Contribution ID: **374** Type: **not specified**

Mitigating Spectre-PHT using Speculation Barriers in Linux eBPF

Friday 20 September 2024 12:30 (30 minutes)

To mitigate the Spectre-PHT (v1) vulnerability, mitigations which reject potentially-dangerous unprivileged eBPF programs have been merged into the kernel [1]. To assess their potential real-world impact, we analyze 364 object files from open source projects (Linux Samples and Selftests, BCC, Loxilb, Cilium, libbpf Examples, Parca, and Prevail) and find that this affects 31% to 54% of programs.

Motivated by this, we explore the possibility of mitigating Spectre-PHT using speculation barriers in eBPF. For this, we prototype the **VeriFence** [2] kernel patch set, which optimistically attempts to verify all speculative paths but falls back to speculation barriers when unsafe behavior is detected. As expected, this allows all real-world application programs in our dataset to be successfully loaded into the kernel with all mitigations enabled. We measure the overhead of VeriFence for event tracing and stack-sampling profilers, and find that it increases eBPF program execution time by 0% to 62%. Further, for the Loxilb network load balancer, we measure a 14% slowdown in SCTP performance but no significant slowdown for TCP. Besides discussing the feasibility of unprivileged eBPF as whole and whether mitigations should be enabled for privileged eBPF, we present the lessons learned and potential for optimizing the VeriFence prototype further.

1. bpf: Fix leakage under speculation on mispredicted branches (Linux Commit #9183671a)
2. VeriFence: Lightweight and Precise Spectre Defenses for Untrusted Linux Kernel Extensions (arXiv)

Presentation PDF
Patch Series Draft

Primary authors: GERHORST, Luis (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)); HERZOG, Henriette (Ruhr-Universität Bochum (RUB)); WÄGEMANN, Peter (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)); OTT, Maximilian (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)); KAPITZA, Rüdiger (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)); HÖNIG, Timo (Ruhr-Universität Bochum (RUB))

Presenter: GERHORST, Luis (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU))

Session Classification: eBPF Track

Track Classification: eBPF Track