Contribution ID: **295**

Type: **not specified**

Module Error Injection with eBPF

We build robust kernel code by properly handling errors and recovering gracefully. But many critical error conditions are hard to replicate in testing, so error injection becomes essential for validation. Past error injection approaches were often considered too intrusive and got rejected [1].

This talk presents moderr, an eBPF tool using libbpf for error injection in the kernel module subsystem. The tool targets paths that are otherwise difficult to simulate and validates both code correctness and memory leak detection in error scenarios.

The approach uses eBPF's lightweight nature where you only need to annotate functions in-kernel that are error injectable, while the complex error injection logic lives in a separate standalone tool. This addresses the intrusiveness problem that killed previous attempts.

I'll show the current implementation [2], share what we learned from community feedback [3], and discuss how moderr could evolve into a generic error injection framework for kernel developers.

Link: https://lore.kernel.org/all/20210512064629.13899-1-mcgrof@kernel.org/ [1]
Link: https://git.kernel.org/pub/scm/linux/kernel/git/da.gomez/linux.git/?h=b4%2Fmodules-error-injection [2]
Link: https://lore.kernel.org/all/20250122-modules-error-injection-v1-0-910590a04fd5@samsung.com [3]

Primary author: GOMEZ, Daniel

Presenter: GOMEZ, Daniel

Session Classification: Linux System Monitoring and Observability MC

Track Classification: Linux System Monitoring and Observability MC