Hello everybody!

First a big shout-out on the impressive work you guys have done regarding SGX integration.

I have a general question on the state of SGX's remote attestation (RT), as I'm quite confused by the information I can find publicly.

Foreshadow (L1TF) allowed adversaries to extract the long-term private key of the enclave used for RT. This basically brakes the entire RT concept, as it's possible to forge fake enclaves.

Also, the early mitigations by Intel don't help here (micro-code updates and OS fixes) as we can't trust the OS.

However, now first CPUs (e.g. CFU) ship with hardware fixes for L1TF:

a) Is there any public information about how L1TF is now fixed on the hardware level? - do they simply flush the cache when entering the enclave? - how about the hyper-threading attack vector (using a shadow thread)

b) Is the application vendor able to verify that a CPU with hardware fixes is being used in that particular attestation? - Specifically, are some CPU details (like model, stepping,…) populated in the Remote Attestation protocol?

Thanks a lot!