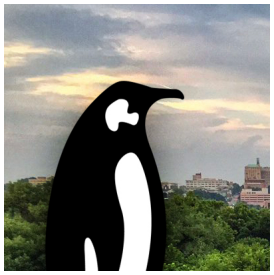

Contribution ID: **285** Type: **not specified**

Verifying the Verifier: eBPF Range Analysis Verification

Monday, 13 November 2023 11:30 (30 minutes)

This talk will present our automated tool, Agni, to check the correctness of range analysis in the Linux kernel's eBPF verifier. Agni automatically extracts the semantics of the verifier's range analysis in logic (SMT) from the kernel's C source code. We use abstract interpretation theory to provide a formal specification of the soundness of range analysis. Our tool checks the verifier's range analysis against this specification. When the soundness checks fail, it implies a possibility that a register's actual value during program execution can deviate from the verifier's beliefs regarding that register's value. Agni further synthesizes an eBPF program that can trick the verifier into constructing a range for a register that deviates from its actual concrete value.

We ran Agni on 16 kernel versions, starting from 4.14 (the earliest we support). We were able to show that the range analysis in kernel versions 5.13 through 5.19 (the latest we checked) are sound. In older kernels where our soundness checks failed, in ~97% of the cases, Agni was able to synthesize eBPF programs that manifest bugs in the verifier.

The talk will consist of:
- An overview of why the eBPF verifier implements a non-standard range analysis.
- How we extract the semantics of the verifier's range analysis code into logic.
- How one goes about proving the soundness of range analysis, and our soundness specification.
- An overview of how Agni constructs (synthesizes) eBPF programs that manifest bugs in the verifier.
- The results of our experiments on the 16 kernel versions we tested.
- A demo of the entire toolchain in action: how we go from kernel source code to actual eBPF programs that manifest bugs in the verifier.
- A discussion about the future direction with potential for checking other parts of the eBPF verifier analyses for soundness.

Some useful links:
- Our tool Agni: https://github.com/bpfverif/agni
- A collection eBPF programs synthesized by Agni, that manifest bugs in the eBPF verifier's range analysis, with instructions on how to run them: https://github.com/bpfverif/ebpf-verifier-bugs
- Our recent post about Agni to the kernel mailing list: https://lore.kernel.org/bpf/SJ2PR14MB6501E906064EE19F5D1666BFF93BA@SJ2PR1

Primary authors: VISHWANATHAN, Harishankar (Rutgers University); SHACHNAI, Matan (Rutgers University); Dr NAGARAKATTE, Santosh (Rutgers University); Dr NARAYANA, Srinivas (Rutgers University)

Presenter: VISHWANATHAN, Harishankar (Rutgers University)

Session Classification: eBPF & Networking

Track Classification: eBPF & Networking Track