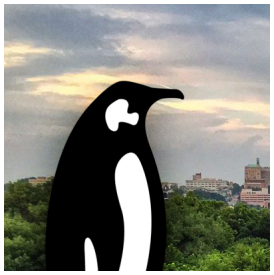

Contribution ID: **246** Type: **not specified**

Secure TSC for AMD SEV-SNP guests

Tuesday, 14 November 2023 17:40 (10 minutes)

TSC value calculations for guests are controlled by the hypervisor. A malicious hypervisor can prevent guests from moving forward. The Secure TSC feature for SEV-SNP allows guests to securely use RDTSC and RDTSCP instructions. This ensures the guest gets a consistent view of time and can prevent a malicious hypervisor from making it appear that time rolls backwards, increments at a ridiculously fast rate, or similar tricks. In this talk we will discuss the Secure TSC changes needed to support hypervisor/guest and current upstreaming status.

Primary author: DADHANIA, Nikunj

Presenter: DADHANIA, Nikunj

Session Classification: Confidential Computing MC

Track Classification: LPC Microconference: Confidential Computing MC