Contribution ID: **369** Type: **not specified**

Applying Program Verification to Linux Kernel Code: Challenges, Practices, and Automation

Friday 12 December 2025 10:35 (25 minutes)

To maintain software safety, defining specifications and ensuring that implementations meet them are both important. The former has become popular in the Linux kernel in various ways [1,2], while the latter still depends on developers' manual effort. Recent advances in techniques and tools, however, have made it feasible to systematically apply program verification to Linux kernel code.

In this talk, we share our experience and practices from ongoing work on verifying task-scheduler code of the Linux kernel. We illustrate the challenges we encountered and how verification can be effectively applied in practice, through case studies (e.g., [3,4]) where proving the correctness of certain kernel features resulted in uncovering real bugs (e.g., [5,6]). Furthermore, we present our work to automate this process as much as possible, making verification more practical and scalable. Our goal is to explore how verification can be made a practical part of the Linux kernel development process.

[1] https://lore.kernel.org/all/20250614134858.790460-1-sashal@kernel.org/ "Kernel API Specification Framework"
[2] https://lore.kernel.org/all/20250910170000.6475-1-gpaoloni@redhat.com/ "Add testable code specifications"
[3] Julia Lawall, Keisuke Nishimura, and Jean-Pierre Lozi. 2024. Should We Balance? Towards Formal Verification of the Linux Kernel Scheduler. SAS 2024.
[4] Julia Lawall, Keisuke Nishimura, and Jean-Pierre Lozi. 2025. Understanding Linux Kernel Code through Formal Verification: A Case Study of the Task-Scheduler Function select_idle_core. OLIVIERFEST '25.
[5] https://lore.kernel.org/all/20231030172945.1505532-1-keisuke.nishimura@inria.fr/ "sched/fair: Fix the decision for load balance"
[6] https://lore.kernel.org/all/20231214175551.629945-1-keisuke.nishimura@inria.fr/ "sched/fair: take into account scheduling domain in select_idle_smt()"

Primary author: NISHIMURA, Keisuke

Presenter: NISHIMURA, Keisuke

Session Classification: Safe Systems with Linux MC

Track Classification: Safe Systems with Linux MC