



Contribution ID: 237

Type: **not specified**

Advanced BPF profiling techniques: how to escape the curse of NMI and fetch ELF contents at runtime

Writing basic BPF-based profilers nowadays isn't too hard. The challenges start when one needs to go a step further beyond just capturing a bunch of stack traces. When profiler needs to capture user data reliably bypassing restrictions of NMI and/or non-sleepable context, that's when the real fun begins.

This talk will describe recent advancements in BPF tracing domain which now allow BPF programs to escape limitations of NMI context and perform reliable user memory reading in "benign" sleepable BPF mode. We'll also demonstrate how it's now possible to fetch the contents of thread-local variables at runtime (among other things), with no upfront preprocessing required, just by fetching ELF binary contents on demand.

Primary author: NAKRYIKO, Andrii (Meta)

Presenter: NAKRYIKO, Andrii (Meta)

Session Classification: eBPF Track

Track Classification: eBPF Track