Contribution ID: **374** Type: **not specified**

ARM v8.5 Memory Tagging Extension

Tuesday, September 10, 2019 6:45 PM (15 minutes)

What is MTE and why we do need to add the support for the Linux Userspace? Memory Tagging is an ARMv8.5 extension and provides architectural support for run-time detection of various classes of memory errors. It can be used to aid with software debugging to eliminate vulnerabilities before they can be exploited (i.e. bounds violations, use-after-free,use-after-return, use-out-of-scope and use-before-initialisation).

What does MTE support for a Linux Userspace application mean? We can divide this topic in two main parts: userspace awareness (initialization, relaxation of the ABI, paging support for the tags, swapping) and userspace debugging (enable tagging in the userspace memory allocator).

The presentation will briefly introduce the MTE concepts trying to put them in the context of what is required for the Linux OS support. It will focus then on the enablement of the ARMv8.5 extension in the userspace trying to analyze the challenges that we faced during the endeavor: memory alignment, tags management, memory impact, etc.

Primary author: FRASCINO, Vincenzo (ARM)

Presenter: FRASCINO, Vincenzo (ARM)

Session Classification: Android MC