Formally Proving Security Properties of CHERI Architectures

Thomas Bauereiss Kyndylan Nienhuis Peter Sewell

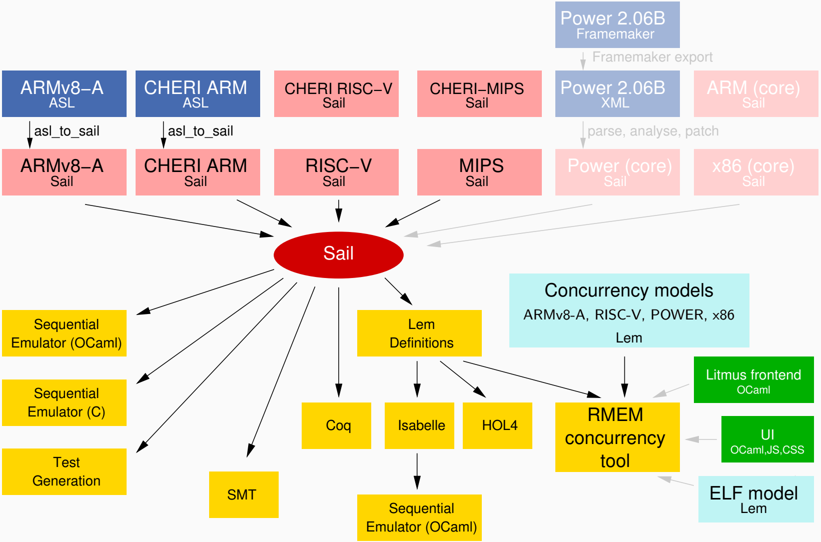
16 June 2019

University of Cambridge `firstname.lastname@cl.cam.ac.uk`

ISA Specifications

IA-32 Intel® Architecture
Software Developer's Man
VOLUME 2A: Instruction Set Reference, A-M
Intel® 64 and IA-32 Architectures Software Developer's Manual
VOLUME 2B: Instruction Set Reference, N-Z
2B
Intel® 64 and IA-32 Architectures Software Developer's Manual
VOLUME 3A: System Programming Guide Part 1
3A
Intel® 64 and IA-32 Architectures Software Developer's Manual
VOLUME 3B: System Programming Guide Part 2
3B
Intel® 64 and IA-32 Architectures Software Developer's Manual
VOLUME 1: Basic Architecture
1
Intel® 64 and IA-32 Architectures Optimization Reference Manual

Need for machine-checked proofs of security properties


Power 2.06B
Framemaker
Framemaker export
ARMv8–A
ASL
CHERI ARM
ASL
CHERI RISC–V
Sail
CHERI–MIPS
Sail
Power 2.06B
XML
ARM (core)
Sail
asl_to_sail
asl_to_sail
parse, analyse, patch
ARMv8–A
Sail
CHERI ARM
Sail
RISC–V
Sail
MIPS
Sail
Power (core)
Sail
x86 (core)
Sail
Sail
Concurrency models
ARMv8-A, RISC-V, POWER, x86
Lem
Sequential
Emulator (OCaml)
Lem
Definitions
Litmus frontend
OCaml
Sequential
Emulator (C)
Coq
Isabelle
HOL4
RMEM
concurrency
tool
UI
OCaml,JS,CSS
Test
Generation
SMT
ELF model
Lem
Sequential
Emulator (OCaml)

Proving Properties of ARMv8-A

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, . . .

Proving Properties of ARMv8-A

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)});
```

$$\begin{aligned} t = [&\texttt{E\_read\_reg}(\texttt{cs}, c), \\ &\texttt{E\_read\_reg}(\texttt{ct}, c'), \\ &\texttt{E\_write\_reg}(\texttt{cd}, c'')] \end{aligned}$$

$$c'' \in \mathit{derivable}(\{c, c'\})$$

Monotonicity of Reachable Capabilities

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 $\mathit{reachableCaps}(s') \subseteq \mathit{reachableCaps}(s)$.

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

Conclusion

Secure compartmentalisation

$\Uparrow$

T-CHERI properties of instructions

$\Uparrow$

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