Contribution ID: **226** Type: **not specified**

Assessing kernel system call correctness by testing

Tuesday, 25 August 2020 08:30 (30 minutes)

Key question: Can system calls be regarded as independent and consequently tested individually rather than in some form of use-case specific call sequence?

The kernel has a set of asynchronously operated state machines, e.g., RCU, buddy-system, ratelimits of all sorts, that cause a repeated identical system call to take different paths in consecutive invocations. The model thus is that the result of a system call is effected by two aspects:

1. the formal input, i.e., parameters to the system call, and
2. the kernel's global system space.

As the global system state space is modified by all active processes, the "global system state" input is uncontrolled (and assumed to be uncontrollable) whereas the formal input, i.e., the arguments pass to system_call_X(), is assumed to be held constant.
In that case, the assumed path variability is assumed to be causally related to the code being conditioned in part on the global system state. To now judge the correctness of the system_call_X() implementation, the repeated tests need to be conducted while allowing the system state space to freely roam around.

In practical terms, if we have two processes, i.e., process A calling fd = open(...); ret = read(fd,...), and process B, calling other system calls, X, Y, Z, etc., be it on the same or different cores, do we expect the execution path of the read() to causally depend on the order or unrelated calls concurrently being executed on the system?

This is relevant for dependability as:
If calls may be treated as independent, then assessment of correctnes can be done by repeated testing of individual calls while exercising some background load of arbitrary type. If this assumption is invalid due to the design of the kernel, then assessment of correctness is only possible by testing permutations of call sets.

We would like to discuss: What arguments would you see in favor of "calls are independent" or to bolster the claim of "calls are non-independent"?

I agree to abide by the anti-harassment policy

I agree

Primary authors: Dr PETERSOHN , Jens (Elektrobit Automotive GmbH); Prof. MC GUIRE, Nicholas (OpenTech)

Presenters: Dr PETERSOHN , Jens (Elektrobit Automotive GmbH); Prof. MC GUIRE, Nicholas (OpenTech)

Session Classification: Kernel Dependability & Assurance MC

Track Classification: Kernel Dependability & Assurance MC