Contribution ID: **378** Type: **not specified**

Making Sense of Tristate Numbers (tnum)

Thursday 19 September 2024 13:00 (30 minutes)

Despite its vast use in the BPF verifier, tnum (tristate numbers or tracked numbers, i.e. var_off field in struct bpf_reg_state) remain less understood compared to its more intuitive min/max counter parts, and for good reason (also perhaps to its own peril) —it works very well and comes with a comprehensive set of APIs; leaving little reason for further mangling and learning.

Nevertheless, good code should be read and understood. More importantly, there could never be too many reviewers when it comes to the safety-critical value tracking logic. As such, this talk aim to discuss tnum in depth, covering:
- concepts
- how it works (i.e. implementation)
- limitations
- explanation of (some) existing operators
- how its used
- related bugs
- crafting operator from scratch
- testing & verification

The goal is that by the end of the talk, the audience will feel much more confident when it comes to reasoning, reviewing and writing tnum-related code.

Primary author: YU, Shung-Hsi (SUSE)

Presenter: YU, Shung-Hsi (SUSE)

Session Classification: eBPF Track

Track Classification: eBPF Track