Contribution ID: **366** Type: **not specified**

Fuzzing the Verifier with a Test Oracle

Several fuzzers are able to target the BPF verifier, some achieving high coverage. They are fairly efficient at uncovering deadlocks, unnecessary warnings, and memory errors, but struggle to uncover false negatives: cases where the verifier incorrectly accepts a program. Without a test oracle for these false negatives, fuzzers remain silent.

This talk proposes a new test oracle for the verifier, inspired by recent research results [1] and discussions at last year's Linux Plumbers [2]. When enabled, the oracle preserves the verifier's expectations on registers and stack slots at pruning points. Then, at runtime, the interpreter or JIT compilers check that concrete values are within the verifier's expectations, issuing a warning if any unexpected value is found.

The RFC patchset will be posted to the mailing list before the conference. It relies on a BPF map to save the verifier states (and potentially expose them to userspace for debugging) and focuses on scalar values for now.

1 - https://www.usenix.org/conference/osdi24/presentation/sun-hao
2 - https://lpc.events/event/18/contributions/1933/

Primary author: CHAIGNON, Paul (Isovalent)

Presenter: CHAIGNON, Paul (Isovalent)

Session Classification: eBPF Track

Track Classification: eBPF Track