Capabilities in Barrelfish

Mothy, Barrelfish crew, ETH Zurich
Channelling: David Cock, Simon Gerber, Gerd Zellweger, Reto Achermann, Lukas Humbel, and others
Delta from seL4: lots of types

• Many simultaneous architectures
  – Types for all hardware structures
• Hamlet:
  – DSL for capability type system
  – Fields, formats, semantics, retype rules
  – Generate dispatch/invoke/retype code
Some of the Barre1fish capability type system

PhysAddr

DevFrame

RAM

Null

Kernel

Notify

Domain

VNode_x86_64_pml4

VNode_x86_64_pdpt

VNode_x86_64_pdir

VNode_x86_64_ptable

VNode_x86_32_pdpt

VNode_x86_32_pdir

VNode_x86_32_ptable

VNode_ARM_l1

VNode_ARM_l2

VNode_AARCH64_l1

VNode_AARCH64_l2

VNode_AARCH64_l3

IO space

IRQTable

IRQ source

IRQ vector

Frame

Dispatcher

CNode

EndPoint

FCNode

SGX enclave

KernelControlBlock

Vnode_AARCH64_l1

VNode_AARCH64_l2

VNode_AARCH64_l3

Retype operations

23 April 2016

Cambridge Capability Workshop
Delta from seL4: physical address spaces

- Capabilities **relative** to some physical address space
  - Lots of these: 32-bit identifier
  - At least one per core, and usually more

⇒ Global ids even for resources that only accessible locally.

- Makes sense for modern hardware:
  - SoC / NoC messes
  - Remote buffer allocation at rackscale
  - Core sequestering in large machines

- Capability resolution process
  - To local address space
Simple example: Xeon Phi
Barrelfish is distributed

• **Multiple** capability databases
  – Coexisting in the same physical address space

• Capabilities must be copied between cores
  – May require **serialization**
  – Over some (not all) message channels

• Implications:
  – Need to identify all local copies of a capability based on bits, not reference.
  ⇒ Capabilities must be **indexed**
Retyping requires consensus

1. Copy
2. Retype
3. Retype
4. Copy

Core A can now forge capabilities!
CHERI and Barrelfish

• Format flexibility is great
  – Easy to represent BF capabilities as CHERI ones
  – Barrelfish mapping caps $\iff$ CHERI virtual caps?

• What privilege is required to retype?

• Big challenges:
  – Serialization
  – Revoke / retype
    • Quickly find all copies / derivations