Morello and the challenges of a capability-based ABI

Tuesday, 25 August 2020 09:00 (45 minutes)

The Morello project is an experimental branch of the Arm architecture for evaluating the deployment and impact of capability-based security. This experimental ISA extension builds on concepts from the CHERI project from Cambridge University.

As experimentations with Morello on Linux are underway, this talk will focus on the pure-capability execution environment, where all pointers are represented as 128-bit capabilities with tight bounds and limited permissions. After a brief introduction to the Morello architecture, we will outline the main challenges to overcome for the kernel to support a pure-capability userspace. Beyond the immediate issue of adding a syscall ABI where all pointers are 128 bits wide, the kernel is expected to honour the restrictions associated with user capability pointers when it dereferences them, in order to prevent the confused deputy problem.

These challenges can be approached in multiple ways, with different trade-offs between robustness, maintainability and invasiveness. We will attempt at covering a few of these approaches, in the hope of generating useful discussions with the community.

I agree to abide by the anti-harassment policy

I agree

Primary author: BRODSKY, Kevin (Arm)
Presenter: BRODSKY, Kevin (Arm)
Session Classification: LPC Refereed Track
Track Classification: LPC Refereed Track (Closed)