Contribution ID: **404** Type: **not specified**

The State of eBPF Fuzzing

Thursday, 19 September 2024 10:00 (30 minutes)

Over the past ten years, many fuzzers have been written specifically for the BPF subsystem. They follow diverse strategies, either porting the verifier to userspace [1, 2], describing the BPF syntax in details [3, 4], or devising new test oracles [5, 6]. Several such fuzzers have uncovered bugs and vulnerabilities, but none has a very good coverage of the whole BPF subsystem.

This talk will compare the various BPF fuzzing strategies, with their scope, strengths, and weaknesses. We will then focus on the syzkaller fuzzer, which has the broadest scope and most up-to-date descriptions, to highlight areas of BPF that have received less attention. The aim of this talk is to discuss approaches to improve the status quo.

1 - https://github.com/iovisor/bpf-fuzzer
2 - https://github.com/atrosinenko/kbdysch
3 - https://github.com/google/buzzer
4 - https://github.com/google/syzkaller
5 - https://dl.acm.org/doi/10.1145/3627703.3629562
6 - https://www.usenix.org/conference/osdi24/presentation/sun-hao

Primary author: CHAIGNON, Paul (Isovalent)

Presenter: CHAIGNON, Paul (Isovalent)

Session Classification: eBPF Track

Track Classification: eBPF Track