Formal, machine-checked verification of concurrent OS-code

(Internship @ Data61, CSIRO, Sydney, Australia)

The project

Formal verification is important in safety critical software. To make sure a verified system runs correctly one also needs to provide formal guarantees about the correctness of the underlying operating system (OS) that the program runs on. Data61's Trustworthy Systems group is famous for its formal verification of the seL4 microkernel in the Isabelle-HOL theorem prover.

Most recent successfully verified operating systems, including seL4, run on uniprocessor platforms and with interrupts largely disabled. However, there is an increasing demand for verified real-time operating systems (RTOS) which require support for concurrency.

Our team is aiming at providing frameworks for reasoning about concurrency in OS-code [0]. In particular, our main two projects are to model and verify

1. the small, embedded eChronos RTOS [1], and
2. a multicore version of seL4.

Both seL4 and the eChronos RTOS have been embedded in high-assurance autonomous flying vehicles that have been developed in collaboration with industry and university partners.

In the eChronos verification project we have successfully proved the correctness of eChronos' scheduling behavior in the presence of concurrency [2,3]. This proof is for an abstract model of the eChronos RTOS, using a framework adapted from the foundational Owicki-Gries concurrency method for shared-variable programs.

The verification of multicore seL4 is the project we are currently focused on. It targets the "big lock" version of seL4 [4] and is aiming at providing a formal model of interleaved execution. This also includes investigation of the best logic and concurrency model to use.

The candidate would be embedded in our team. To begin with they would work on investigating and comparing various approaches in terms of their expressiveness, applicability and scalability, and/or on improving the automation, and compositionality of the frameworks. The exact work to be done will be set according to the applicant's interests and strengths.

References

[0] https://ts.data61.csiro.au/projects/concurrency/os-concurrency
[1] https://ts.data61.csiro.au/projects/TS/echronos
[2] "Controlled owicki-gries concurrency: reasoning about the preemptible eChronos embedded operating system" MARS'15. https://arxiv.org/abs/1511.04170
[3] "Proof of OS scheduling behavior in the presence of interrupt-induced concurrency" ITP'16. https://ts.data61.csiro.au/publications/nicta_full_text/9261.pdf
[4] "For a microkernel, a big lock is fine" APSys'15. https://ts.data61.csiro.au/publications/nictaabstracts/8768.pdf

General Information

Data61 is Australia's leading digital research powerhouse, offering the research capabilities, IP and collaboration programs to unleash the country's digital and data-driven potential, with a global context. By driving collaboration across industry, academia, government and the startup space, Data61 is able to help existing industries transform, and act as a catalyst in the creation of new technology-based industries.

The intern will be part of *Concurrency and Protocol Verification* (http://ts.data61.csiro.au/projects/concurrency/home.pml), a highly motivated group with different backgrounds (e.g., formal methods and network engineers), working at different institutes (Data61, UNSW). The successful applicant will work together with Corey Lewis and the rest of the *Concurrency in Operating Systems* team.

Sydney is the largest and most populous city in Australia. It is located on Australia's south-east coast of the Tasman Sea. With an approximate population of 5 million in the Sydney metropolitan area the city is the largest in Oceania. Sydney also ranks among the top 10 most liveable cities in the world according to Mercer Human Resource Consulting and The Economist.

Contact Information

If you have any questions concerning the internship, please do not hesitate to contact Corey Lewis.