Capable VMs: Intro to CHERI

Jeremy Singer

20 Aug 2020

What is a ‘capability’ ?

- token of authority
- hardware supported permission descriptor
- fine-grained memory protection mechanism

Capability replaces pointer

- all mem accesses must be authorized by capability
- cap is double width of ptr; it includes:
  - address
  - 1-bit validity
  - bounds info
  - perms (r/w/x)
  - other metadata

Enforced by Architecture

- we cannot ‘fake’ a capability
- we cannot change perms/bounds in a capability

Architectural Extensions

CHERI generally bolted on to existing RISC ISA.

- extra data storage — register file and memory tags
- extra instructions — to manipulate capabilities and access memory through them

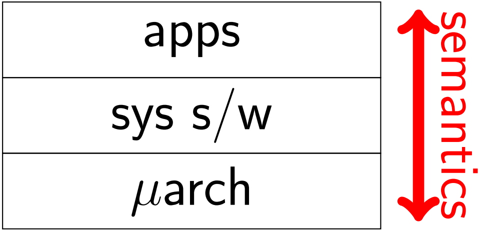
Key uses for CHERI (1)

- fine-grained memory protection in unsafe langs
  - like Valgrind only in hardware

Key uses for CHERI (2)

- software compartmentalization
  - Modern apps isolate components by running them in separate processes (with separate address spaces) — high overhead
  - with CHERI, we can isolate components within a single address space — lower overhead
  - *We want to do this for V8!*

CHERI Concept Stack



apps

sys s/w

μarch

semantics