Contribution ID: **175** Type: **not specified**

The Challenge of Loading 4kB-Aligned ELFs on 16kB Systems

The transition to a 16kB base page size creates a significant compatibility issue for legacy ELFs built with 4kB segment alignment. This misalignment can place Read-Execute (RX) and Read-Write (RW) segments within a single page, which would require insecure RWX mappings. While recompiling is the ideal fix, it is often impossible for apps that depend on **unmaintained, closed-source third-party libraries**. Consequently, these applications fail to load, presenting an open ecosystem challenge that requires a robust compatibility solution.

This talk presents an in-depth analysis of this problem and explores the design space for potential solutions. It will discuss:

1. The ELF segment vs. page permission conflict.
2. The feasibility of a compatibility layer within the user-space dynamic loader.
3. Key hurdles: performance, security risks, and ELF layout stability.
4. Trade-offs of various dynamic remapping strategies.

Primary authors: YESCAS, Juan (Google); SINGH, Kalesh (Google)

Presenters: YESCAS, Juan (Google); SINGH, Kalesh (Google)

Session Classification: Android MC

Track Classification: Android MC