Contribution ID: **297** Type: **not specified**

TPM2 Security in the face of bus interposers

Wednesday, 11 September 2019 17:00 (20 minutes)

TPM2 introduced a plain text authorization scheme with the idea that the system using the TPM should now whether the transport was secure. The presence of interposers on the bus, either as physical devices

https://www.nccgroup.trust/us/our-research/tpm-genie/

Or as compromised pre-boot firmware make this threat a reality. A NULL seed based scheme has been proposed for Linux

https://lore.kernel.org/linux-integrity/1540193596.3202.7.camel@HansenPartnership.com/

we should discuss if this is the best we can do and if it is how should we extend it to the layers below that use the TPM (like UEFI and grub).

I agree to abide by the anti-harassment policy

Yes

Primary author: BOTTOMLEY, James (IBM)

Presenter: BOTTOMLEY, James (IBM)

Session Classification: System Boot and Security MC