Contribution ID: **93** Type: **not specified**

Path Safety in the Trenches

Thursday 11 December 2025 15:45 (45 minutes)

Over the past decade (or three) of container runtimes on Linux, the attacks against container runtimes with the most bang-for-your-buck have generally been filesystem related —often in the form of a confused-deputy style attack. This is aided in part by the sheer number of juicy targets accessible through filesystem APIs such as /proc.

In particular, the past few years have seen quite a few security issues of this form in runc and other container runtimes —most recently in a set of CVEs published in November (CVE-2025-31133, CVE-2025-52565, and CVE-2025-52881). However, this is far from a container-specific issue. Many Unix programs have historically suffered from similar issues, and the various attempts at resolving it have not really measured up.

This talk will go through the myriad of issues necessary to protect user space programs against these kinds of attacks, completed and ongoing kernel work to try to make these problems easier to resolve, and our experience migrating a container runtime's codebase to a design which emphasises path-safety. In addition, this talk will also include an update on libpathrs (a library intended to make mitigating these attacks much easier for most Linux programs).

Primary author: SARAI, Aleksa (SUSE LLC)

Presenter: SARAI, Aleksa (SUSE LLC)

Session Classification: LPC Refereed Track

Track Classification: LPC Refereed Track