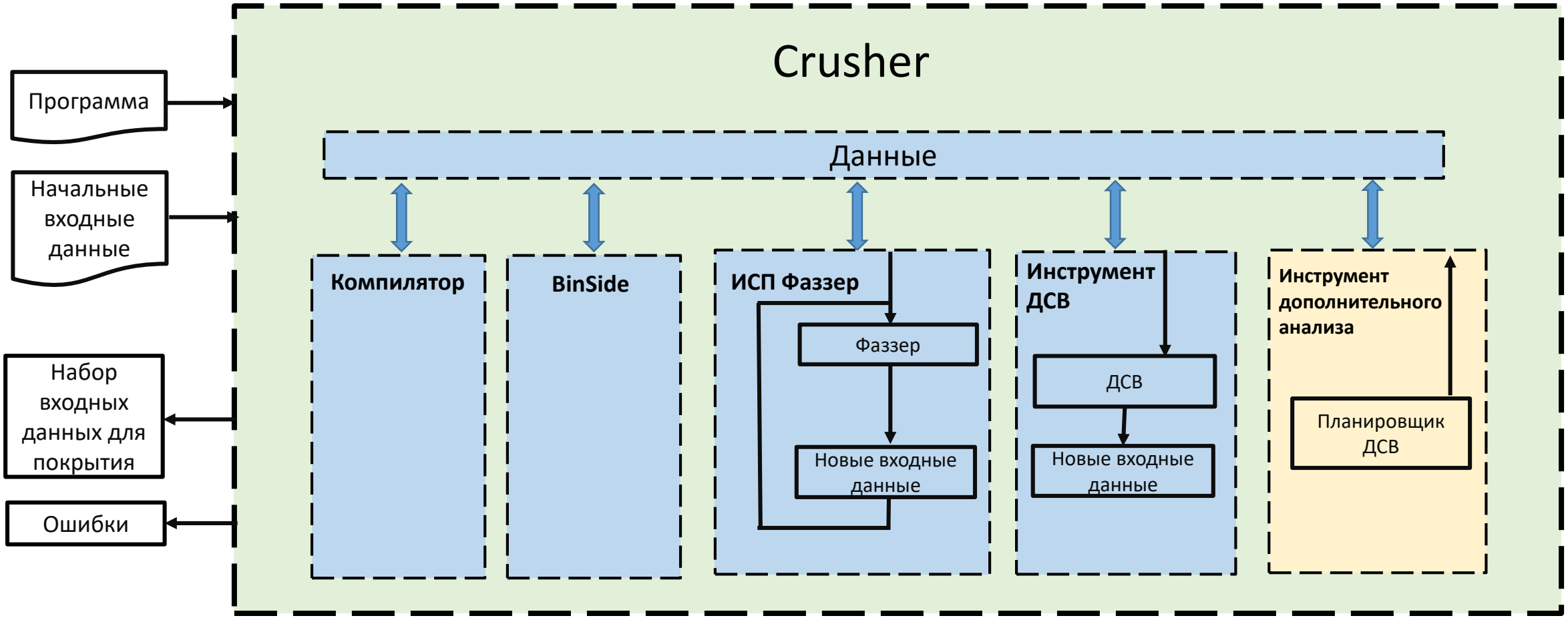
- KLEE
- QSYM
- SymCC
- Sydr
- Fuzzolic

Динамический анализ

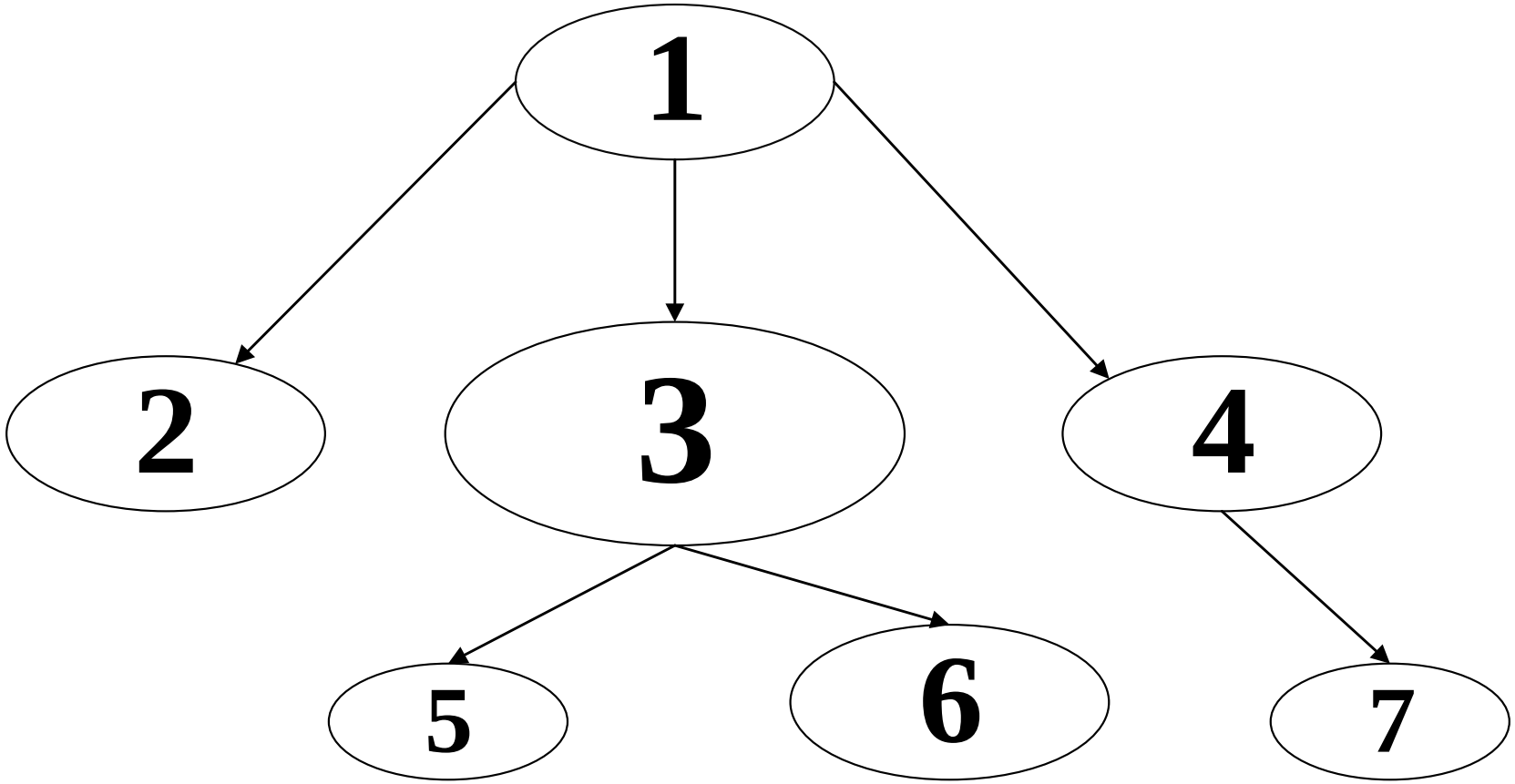
Фаззеры с использованием статического анализа:

- PathAFL
- MaxAFL
- K-Scheduler

Гибридный фаззинг в Crusher

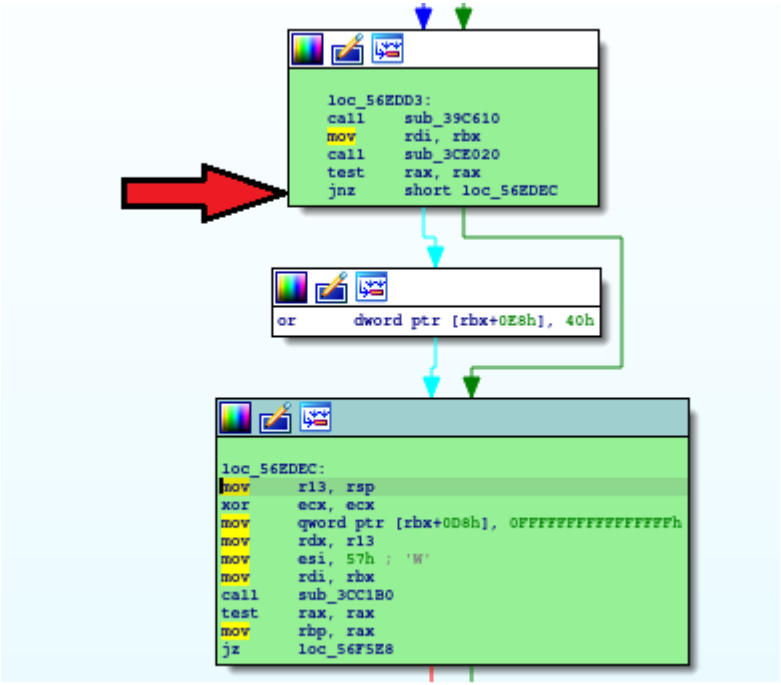


Стратегии фаззинга ПО

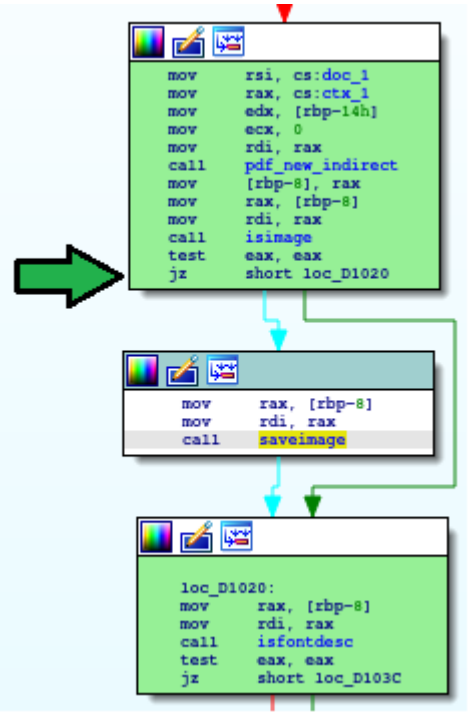


Условные переходы

Обычный условный переход

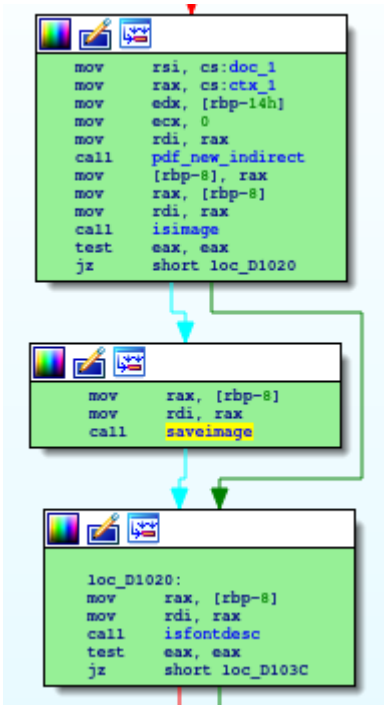


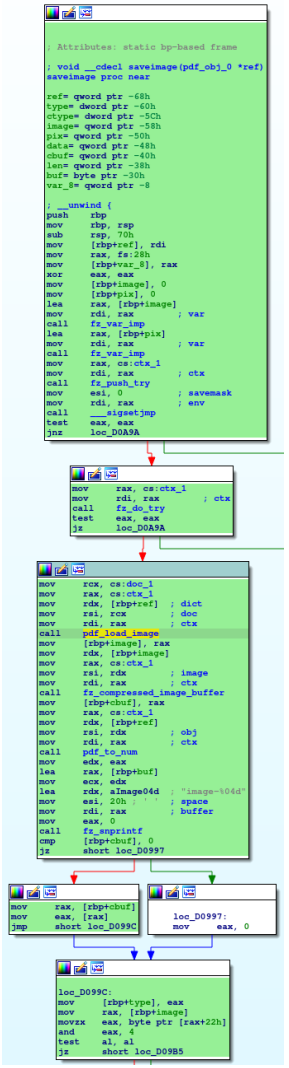
Перспективный условный переход

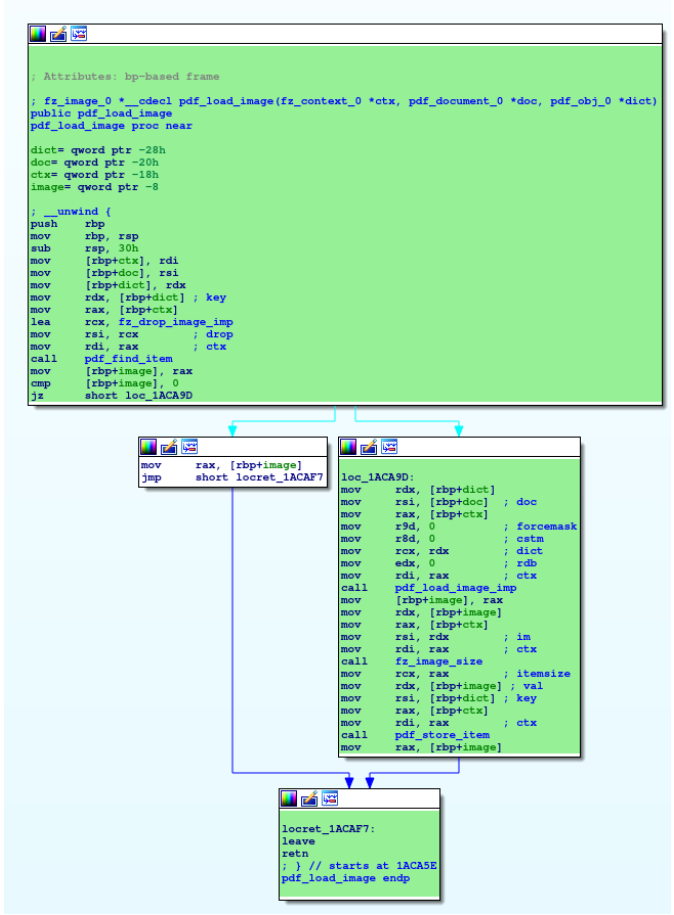


На примере программы mutool

Прирост покрытия при выполнении через перспективный переход







Алгоритм поиска перспективных условных переходов

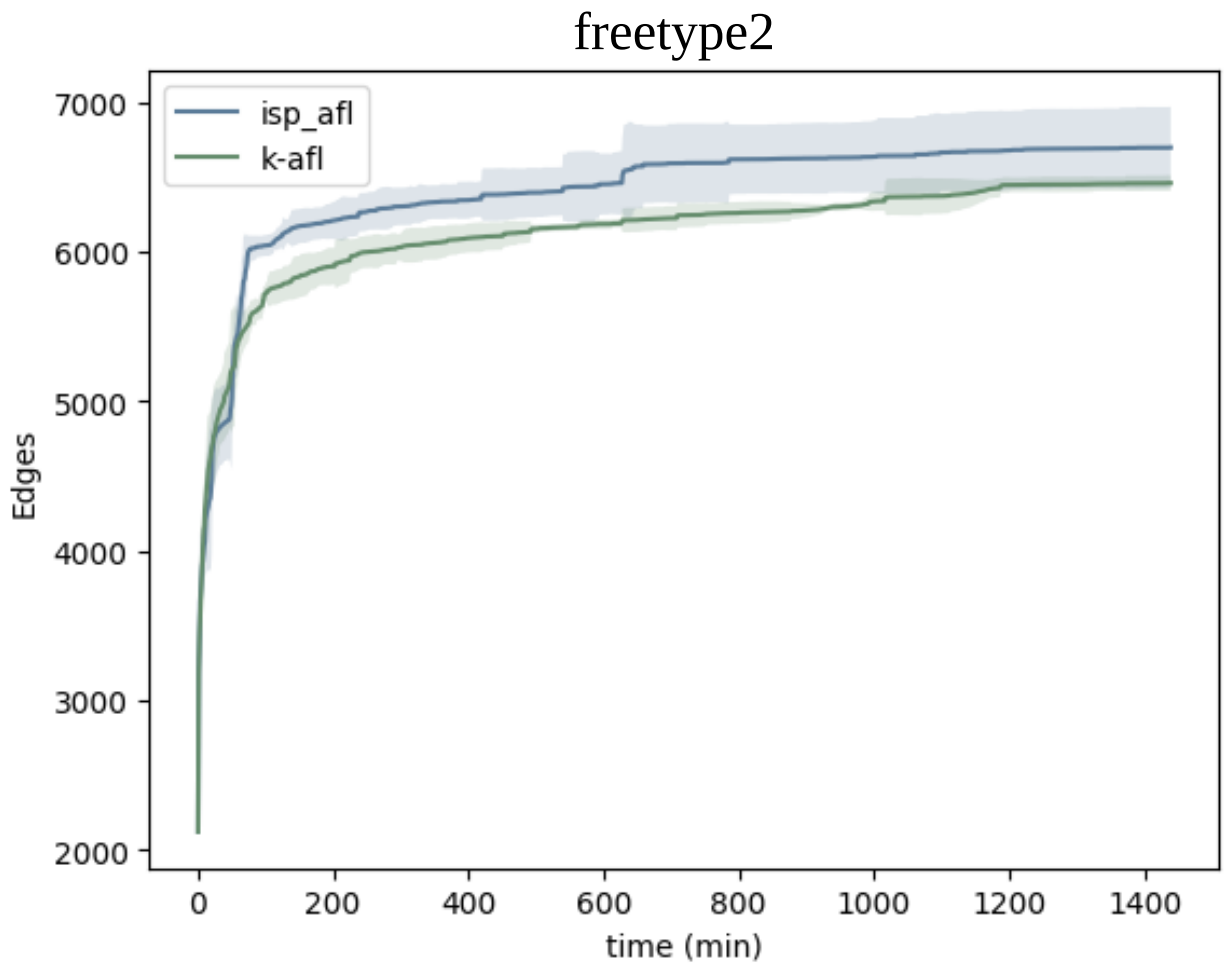
- Сбор информации о графе вызовов и графах потока управления;
- Граф вызовов: удаление циклов, топологическая сортировка;
- Контекстно-чувствительный подсчет весов функций в графе вызовов:
  - Подсчет весов перспективных условных переходов в графе потока управления;
  - Подсчет всех весов условных переходов;
  - Информация о смежных ребрах;
  - Подсчет веса функции в целом и ее аннотация для дальнейшего межпроцедурного анализа.

Алгоритм поиска перспективных условных переходов

Модификация компонента планировщика фаззера:

- Сбор информации о выполнении на входных данных;
- Подсчет веса трассы с использованием контекстных весов;
- Подсчет веса перспективных переходов вдоль трассы;
- Повышение приоритета входных данных с высокими контекстными весами в планировщике.

Результаты


freetype2
isp_afl
k-afl
Edges
7000
6000
5000
4000
3000
2000
0
200
400
600
800
1000
1200
1400
time (min)

Результаты

By avg. score

fuzzer	average normalized score
isp_aflplusplus	99.68
aflplusplus_stdin	98.46
isp_aflplusplus_norm2	97.94

Higher value is better

By avg. rank

fuzzer	average rank
isp_aflplusplus	1.67
aflplusplus_stdin	1.89
isp_aflplusplus_norm2	2.22

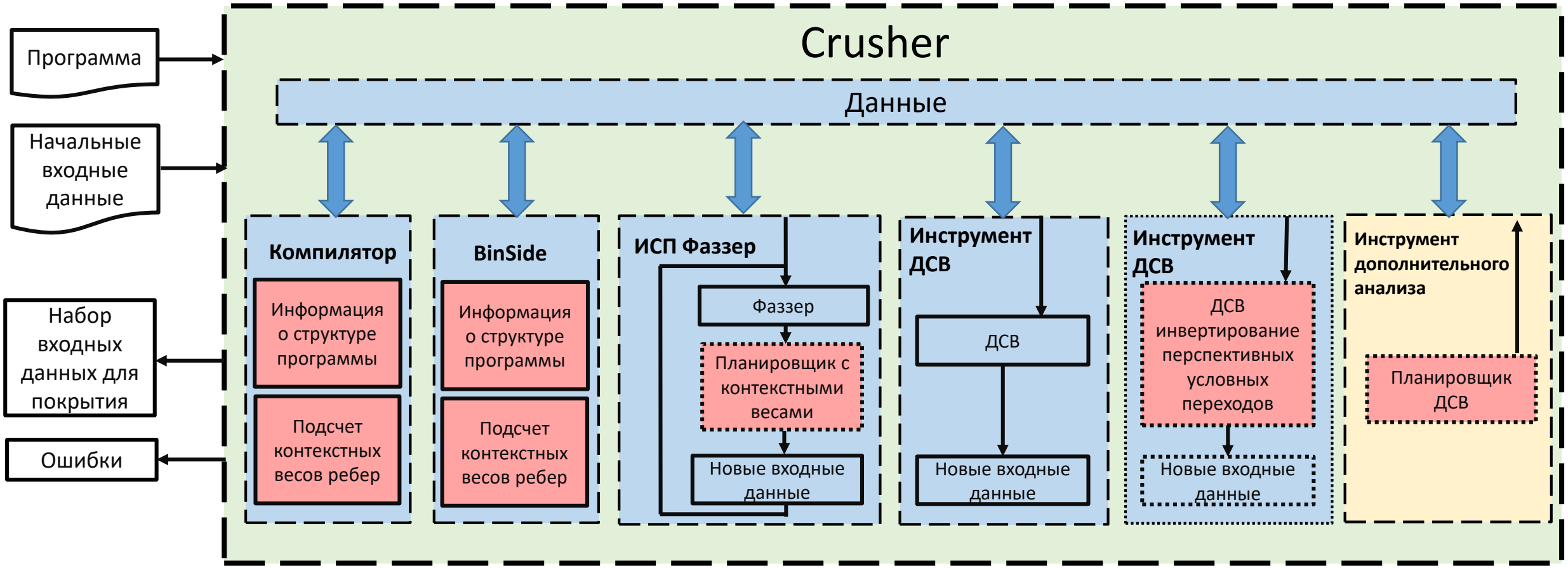
Lower value is better

Результаты

	isp_aflplusplus	aflplusplus_stdin	isp_aflplusplus_norm2
FuzzerMedian	97.00	96.00	96.00
FuzzerMean	92.56	91.78	91.11
arduinojson_json_fuzzer	98.00	98.00	97.00
double-conversion_string_to_double_fuzzer	98.00	98.00	97.00
freetype2_ftfuzzer	93.00	95.00	93.00
lcms_cms_transform_fuzzer	61.00	58.00	59.00
libxml2_xml	97.00	97.00	98.00
re2_fuzzer	98.00	98.00	98.00
sqlite3_ossfuzz	94.00	94.00	90.00
vorbis_decode_fuzzer	97.00	92.00	92.00
zlib_zlib_uncompress_fuzzer	97.00	96.00	96.00

Higher value is better

Гибридный фаззер Crusher с алгоритмом поиска перспективных условных переходов



Выводы

- Реализованы модули статического анализа перспективности условных переходов и подсчета контекстных весов для исходного кода в компиляторе и бинарного кода в инструменте BinSide;
- Реализована стратегия планировщика для выбора последующих входных данных для фаззинга с учетом контекстных весов в фаззерах K-Scheduler и AFL++ и проведены замеры в тестовых системах;
- Предложенные метод показал лучшие результаты в тестовой системе FuzzBench;

Вопросы и ответы