WG Summary

Goal of the working group:

Study how use of analysis tools may impact qualities of collaboratively developed open-source software elements used in Linux-based systems

* Use of analysis tools:
  + Includes
* May impact:
* Collaboratively developed software:
* Open question:
  + analysis tools
* Start with the collaboratively-developed Linux kernel.
* The elisa test & verification server is up and running.

Fuzzing the kernel with Syzkaller

The group has set up an syzkaller instance fuzzing the kernel and identifying bugs at https://syzkaller.elisa.tech.

These fuzzing campaigns have identified:

* Four reports have syzkaller reproducers.
* Six reports have C reproducers.
  + 5 cases of “BUG:“ warnings
  + 5 cases of General protection fault
  + 2 cases of Inconsistent lock state
  + 10 cases of INFO: Task hung
  + 1 case of INFO: trying to register non-static key
  + 11 cases of KASAN: use-after-free
  + 8 cases of Memory leak
  + 13 cases of Possible deadlock: No reproducer
  + 14 cases of WARNING: 2 C reproducers, and one syzkaller reproducer
  + For completeness:
    - No output from test machine
    - Suppressed report
    - SYZFAIL:

Actions derived from that campaign:

* Report issues.
* Regularly track which issues were resolved in the latest stable versions.

Questions:

* <https://elisa-builder-00.iol.unh.edu/syzkaller/>