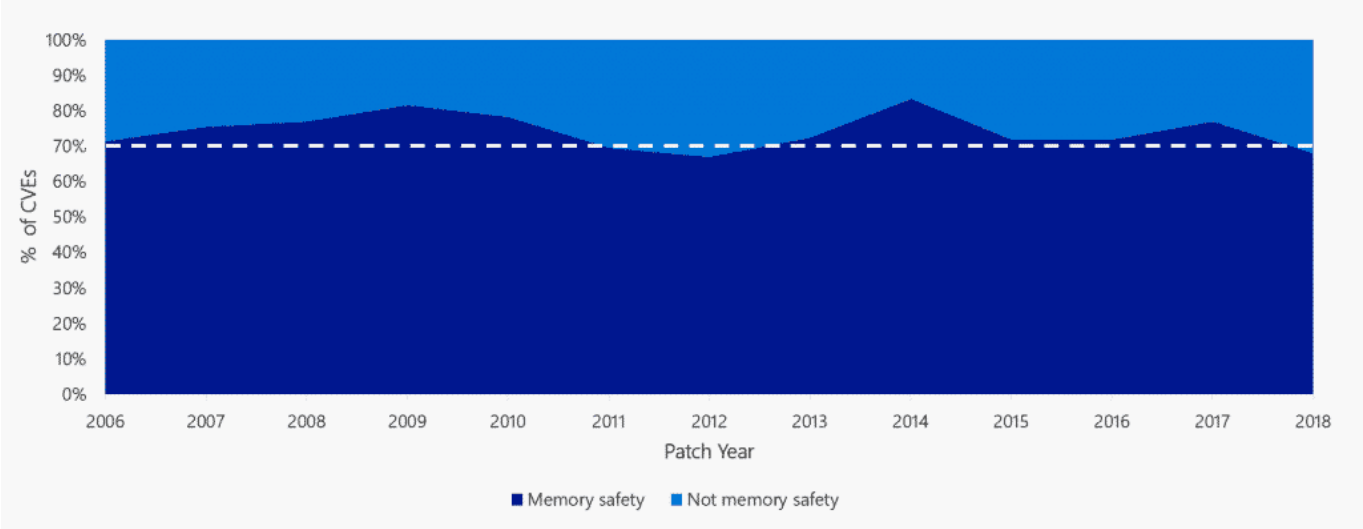
Sécurité : Microsoft expérimente CHERI pour résoudre ses problèmes de mémoire

La sûreté temporelle reste problématique, tout comme la mémoire non initialisée et la protection des adresses de retour. Ce sont là les principaux points d'amélioration que Microsoft fait ressortir après avoir mis CHERI à l'épreuve.

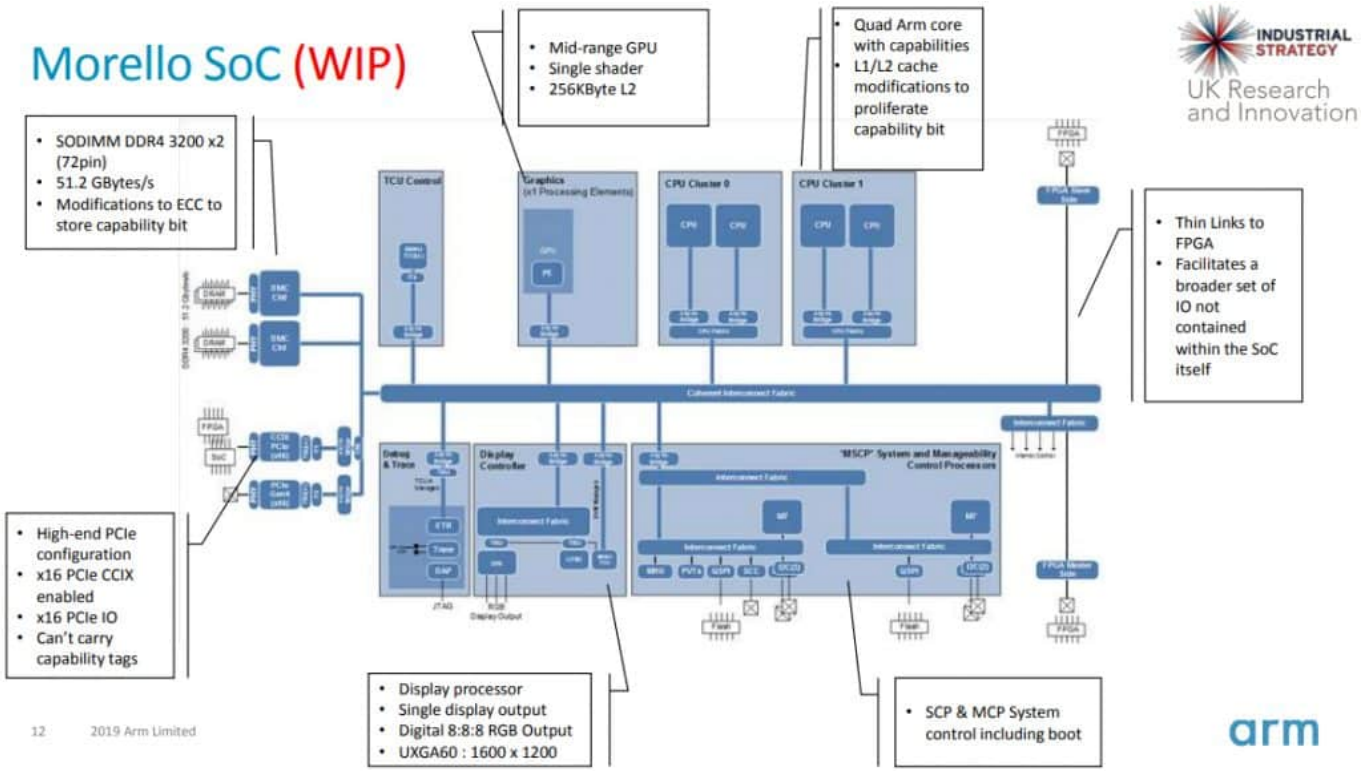
L'université de Cambridge pilote ce projet qui vise à lutter contre les failles de sécurité liées à la mémoire. Il intéresse d'autant plus Microsoft que la majorité des vulnérabilités que corrige l'éditeur entrent dans cette catégorie.



Face à ces failles, Microsoft s'est notamment appuyé sur Rust, le langage « origine Mozilla ». Il a expérimenté la réécriture de certains composants Windows. Ainsi que la création d'un langage dérivé, dans le cadre de l'initiative Project Verona menée avec l'Imperial College de Londres.

Avec CHERI, on touche au matériel. L'acronyme signifie en l'occurrence « Capability Hardware Enhanced RISC Instructions ». Le principe : développer un « modèle de protection » qui étende les architectures de jeux d'instructions.

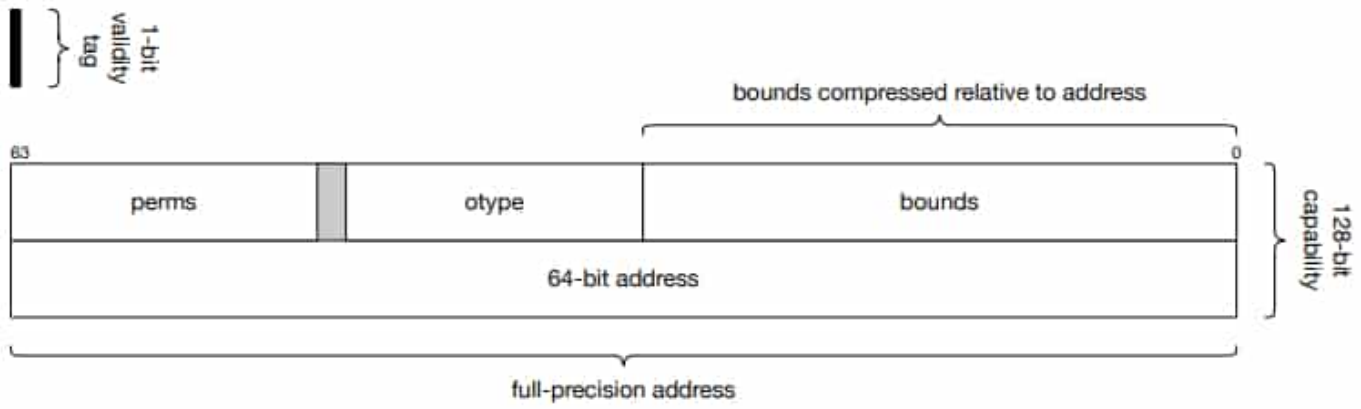
À leur démarrage en 2010, les travaux portaient sur MIPS64. Avec le support de la DARPA, ils se sont étendus depuis lors à RISC-V et à ARM64. Avec, pour ce dernier, un SoC expérimental annoncé pour fin 2021 sur base Neoverse N1. L'architecture x64 est arrivée plus récemment sur la feuille de route.



ISA	Status	Width(s)	Register file	On fail?	MMU	Cap mode
MIPS	Full	64-, 128-bit	Split	Exception	TLB	No
ARMv8-A	Experimental	128-bit	Merged	Clear tag	PTE	Yes
RISC-V	Draft	64-, 128-bit	Both	Exception	PTE	Yes
x86-64	Sketch	128-bit	Merged	TBD	PTE	Yes

Les capacités de CHERI

Au cœur de CHERI, il y a des « capacités ». Définies en langage Sail, elles constituent une extension des pointeurs, à travers l'ajout de métadonnées de protection.



Les « capacités » offrent aussi une alternative à l'isolation de processus basée sur la mémoire virtuelle. Plus légère en l'occurrence, car exploitable au sein des espaces d'adressage.

En première ligne du projet, les langages C et C++, particulièrement exposés aux failles « de mémoire ».
Au catalogue des prototypes logiciels, on trouve des extensions d'outils de développement (Clang/LLVM, GDB), de systèmes d'exploitation (FreeBSD, FreeRTOS) et d'applications (WebKit, OpenSSH, PostgreSQL).

Pour sa mise à l'épreuve, Microsoft a considéré les « failles de mémoire » que son Centre de réponse aux problèmes de sécurité a enregistrées en 2019. Sur les 456 qu'il a finalement retenues, CHERI en aurait bloqué 45 %. En y couplant l'initialisation de la pile et du tas, on dépasse les 50 %.

Illustration principale :« NEC VR5000 die » by Birdman– CC BY 2.0