Linux Plumbers Conference 2022

Tuesday, September 13, 2022

Confidential Computing MC - "Herbert" (10:00 AM - 1:30 PM)

time	[id] title	presenter
10:00 AM	[98] Upstream & Guest Distro support for Confidential Compute	GAO, Jianxiong
10:20 AM	[142] Unmapped Private Memory for Confidential Guests	ROTH, Michael
10:40 AM	[117] Securely booting confidential VMs with encrypting disk	MURIK, Dov FELDMAN-FITZTHUM, Tobin
11:00 AM	[137] Using DICE Attestation for SEV and SNP Hardware Rooted Attestation	GONDA, Peter
11:20 AM	[228] Hardening Linux guest kernel for CC	RESHETOVA, Elena
11:40 AM	Break	
12:10 PM	[252] The elephants in the confidential room: Attestation and verification	Mr ORTIZ, Samuel
12:30 PM	[235] Identifying and Eliminating Contention from Booting Concurrent SNP VMs	LI, Jacky ORR, Marc
12:50 PM	[113] Testing Intel TDX functionality with new set of self tests	SHAHAR, Sagi
1:10 PM	[158] Interrupt Security for AMD SEV-SNP	KALRA, Ashish