Standardizing CHERI -RISC-V

Abstract

Tariq Kurd, Codasip
Ben Laurie, Google

CHERI-RISC-V is a game-changing security extension for deterministic memory safety and memory compartmentalization. Once ratified, this standard will see huge adoption across the industry, greatly accelerating the ecosystem development, with multiple vendors planning silicon for 2025. CHERI aims to address the root cause of the problems that are caused by a lack of memory safety in common implementations of languages such as C/C++, which are responsible for around 70% of security vulnerabilities in modern systems.

Introduction

Losses due to memory safety vulnerabilities are costly. For example losses due to the well-known OpenSSL heartbleed bug are estimated to exceed $500 million. CHERI is the deterministic solution to mitigating the vast majority of such vulnerabilities.

CHERI is the latest incarnation of capability machines which date back to the 1970s with the CAP computer, although the concepts date back further than that.

The CHERI TG was officially formed in October 2024, but the research leading to CHERI started way back in 2010 when DARPA launched the Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) programme, which tasked participants with redesigning computer systems to improve security. SRI International and the University of Cambridge team revisited capability architectures, seeking to address memory safety challenges inherent in conventional designs. [1]

CHERI development involves major industry players (Google – who chair the SIG and TG), Microsoft Research who were primarily responsible for CHERIoT which is an adapted version of CHERI-RISC-V for small embedded devices with novel features such as a hardware garbage collector. Smaller companies are also involved such as SCI and lowRISC who continue with CHERIoT development, and Codasip who develop cores such as the X730 meeting the base standard.

In 2025 and there are commercial CHERI-RISC-V FPGA based development boards such as the SONATA board developed by lowRISC, and also silicon planned for this year such as the ICENI family of devices based on the open-source CHERIoT platform.

The CHERI TG's agreed ratification plan is set to complete late summer 2025[2]. This comes late for existing silicon projects, risking a defacto standard forming, but is desperately required to allow the industry to converge on a single ratified specification for both hardware and software development.

This talk is about the status of the CHERI specification in the weeks leading up to the RISC-V summit and will discuss in detail the status of the TG, the specification and the ratification process.

This talk is suitable for members day or the main Conference programme, as the organizers see fit.

References

[1] Wikipedia, https://en.wikipedia.org/wiki/Capability_Hardware_Enhanced_RISC_Instructions

[2] CHERI-RISC-V ratification plan https://lf-riscv.atlassian.net/wiki/spaces/CTXX/pages/47022116/CHERI+Ratification+Plan