Linux Plumbers Conference 2025

Saturday 13 December 2025

System Boot and Security MC - "Hall B2" (10:00 - 13:30)

-Conveners: Daniel Kiper; Piotr Król

time	[id] title	presenter
10:00	[423] Ultraviolet: A Code Integrity Model for Minimal Container Hosts	MORRIS, James
10:25	[448] The Future of Platform Security Measurement in Linux	PIJANOWSKI, Maciej
10:50	[401] Reconcilable Differences: Booting Linux on IBM PowerVM LPARs	WILSON, George
11:10	[485] ReLaunch Revisited: A Refresher on TrenchBoot Late Launch	KIPER, Daniel SMITH, Daniel
11:30	Break	
11:45	[417] Design Space and Challenges in Design of Attested TLS Protocols	SARDAR, Muhammad Usama
12:05	[334] Oak stage0: a minimal firmware for (confidential) virtual machines	Mr SAAR, Andri HUI, Kevin
12:30	[58] Who Authenticates Linux? Rethinking PAM & NSS in the Age of Cloud Identity	Mr MULDER, David
13:00	[150] Android Boot, DRTM, UKIs	MERKUREV, Dmitrii LINDHOLM, Leif MUTHIAH, Ram