Linux Plumbers Conference 2024

Friday 20 September 2024

Confidential Computing MC - "Room 1.15 - 1.16" (10:00 - 13:30)

time	[id] title	presenter
10:00	[386] SVSM vTPM: From Boot Attestation to Persistent Storage and Beyond	CARVALHO, Claudio GARZARELLA, Stefano FANELLI, Tyler
10:20	[387] Intel TD Partitioning and vTPM on COCONUT-SVSM	DONG, Chuanxiao CHEN, Jason Mr YAO, Jiewen FANG, Peter DHANRAJ, Vijay
10:40	[207] Arm CCA Planes and Interplane Communication Interface Proposal	MILLER, Derek
11:00	[333] OpenHCL: A Linux based paravisor for Confidential VMs	OO, Chris
11:15	[335] Attested TLS and Formalization	SARDAR, Muhammad Usama
11:30	Break	
12:00	[94] Beneath the Surface: Analyzing Nested CVM Performance on KVM/QEMU and Linux Root Partition for Microsoft Hyper-V/Cloud-Hypervisor	JAIN, Jinank Mr ISLAM, Muminul
12:20	[410] Trusted I/O: Architectures and Implementations for Confidential Computing	KARDASHEVSKIY, Alexey WILLIAMS, Dan Mr YAO, Jiewen ORTIZ, Samuel KURUPPASSERY POULOSE, Suzuki
12:50	[293] SoC peripheral TDISP	HARTLEY, David
13:00	[318] Updates on RISC-V Confidential VM Extension (CoVE) and CoVE-IO	SAHITA, RAVI
13:10	[388] Going Beyond Confidential Attestation with Trustee	PORTER, Chris CARVALHO, Claudio BUONO, Daniele DUBEY, Niteesh FELDMAN-FITZTHUM, Tobin