PASTIS

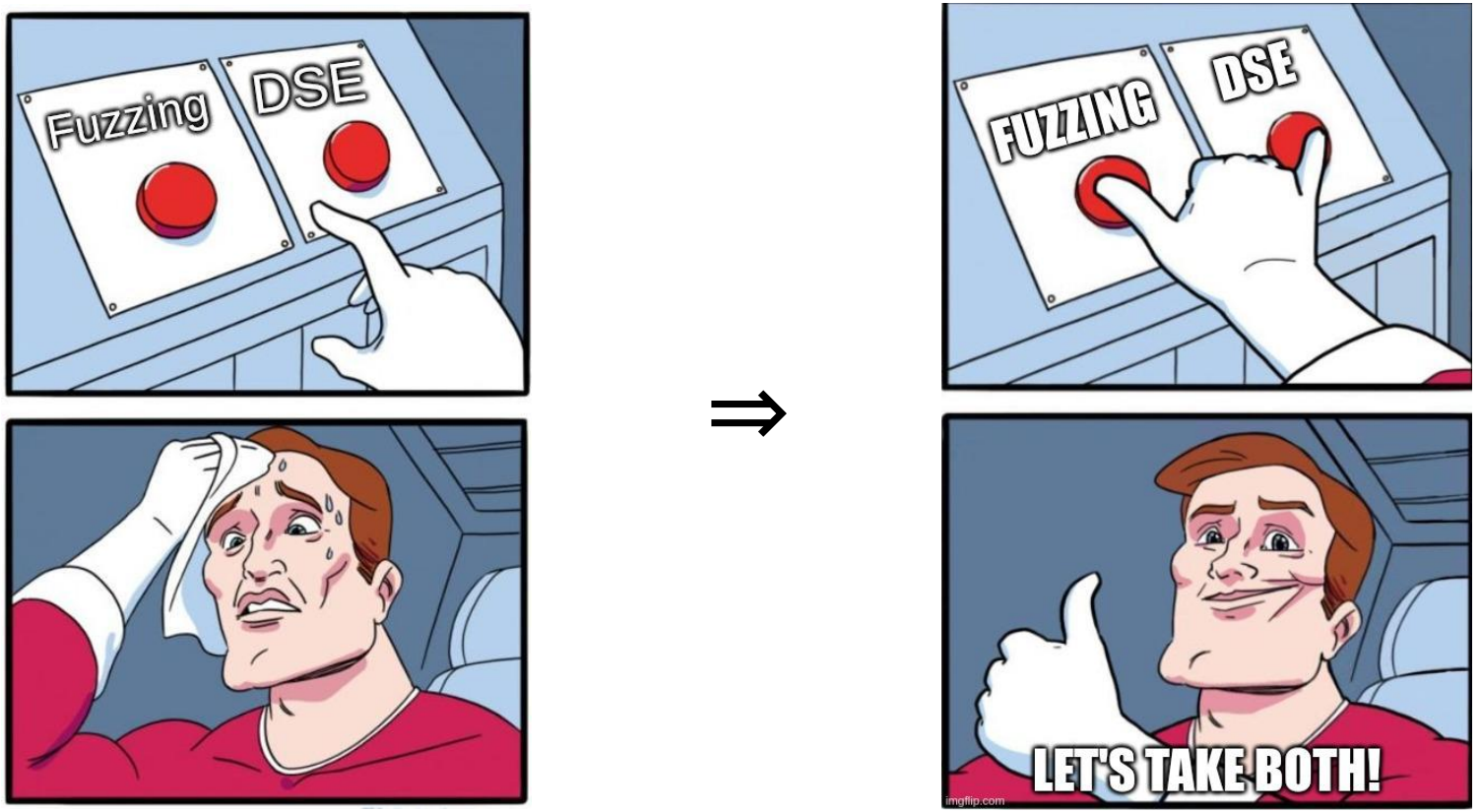
(Tool competition)

SBFT 2024, Lisboa, Portugal

Robin David <rdavid@quarkslab.com>
Christian Heitman <cheitman@quarkslab.com>

Quarkslab

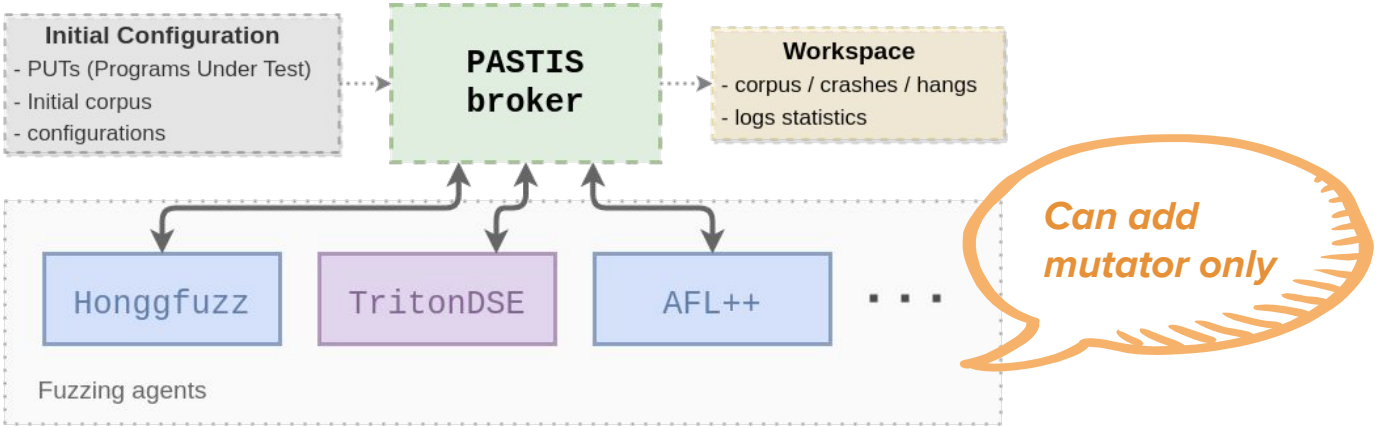
Which approach to choose ?



PASTIS: Ensemble Fuzzing

Goal

Combining greybox and whitebox fuzzing to leverage their respective strengths *(on OSS software).*



Key aspects:

- broker based *(for input sharing)*
- libpastis *(library to integrate in the fuzzer)*
- message-queuing based (TCP with ZeroMQ)

Fuzzers:

- Honggfuzz
- AFL++
- TritonDSE
- Sydr-Fuzz

What's up since SBFT-2023 ?

News:

- Full binary fuzzing compatibility *(no source needed!)*
  - Honggfuzz via QBDI instrumentation
  - AFL++ with QEMU mode
  - TritonDSE, Sydr *(natively binary-based)*
- Multi-layered broking system
- Input filtering mechanism *(at broker level)*

⇒ Yet nothing specific to improve mutation quality

(also DSE RAM usage have been an issue)

Thank you

Contact information:

Email: contact@quarkslab.com

Phone: +33 1 58 30 81 51

Website: quarkslab.com

@quarkslab

Quarkslab