MMU-based systems — Hybrid capability/MMU systems — Pure capability systems

MMU-based virtual address spaces

zlib **libssl**

Fetch command-line
HTTP client

libssl **libpng**

Netsurf
web browser

FreeBSD kernel

Hypervisor / Separation Kernel

CHERI CPU

zlib **libssl**
ABI wrapper

Legacy Fetch uses
pure-capability zlib
via an ABI wrapper

Address-space executive

libssl **libpng**

Hybrid Netsurf links
against legacy and
pure-capability code

Address-space executive

zlib **libssl**
ABI wrapper

Pure-capability
Fetch can still use
legacy code in
compartments

Address-space executive

class1

class2

libssl
ABI wrapper

Capability-based
unikernel OS +
applications

Address-space executive

FreeBSD kernel
+ CHERI support for userspace capabilities

Hypervisor / Separation Kernel
+ CHERI support for guest capabilities

CHERI CPU

class1 **class2**

class3

Capability-based
single-address-space
OS and applications

Address-space executive

CHERI CPU

□ 'Legacy' code compiled against a RISC ISA

□ 'Hybrid' code uses RISC pointers or source-code annotated CHERI capabilities

□ 'Pure-capability' code uses CHERI capabilities for all C pointers

□ Per-address-space memory-management and capability executive

□ Regular linkage

□ Compartment boundary