Adapting to demand- seL4 proofs and proof engineering practice

Submitted by Anonymous on Fri, 08/14/2020 - 12:22pm. Contributor: Matthew Brecknell

In this talk, we'll discuss some of our experiences scaling the formal verification of the seL4 microkernel to meet customer demand for increasingly complex requirements.

The formal verification of the seL4 microkernel [1] broke new ground, showing that comprehensive verification of a complex software system was possible. That initial effort required solutions to many proof engineering problems, for example, how to decompose refinement proofs so that the work could be distributed across a team [2].

Since the successful deployment of seL4 in the DARPA HACMS program, and the 2014 open-source release, there has been a growing interest in using seL4 in applications across a range of CPU architectures and platform configurations. At the same time, the kernel has gained significant new features, including symmetric multiprocessing (SMP), and support for real-time mixed-criticality systems (MCS). Verification of new ports and features is work in progress.

This growth has presented our proof engineering team with new grand challenges. We are no longer building new proofs about a relatively stable system. Rather, we're now adapting a large collection of existing proofs to rapid and sometimes radical changes to that system. Multi-processing requires changing the execution model underlying specifications and proofs [3]. Mixed-criticality features add complex interactions to interprocess communication (IPC) and scheduling [4], the two primary functions of a microkernel, while also demanding proofs of more interesting properties. Supporting many CPU architectures and platform configurations requires better abstraction of platform-specific aspects, especially virtual memory structures.

In this talk, we'll look more closely at these challenges, from both technical and organisational perspectives. We'll discuss some of the approaches we've taken so far, as well as ideas we have to improve on these in the future. While much of this work is currently domain-specific, we think that we will be able to extract general principles that will be useful to other verification projects.

References:

Matthew Brecknell works with the Trustworthy Systems group at CSIRO's Data61, developing proofs and verification tools for the seL4 microkernel and its ecosystem. He has also consulted with other organisations doing verification in this ecosystem, and is a member of the Technical Steering Committee of the seL4 Foundation. He has contributed to the verification of the x86-64 port of seL4, and new features for mixed-criticality real-time systems. He is currently working on binary verification for the RISC-V port of seL4.
Other available formats:

Adapting to demand- seL4 proofs and proof engineering practice

Matthew Brecknell

License: Creative Commons 2.5

Presentation HCSS 2020