Mr. George V. Neville-Neil 演講：Capability Hardware Enhanced RISC Instructions (CHERI) 計劃經驗分享

文／林熙哲 資訊科學與工程研究所碩士生

George V. Neville-Neil 是一位作業系統與資訊安全的專家，他從 2011 年開始參與 FreeBSD 基金會的運作，也是〈The Design and Implementation of the FreeBSD Operating System〉的共同作者，除此之外，George 也是劍橋大學 Capability Hardware Enhanced RISC Instructions (CHERI) 計劃的主要技術成員之一，這次很高興能夠在他造訪陽明交通大學資訊學院之際聆聽他對於 CHERI 計劃的分享。

CHERI 是 SRI International 與劍橋大學合作，為了從硬體層面解決記憶體漏洞（如 Buffer Overflow）而產生的計劃，能夠提供高效能、基於硬體的細粒度記憶體權限管理，CHERI 包含了基於 RISC 指令集的擴充、硬體實作以及相關的作業系統、編譯器等系統程式移植，是一個相當成熟的計劃。

在過去，有許多資安漏洞肇因於軟體開發者對記憶體操作的疏忽，例如 2014 年知名的 OpenSSL Heartbleed 漏洞，就是因為開發者遺漏了對輸入資料的檢查導致 Buffer Overflow 的問題，導致攻擊者有機會竊取 SSL 的 Private Key 甚至破解 Https 的傳輸內容。 為了避免這樣的問題，許多現代程式語言例如 Rust 特別強調在記憶體安全方面的機制，但因為是在軟體層面做檢查，終究會對效能帶來一定程度的影響。

CHERI 想做的事情，是在硬體設計時就將這些記憶體權限管理的機制考量進去，由硬體提供記憶體權限管理機制的原生支援，並將這些記憶體權限管理的額外指令放入 RISC 指令集的擴充區域，讓其他支援 RISC 的程式也都能支援 CHERI。

CHERI 能夠將指定的記憶體區段分為 Read、Write、Execute 等權限，這些權限可以組合運用，而這些權限會儲存在 CHERI 硬體提供的 Capability Register 中，在 CHERI 硬體要處理相應的記憶體位置時，硬體也會自動檢查是否符合對應的 Capability，而 Capability 的管理本身則需要作業系統的配合。

CHERI 是一個生態系很成熟的計劃，除了指令集本身支援 Arm、RISC-V、MIPS 等等以外，也有對應的硬體、系統程式與軟體配套。硬體方面， Arm 公司有提供 Morello 開發板支援 CHERI 的機制，此外 Qemu 模擬器也有支援 64bit CHERI-MIPS 模擬；作業系統的部份，有從 FreeBSD 移植過來的 CheriBSD；系統程式方面，CHERI 團隊也有移植如 Clang/LLVM、Webkit、OpenSSH、PostgreSQL、Nginx 等軟體，是一個相當成熟的計劃。

對我個人來說，我覺得這是一個很難得的學習機會，我過去的經驗都是偏向系統管理與應用開發，對系統和硬體層比較陌生，剛好在修計算機組織課程後聽到這場關於 CHERI 的分享，許多演講中提到的知識都和課程相扣，為了撰寫這篇文章我也參考了 CHERI 的官網與相關論文，在閱讀這些文獻的過程中更發覺計算機組織課程的重要性，正所謂學以致用，很感謝這場分享讓我能夠將所學到的知識實際應用，也非常感謝 George 能來陽明交通大學資訊學院分享 Capability Hardware Enhanced RISC Instructions (CHERI) 這個題目。

Mr. George V. Neville–Neil's Speech: The Experience of the Capability Hardware Enhanced RISC Instructions (CHERI) Project

George V. Neville-Neil is an expert in operating systems and information security. He has been involved with the FreeBSD Foundation since 2011 and is a co-author of "The Design and Implementation of the FreeBSD Operating System." Additionally, George is one of the key technical members of the Capability Hardware Enhanced RISC Instructions (CHERI) project at the University of Cambridge. It is a pleasure to attend this talk to understand his insights on the CHERI project during his visit to the College of Computer Science at Yang Ming Chiao Tung University."

CHERI is a collaborative project between SRI International and the University of Cambridge. Its goal is to address memory vulnerabilities, such as Buffer Overflow, at the hardware level, offering efficient, hardware-based fine-grained memory permission management. CHERI is a well-developed project that encompasses extensions to the RISC instruction set, hardware implementations, and the porting of related system software.

In the past, security vulnerabilities could occur when software developers neglected memory operations. For instance, the well-known OpenSSL Heartbleed vulnerability in 2014 resulted from developers failing to properly validate input data, which subsequently led to a Buffer Overflow issue. This vulnerability allowed attackers to potentially steal SSL private keys and even decrypt the contents of HTTPS transmissions. To prevent such problems, many modern programming languages, like Rust, emphasize mechanisms for memory security. However, because these checks are performed at the software level, they inevitably impact performance to some extent. CHERI aims to integrate memory permission management mechanisms into hardware design. The hardware offers native support for memory permission management mechanisms, including additional instructions within the custom extensions of the RISC instruction set. This enables other RISC-supporting programs to also work with CHERI.

CHERI can segment the permissions of designated memory sections, such as Read, Write, and Execute. These permissions can be combined and stored in CHERI's hardware provided Capability Register. When CHERI hardware needs to deal with corresponding memory location, it automatically checks whether it complies with the corresponding Capability. This process requires cooperation from the operating system

CHERI is a well-developed project that supports Arm, RISC-V, MIPS, and various hardware, along with accompanying system software. In addition, it provides the Morello development board, which supports CHERI mechanisms. Furthermore, the QEMU emulator also supports 64-bit CHERI-MIPS simulation. In terms of operating systems, there is CheriBSD, a FreeBSD port. As for system software, the CHERI team has ported software such as Clang/LLVM, Webkit, OpenSSH, and PostgreSQL

This talk provided a great learning opportunity for me. I typically focus more on system management and application development rather than systems and hardware. Prior to attending this lecture, I had just completed the course, Computer Organization. Many of the topics discussed in the lecture were related to the material I had covered in that course. I also visited the CHERI official website and reviewed related papers as references for writing this reflection article. While reading those references and documents, I recognized the importance of computer organization, as I was able to apply the knowledge I gained from the course to Mr. George V. Neville-Neil's talk. Lastly, I would like to express my sincere gratitude to George for visiting our school and sharing insights on the topic of Capability Hardware Enhanced RISC Instructions (CHERI).