Linux Plumbers Conference 2022

Monday, 12 September 2022

System Boot and Security MC - "Ulster & Munster" (10:00 - 13:35)

time	[id] title	presenter
10:00	[325] Welcome to System Boot and Security MC	KIPER, Daniel ŻYGOWSKI, Michał
10:05	[77] Secure bootloader for Confidential Computing	LU, Ken YAO, Jiewen
10:40	[57] Secure Boot auto enrollment	DAGONNEAU, vincent
11:15	[258] Kernel TEE subsystem evolution	GARG, Sumit
11:50	Break	
12:20	[104] Remote Attestation of IoT devices using a discrete TPM 2.0	Mr TOMOV, Dimitar Mr KALCHEV, Svetlozar
12:55	[230] TrenchBoot Update	SMITH, Daniel