Sydr

Технология динамического анализа

Андрей Федотов

23 сентября 2022

Sydr: современная наука как продукт для SDL

ИСП РАН

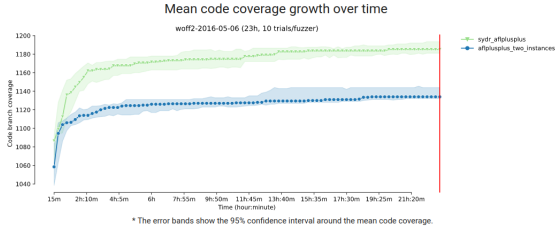
Динамический анализ:

- **Фаззинг:**
  libFuzzer, AFL++, Honggfuzz и др.
- **Динамическое символьное выполнение:**
  Fuzzolic, SymQEMU, KLEE и др.
- **Гибридный Фазззинг:**
  Fuzzolic&AFL++, SymQEMU&AFL++.

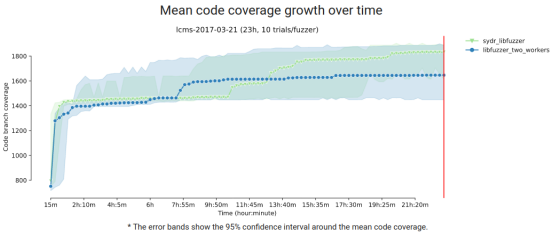
Sydr это:

- DSE на базе проекта Triton;
- Интеграция Sydr с libFuzzer и AFL++;
- Поиск ошибок символьными чекерами;
- Casr: анализ аварийных завершений.

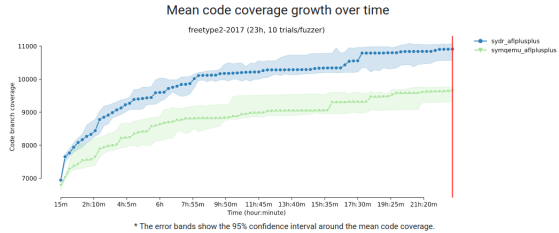
1. Sydr-fuzz достиг большего покрытия, чем другие фаззеры.
2. Sydr-fuzz победил на большем числе бенчмарков.



Sydr+AFLplusplus vs 2xAFLplusplus



Sydr+libFizzer vs 2xlibFuzzer



Sydr+AFLplusplus vs SymQEMU+AFLplusplus

sydr-fuzz.github.io/fuzzbench/

OSS-Sydr-Fuzz: новые ошибки в открытом ПО

ИСП РАН

github.com/ispras/oss-sydr-fuzz — это форк OSS-Fuzz для гибридного фаззинга с помощью Sydr.

- **30+** проектов и **260+** фаззинг-целей.
- Найдено **80** ошибок в PyTorch, TensorFlow, OpenCV, Torchvision, Tarantool и других проектах.
- Чекеры Sydr помогают находить новые ошибки после фаззинга. Найдено **10+** ошибок с помощью предикатов безопасности.
- Casr существенно сокращает время анализа аварийных завершений (1800+ аварийных завершений свелось к 7 ошибкам в PyTorch).
- Хотите пофаззить open source проект с помощью Sydr? **Ждем Ваших PR!!!**

Текущее состояние и планы на будущее

ИСП РАН

Sydr используется в:

- центре Доверенного Искусственного Интелекта ИСП РАН;
- проекте UEFI-прошивки Amaranth (базируется на EDK II);
- проекте OSS-Sydr-Fuzz.

Планы:

- выложить инструмент анализа аварийных завершений **Casr** в open source;
- поддержать фаззинг и анализ аварийных завершений для Python-приложений в Sydr;
- поддержать архитектуру AARCH64 (Baikal-M) в Sydr.

Группа пользователей Sydr в Telegram: @sydr_fuzz