Contribution ID: **124** Type: **not specified**

Guarded Control Stack on arm64: Challenges in Enabling Shadow Stack Support for CRIU

Friday 12 December 2025 11:00 (30 minutes)

Shadow stacks are a key security feature to guard against ROP attacks. Mike Rapoport has worked on enabling checkpoint/restore support for CET-based shadow stacks.

This talk extends that work in the realm of Arm64, specifically the GCS Guarded Control Stack (GCS) ARM extension. I'll present the process of adding GCS support to CRIU, including how process state is detected, dumped and restored, and what changes were required to happen in the parasite code.

I'll cover a key challenge which was meeting the kernel's sigframe expectations for GCS tokens, a critical part of getting reliable restore. I'll also discuss the debugging process that led to identifying and understanding gaps in the kernel's GCS support during dump and restore.

Primary author: SVILENKOV BOZIC, Igor (CRIU)

Co-authors: MIKHALITSYN, Aleksandr (Canonical); VAGIN, Andrei; RAPOPORT, Mike

Presenter: SVILENKOV BOZIC, Igor (CRIU)

Session Classification: Containers and checkpoint/restore MC

Track Classification: Containers and checkpoint/restore MC