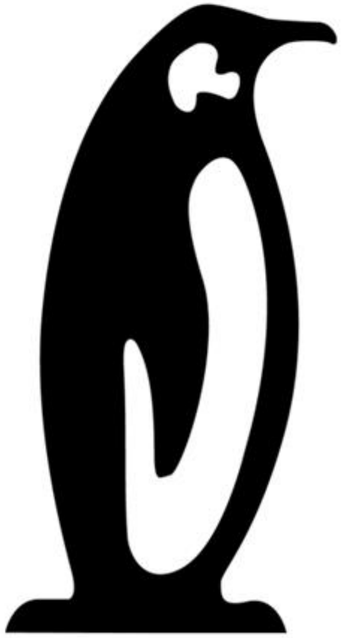

Linux Plumbers Conference

Vienna, Austria | September 18-20, 2024

State of CPU side-channel vulnerabilities and mitigations

Pawan Gupta <pawan.kumar.gupta@linux.intel.com>

LINUX
PLUMBERS
CONFERENCE Vienna, Austria / Sept. 18-20, 2024

whoami

- Kernel engineer at Intel
- Contributed to mitigating:
  - BHI
  - TAA
  - RFDS
  - Retbleed
  - MMIO Stale Data

Mitigation challenges

- **Problem: Trusted workloads pay the penalty**

Introduce: Selective mitigation

- Skip mitigation for trusted workloads.
- Admin chooses which workloads are trusted.
- Separate kernel entry/exit path for trusted applications.

- Example using cgroups:
  - Add admin-only attributes
    - /sys/fs/cgroup/<trusted>/cpu.skip_mitigation = 1
    - /sys/fs/cgroup/<untrusted>/cpu.skip_mitigation = 0

- Optimize trusted<-->untrusted switching with Core scheduling

- **Problem: Complex mitigation selection for user.**

Introduce:

- mitigations=paranoid
- mitigations=light

Problem: Establish criteria what should be mitigated by default?

- Demonstrated threat
- Cost of attack
- Performance impact, etc.
- Avoiding software mitigations when hardware alternatives are present