Linux Plumbers Conference 2023

Tuesday, 14 November 2023

Confidential Computing MC - "Potomac G" (14:30 - 18:00)

time	[id] title	presenter
14:30	[321] Confidential Computing Microconference Introduction	GIANI, Dhaval ROEDEL, Joerg
14:35	[316] COCONUT Secure VM Service Module Discussion	ROEDEL, Joerg
14:45	[213] Remote Attestation in AMD SEV-SNP Confidential VMs	CARVALHO, Claudio
15:00	[191] Shrinking The Elephant - A Confidential Computing Attestation Sequel	ORTIZ, Samuel
15:20	[258] How to Build a Confidential Attestation Client	FELDMAN-FITZTHUM, Tobin
15:40	[276] Supporting Live Migration of Confidential VMs in KVM	GUPTA, Pankaj LENDACKY, Thomas
16:00	Break	
16:30	[317] Secure I/O	WILLIAMS, Dan POWELL, Jeremy ORTIZ, Samuel EIDEN, Steffen LENDACKY, Thomas
17:00	[117] Taming the Incoherent Cache Issue in Confidential VMs	ZHANG, Mingwei LI, Jacky CHRISTOPHERSON, Sean
17:15	[319] Towards unified confidential computing ABIs	WILLIAMS, Dan
17:30	[75] Update on RISC-V Confidential VM Extension (CoVE)	PATRA, ATISH SAHITA, RAVI
17:40	[246] Secure TSC for AMD SEV-SNP guests	DADHANIA, Nikunj
17:50	[201] Secure AVIC: Securing Interrupt Injection from a 'malicious' Hypervisor	I, Kishon Vijay Abraham SUTHIKULPANIT, Suravee