Linux Plumbers Conference 2025

Contribution ID: **288** Type: **not specified**

SDEI Applications in Trusted VM Fatal Handling: Secure Device Sanitization and Reset

Secure devices play a critical role in trusted virtual machines (VMs), serving as the foundation for protecting sensitive data and maintaining system integrity. When a trusted VM enters an abnormal or compromised state, it becomes essential to sanitize and reset secure devices properly to prevent the leakage of confidential information into untrusted environments. This presentation explores the application of the Secure Device Event Interface (SDEI) in virtualization. It demonstrates how SDEI can be leveraged to efficiently sanitize and reset secure devices within trusted VMs, thereby enhancing security isolation and improving the robustness of virtualization platforms.

Primary author: ZHANG, Cong

Presenter: ZHANG, Cong

Session Classification: Android MC

Track Classification: Android MC