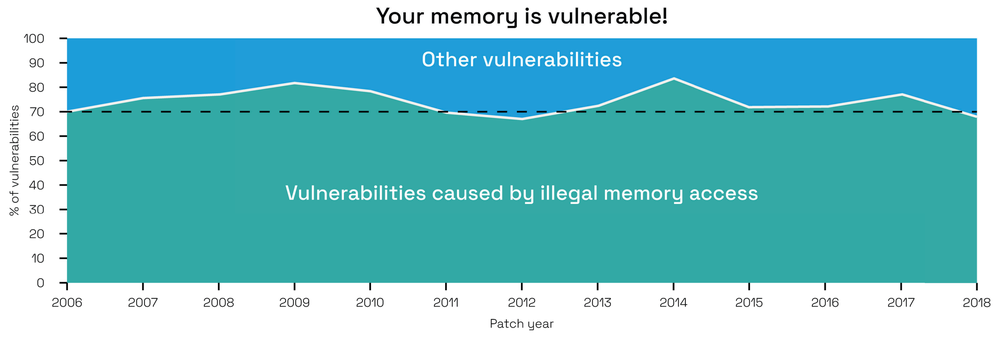
Commercializing CHERI on a Codasip A730 RISC-V application core

Andrés Amaya García

Codasip

→ The problem

Even the best programmers can introduce memory-related software bugs! Thus, memory safety continues to cause widespread and costly cyber security problems.



Source: "Trends, challenges and shifts in vulnerability mitigation", Matt Miller (MSRC), BlueHat IL 2019.

Memory safety vulnerabilities are costly. For example, losses due to the well-known OpenSSL heartbleed bug are estimated to exceed $500 million. So there is increasing interest, even from the White House and UK government, to mitigate these vulnerabilities.

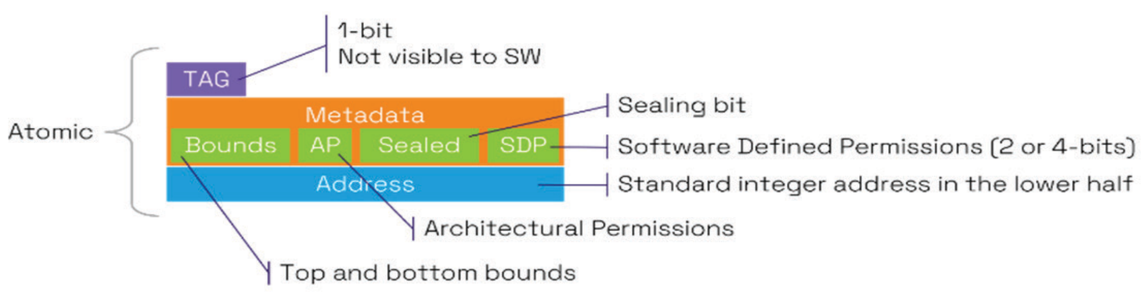
→ An emerging solution

The Capability Hardware Enhanced RISC Instructions (CHERI) provide a solution to memory access vulnerabilities, compartmentalization and control flow integrity without having to re-write all software.

CHERI has been primarily a research project until now! Codasip recently proposed a CHERI extension for RISC-V in collaboration with the University of Cambridge. Codasip also unveiled the first commercial implementation of CHERI-RISC-V: the A730 processor.

→ The CHERI extension for RISC-V

Capabilities are CHERI's beating heart! They are unforgeable tokens of authority that grant software the ability to perform a specific set of operations like load or store to memory.



Integer-based memory pointers are replaced with capabilities to protect memory. For example, the Program Counter (pc) is a capability that grants permission to execute instructions from a constrained region of memory.

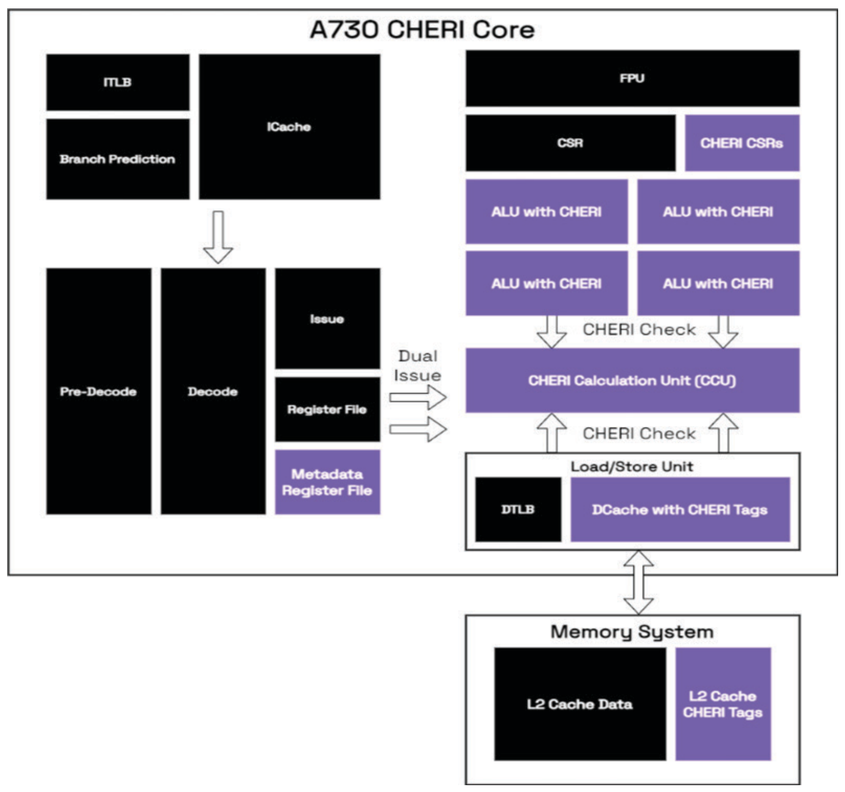
CHERI also extends RISC-V with new instructions that allow software to use these capabilities. In most cases, porting a program to CHERI RISC-V only requires recompiling.

Example: a desktop application port required change to 0.026% of 6M lines of code.

→ Commercializing CHERI on an A730

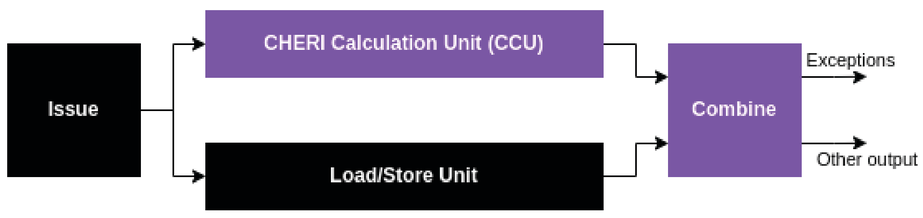
The A730 is the first commercially licensable processor implementing CHERI RISC-V. It is written using Codasip's CodAL processor description language to maximize customization.

The baseline A730 microarchitecture is 64-bit and dual-issue. It has been extended to efficiently handle capabilities and implement CHERI's new instructions and functions.



The register file, and some CSRs, are extended to 129 bits to accommodate capabilities. The memory system is extended to atomically handle capability tags while still using standard interfaces.

Most CHERI operations are implemented in the CCU including all safety checks. So every instruction is issued to the CCU along with another execution unit, like the Load/Store Unit for a store, and their outputs are combined when the instruction is committed.



→ Performance

The A730's performance is comparable to the performance of the baseline microarchitecture at the cost of about 4% more area.

Find out more