Capability Machine Meeting

March 13, 2020

Current Meeting

Status report of mechanization:

- A looping version of the awkward example has been proven, which turned out not to exactly correspond to the original awkward example
- Discussion on how we should build the WP rules on top of the semantics, and if we should model WP and semantics after each other or no
- Most of the refactoring of the WP rules and the corresponding ftlr cases has been completed.
- The ftlr case for Store, and rewriting parts of the WP for load and store in order to prove their concrete WP cases remain.

Status report of IO-Drivers:

- A basic introduction to IO-related concepts of MMIO, Port-mapped IO, DMA, IOMMU
- IO in Linux 2.5
- Discussion on what model we could\should aim for. The principles that were discussed in the above introduction were very general, and we should think about what things are easy\hard to model in our current formalism, and given this set of features, look for a realistic architecture and corresponding driver we could perhaps base our implementation on. In this context, aRTOS, Contiki and CheriOS were mentioned.

Coming Week

Work on the mechanization front during the coming week:

- Aïna: finding a fix to convert the proof of the current awkward example to a proof of the classic awkward example.
- Thomas, Alix, Armaël: finishing the refactoring of the WP cases. Thomas will write out the ftlr case for Store.
- Alix will take a closer look at the WP rules for StoreU, LoadU and PromoteU in the uninitialized branch.
- Thomas and Armaël will take a closer look at the systems that were mentioned (particularly CheriOS) and will write out a proposal annex spec. for the features our driver might want to support, its operational semantics and the corresponding statement of security.