Contribution ID: **28** Type: **not specified**

x86 Microconference

CFP closes on July 12th.
X86-focused material has historically been spread out at Plumbers. This will be an x86-focused microconference. Broadly speaking, anything that might affect arch/x86 is on topic, except where there may be a more focused discussion occurring, like around Confidential Computing or KVM.

This microconference would look at how to address new x86 processor features and also look back at how older issues might be made less painful. For new processor features like APX, what is coming? Are the vendors coordinating and are they compatible? For older issues like hardware security vulnerabilities, is the current approach working? If not, how should they be dealt with differently? Can new hardware features or vendor policies help?

As always, the microconference will be a great place for coordination among distributions, toolchains and users up and down the software stack. All the way from guest userspace to VMMs.

Potential Problem Areas to Address:

- CPU Vulnerabilities
- Default options for mitigations
- Are they being mitigated right?
- Are hardware interfaces for Data Independent Execution being plumbed into applications?
- FRED - new kernel entry/exist hardware
- What doors does FRED open?
- What things will be FRED-only?
- CET - Control flow Enforcement
- Security Hardware feature, includes Shadow Stacks and Indirect Branch Tracking
- Kernel Shadow Stacks
- User IBT/FineIBT?
- APX - new Intel ISA, more general purpose registers (GPRs) ⋯(and more)
- What would a kernel with more GPRs look like?
- What plumbing implications does the MPX XSAVE offset reuse have?
- x86-S - Some future x86 CPUs may have a Smaller feature set and not be backward compatible
- SIPI64 is nice-ish, but other aspects are going to be especially nasty for virt
- Memory Protection Keys
- Userspace: Should we expand the ABI to cover more use cases?
- Can it be used to improve userspace security?
- Kernel: Page Table protections, mitigate malicious writes
- Memory Tagging / LAM / UBI
- CoCo Pain Points - what should the vendors be doing to ease them?
- XSAVE - Stay the course, or give up?
- How to ease the pain on gdb of AMD and Intel format divergence?

- x86 feature detection
- X86_FEATURE* - Is the code patching variants worth it? Should we pare down the choices? Do they really need to be per-cpu or should they be global?
- Should we impose more order in early boot about when it is OK to start checking feature flags or other parts of ‘boot_cpu_data’? Is this a good idea? Should ‘cpuinfo_x86’be slimmed down further? - DaveH Boot
- Can the decompressor be entirely separated from the rest of the kernel proper?
- What old code imposes a maintenance burden and might be removed?

Primary authors: PETKOV, Borislav; HANSEN, David

Track Classification: LPC Microconference Proposals