Project suggestion from Dr Matthew Naylor

Exploring software memory safety on a CHERI-enabled GPGPU

Supervisors: Dr Matthew Naylor, Dr Theo Marketos and Dr Paul Metzger

This project would explore memory safety for GPU kernels in programming environments such as CUDA and OpenCL, and investigate whether it is possible to build a more secure environment using CHERI capabilities.

Here in the department, we’re developing a new open-source RISC-V GPGPU (SIMTight) with support for CHERI security extensions. The SIMTight distribution ships with a basic CUDA-style library (called NoCL, 500 lines of C++) and a suite of benchmark kernels. This project would extend NoCL with additional functionality, such as the ability to run multiple kernels concurrently, and perform a security evaluation of the library, for example looking at kernel isolation properties (the ability to prevent data leakage/corruption between kernel instances).

First, a literature review would consider the memory safety properties afforded by existing GPU execution models such as CUDA or OpenCL. If experimentation is required, this may be done on commercial hardware such as an NVIDIA GPU. Subsequently, the NoCL library would be studied and any important missing functionality would be identified and implemented. Security and performance properties of the library would then be evaluated with and without CHERI enabled, and compared with commercial offerings.

As well as software improvements to NoCL, there is also scope for hardware improvements to SIMTight. For example, a fast tag-zeroing feature could be added to the hardware to improve the speed of capability revocation (particularly useful when the same stack memory regions are being reused by different kernels at different times).

A more constrained, engineering-focused version of this project is due to be performed by a Part II student this year. This Part III / MPhil project would differ by being an open-ended research project, focusing on the security evaluation, with the possibility to extend the hardware as well as the software, and would be carried out entirely independently of the Part II project.

Links:

SIMTight: https://github.com/CTSRD-CHERI/SIMTight/blob/master/README.md
NoCL: https://github.com/CTSRD-CHERI/SIMTight/blob/master/doc/NoCL.md