OS-State–Aware Fuzzing for Worst-Case Response Times

Alwin Berger[†] and Simon Schuster[§] and Peter Wägemann[§] and Peter Ulbrich[†]

[†]*Technische Universität Dortmund,* [§] *Friedrich-Alexander-Universität Erlangen-Nürnbgerg*

Abstract

Determining the worst-case response time remains a significant challenge in developing real-time systems. These input-to-output latencies are composed of the worst-case execution times of the individual tasks plus the interference and administrative overheads caused by preemptive scheduling, interrupts, and platform specifics. One possible way to estimate these costs is static analysis of the processes and operating system, typically burdened with high pessimism or even unavailable for the given execution platform. Therefore, measurement-based timing analysis of tasks and systems is widely used. However, worst-case measurements are, for example, challenged by the need to know the triggering worst-case inputs. Consequently, methods for structured exploration of execution paths and OS states are required. Recently, the fuzzing of input parameters has gained popularity in the context of system security. However, the goal here is to study computational DoS attacks, which are only indirectly related to the worst-case timing behavior of the system.

We aim to enable fuzzing of WCET/WCRT input patterns in complex system settings without prior knowledge. We first highlight the challenges in adapting existing fuzzing techniques for timing analysis and show how to adjust feedback function and queuing. Consequently, we discuss the changes and extensions necessary for state awareness. That is how to make OS states, hardware interactions, and asynchronous inputs (i.e., interrupts) integral to fuzzing, thus making their impact accessible to the analysis. Next, we highlight the necessary changes to the emulator and tracing and implement adapted mutators and schedulers. Finally, we show the viability of our approach by presenting preliminary results.