Linux Plumbers Conference 2020

Thursday 27 August 2020

System Boot and Security MC - Microconference2/Virtual-Room (07:00 - 11:05)

time	[id] title	presenter
07:00	[263] Introduction	
07:10	[129] Secure boot without UEFI: booting VMs on Power(PC)	AXTENS, Daniel
07:35	[62] System Firmware and Device Firmware Updates using Unified Extensible Firmware Interface (UEFI) Capsules	HSIUNG, Harry
07:55	Break	
08:10	[84] ASI: Efficiently Mitigating Speculative Execution Attacks with Address Space Isolation	Dr WEISSE, Ofir
08:35	[125] LinuxBoot Ready is not ready: making linuxboot systems work	MINNICH, ronald
09:00	[128] Native Booting using NVMe over Ethernet Fabrics	FARLEY, Doug SZUBOWICZ, Lenny
09:20	Break	
09:35	[143] A Ridiculously Short Intro into Device Attestation	Mr TOMOV, Dimitar Mr OLIVER, Ian
10:00	[130] Advanced Applications of DRTM with TrenchBoot SecureLaunch for Linux	SMITH, Daniel
10:25	[124] Passing and retrieving information from bootloader and firmware	Mr KIPER, Daniel Mr ŻYGOWSKI, Michał