Capability Machine Meetings

February 5, 2020

1 Week 6

Status report of mechanisation:

- FTLR is done
- Two examples are done (one that depends on LSE, another that depends on WBCF)

Current work on mechanisation (during week 6):

- Thomas: refactoring the FTLR Store case (one goal is to find out if there is a nicer way to prove each FTLR case, another is to consolidate certain equivalent definitions)
- Aïna: creating a spec for scall, and use that spec for much shorter proof of the examples. This involves also generalising the examples over some contiguous region of memory.

Steps needed to mechanise uninitialised capabilities:

1. Update the operational semantics
2. Design the ghost state
3. Weakest precondition rules (either update existing ones or create new ones)
4. Define the logical relation for the new U permission
5. FTLR (either update existing instructions or prove new cases)
6. Make a new calling convention and prove that it satisfies the scall spec

Alix will start out by updating the operational semantics.
During week 7, Thomas and Aïna will determine the ghost state and the new LR definition. After that the weakest precondition/FTLR work (Alix/Thomas) can be done in parallel with the new calling convention (Aïna)

In week 8, we will discuss more concretely what refactoring is needed to get the work into a more presentable state.

Reading list:

- OPCL paper (Armaëlle has offered to present the paper), Thomas can give a small presentation of the work he did in expanding the Iris implementation to handle effects (printing)
- The high level benefits of low level sandboxing
- Benjamin Pierce ongoing work on property-based testing of a stack-protection micropolicy: [1] [2] [3]

[1] https://prosecco.gforge.inria.fr/personal/hritcu/talks/2017-12-18-Secure-Compilation-Infoiasi.pdf
[2] https://web.cs.wpi.edu/~rjwalls/nesd/slides/SullivanDraperNESDFall2016Dover.pdf
[3] https://semiwiki.com/ip/arm/7839-dover-microsystems-spins-new-approach-to-security/

SAIL:

- Armaëlle will look into SAIL
- One goal is to investigate how the current idealised machine can be extended to make it more realistic. To start out with this extension could be to add one of the following:
  - Virtual memory
  - Memory mapped I/O

In general, we should think about more security related properties (other than LSE and WBCF) that we can enforce with capabilities, and how to make the properties understandable for non PL people.