Linux Kernel Getting New Option So SSBD Isn't Over-Protective - Helping Performance

By Roy Schestowitz
Created 31/01/2019 - 10:46pm
For the Linux kernel's Speculative Store Bypass Disable (SSBD) handling for Spectre Variant 4 protection is support for processes opting into force disabling of speculation via a prctl() interface. Currently when speculation is disabled, that is carried through to new processes started via the execve() system call. But a new bit will allow clearing that state when a new program is started by a process otherwise relying upon PR_SPEC_DISABLE, in what will help the performance in such cases.

Queued for introduction to the mainline Linux kernel is a new PR_SPEC_DISABLE_NOEXEC option for prctl as part of the Speculative Store Bypass Disable options but where the state is cleared on execve() calls. The premise is that programs opting into disabling speculation are doing so, but programs that aren't vulnerable to the speculation-related misfeatures normally aren't checking to see that the PR_SPEC_ENABLE bit is set rather just assuming the status quo. Thus with the current PR_SPEC_DISABLE behavior, programs spawned via execve() may be protected when they really don't need to be and carrying with that the added performance overhead.

[3]

Also: [A new Linux Foundation effort for the edge][4]

Linux Security

Source URL: [http://www.tuxmachines.org/node/120153](http://www.tuxmachines.org/node/120153)

Links: