Contribution ID: **53** Type: **not specified**

TDX Linux guest

Tuesday, 21 September 2021 08:00 (25 minutes)

Intel TDX is an upcoming confidential computing platform for running encrypted guests on untrusted hosts on Intel servers. It requires para virtualization to do any required emulation inside the guest. There are some unique challenges, in particular in hardening the Linux guest code against untrusted host input through MMIO, port and other IO, which is a new security challenge for Linux. The guest has to "accept" all memory and to get acceptable boot performance this acceptance has to be done lazily. We'll give an overview of the current TDX status, talk about the challenges and hope for a good discussion.

I agree to abide by the anti-harassment policy

I agree

Primary authors: KLEEN, Andi; KUPPUSWAMY, Sathyanarayanan; RESHETOVA, Elena

Presenters: KLEEN, Andi; KUPPUSWAMY, Sathyanarayanan; RESHETOVA, Elena

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC