Formally Proving Security Properties of CHERI Architectures

Thomas Bauereiss    Kyndylan Nienhuis    Peter Sewell
16 June 2019

University of Cambridge firstname.lastname@cl.cam.ac.uk
ISA Specifications

Need for machine-checked proofs of security properties
Key question: Is the Sail model of this large specification usable for formal verification?

Address translation: Most complex part of ARMv8 model!

- 9000 lines of specification required
- Page table walk: Over 500 LOS excluding helper functions
  - . . . and there are lots of page table helper functions
- Involves iteration, variable-length bitvectors, memory effects, nondeterminism, . . .
We define a simplified, purely functional characterisation of address translation suitable for reasoning about non-system code.

About 500 lines of Isabelle total.

**Theorem**

_Simplified address translation is equivalent to full ARMv8 address translation under certain assumptions:

*user mode, no virtualisation, valid translation tables, hardware updating of translation table flags*_

Uncovered a small bug in the ASL specification, reported to ARM, fix in v8.5
Security Properties

Stating and verifying fundamental security properties of CHERI architectures

- Characterisation of how individual instructions are allowed to use and manipulate capabilities
- Upper bounds on capabilities that arbitrary code running in a compartment can obtain from its initial capabilities
- Corollary: Isolation of a user space compartment under specific conditions
Example: Intra-Instruction Property

... let \( cs\_val \) = readCapReg(cs); let \( ct\_val \) = readCapReg(ct); ...

if not(ct_val.permit_unseal) then raise_c2_exception(...) else

writeCapReg(cd, 
{unsealCap(cs_val) with global=(cs_val.global &
ct_val.global)})

\[
t = [E\_read\_reg(cs, c), E\_read\_reg(ct, c'), E\_write\_reg(cd, c'')]
\]

\[
c'' \in derivable(\{c, c'\})
\]
Theorem
If a sequence of arbitrary instructions of a CHERI ISA is executed in state $s$ leading to state $s'$, if

- no exception is raised,
- no capability invocation occurs, and
- address translation stays invariant,

then $\text{reachableCaps}(s') \subseteq \text{reachableCaps}(s)$. 
Proving the Properties

- Properties proved for CHERI-MIPS

- Initial results for CHERI-ARM research prototype:
  Proved properties of selected instructions

- **Scalability challenge:** 64-bit v8.5 specification contains
  - 66558 LOS for all 64-bit instructions
  - 3825 Sail functions
  - 561 registers
  - 981 instructions (each may be multiple assembly mnemonics)
  - ca. 800 calls to auxiliary functions per instruction on average

- Proof automation is crucial
Secure compartmentalisation

↑

T-CHERI properties of instructions

↑

Sail specifications of production ISAs
(complete with systems features)
and their CHERI extensions