

Re: TXT and VT both required for...

[TxT-VT-d_Noob](#) 5 posts since

Jun 9, 2009

Below is a thread I posted to the VPro forum and have reposted it here, along with Javed's response. My next question is posted below his response.

Thanks,

Noob

>>My Initial Post

Hi Folks,

Excuse my ignorance, but as my username says, I am a somewhat a "noob" to the whole TxT/VT world. Anyway, what I am trying to figure out is, if you just want to have measured launch of a PC do you have to have both TxT and VT-d (Yes, assume the TPM is there)? Or is the VT only needed if you're doing virtualization? Of course, having VT-d makes sense if you're doing Virtualization, but I guess my real question is whether or not TxT requires the VT technology no matter your scenario. Say, for instance, an organization only wants to perform remote attestation (using SRTM/DRTM) of a host and doesn't use virtualization at all. I hope that all makes sense. Also, what other chip makers out there are currently supporting Measured Launch? I think AMD's version of VT-d is called IOMMU. Just trying to see who else does this and if there is a standard as well.

Thanks!

Noob :-0

>>Response from Javed:

Re: TXT and VT both required for...

Hi!

We all were once a noob but then one learns with time :-)

Anyway, coming to your query, first let me brief you a bit on VT-d.

VT-d:

While you are doing Virtualization, the guest OS uses the hardware resources of the server/desktop to run through virtualization. An input/output memory management unit (IOMMU) enables guest [virtual machines](#) to directly use [peripheral](#) devices, such as ethernet and accelerated graphics cards, through [DMA](#) and [interrupt](#) remapping. Both AMD and Intel have released specifications. The AMD specification labels this technology "IOMMU" (an acronym for the common name of this form of virtualization) while Intel has called their implementation "Intel's Virtualization Technology for Directed I/O" (VT-d).

Now as for VT-d and TXT relationship:

The TXT is commercially distributed with another technology VT-d. The VT-d provides hardware remote security, protecting hardware, storage and communications, adding another security level against software attacks.

VT-d is an environment model that shares hardware resources using I/O virtualization. This can then allow control over each process's access to resources without using reprobativ exclusive access methods.

Then for that matter, is TXT required for Virtualization too?

NO! If TXT is being used with VT-d, it does not mean that TXT is necessarily required for Virtualization cause basically TXT (Trusted Execution Technology) is commonly advertised by Intel as a security technology. TXT is intended to provide users and organizations with a higher level of trust while accessing, modifying or creating sensitive data and code and of course, TPM is required for that matter. This technology could be coupled with VT-d (Intel Virtualization Technology for Directed I/O) designed to backup the TXT outside of the chip, and even outside the Computer itself.

Re: TXT and VT both required for...

So what do we conclude?

So from the look of it and what I have worked on so far, I surmise that for a measured launch, you would need to enable them both as VT-d works in conjunction with TXT because VT-d would provide hardware remote security adding another level of security against the software attacks unless you opt out otherwise.

Any reference for that matter?

However if you experience something new, please update us on that as well. I would also encourage you to brush through the PDF document at the URL below and for further details, do look into the references provided at the end of that document:

<http://www.docstoc.com/docs/2382371/Analysis-of-a-Measured-Launch>

I have a few documents on this that can actually give you further information on this however respecting the confidentiality of those documents, can not share them but always help you in this regard to resolve any problem or answer any query that you may have

Get back to us if need be

Hope this helps however if you further questions especially regarding this, be sure to post it in our server room section and we'd be glad to help.

Thank you, have a great day!

--

Warm Regards,

Javed Lodhi

Intel Go Green, Save The Environment!

Thanks Javed!

Re: TXT and VT both required for...

Ok, so what you're saying is that VT-d does more than just provide protected support for virtualization, and that it provides more security when paired with TxT, correct? In other words, if I am not using virtualization software at all, VT-d is still useful with TxT for a measured launch? Last one: If that is correct, then is that to say that you Can't have a measured launch if you only use TxT?

I also actually have that document you referenced, but did not see the answer I was looking for specifically, which is why I decided to post here. I'll give it another look though.

Thanks again,

N

Tags: vt-d, tpm, tcg, virtualization, txt, measured_launch, iommu

[Javed Lodhi](#) 370 posts since

Jul 4, 2008 1. **Re: TXT and VT both required for Measured Launch?** Jun 11, 2009 11:36 AM

Thank you for posting it here, indeed we can help you on Server Room since vPro Expert Center is fashioned for vPro technology and related matters.

Resuming from where we left off, since you could not find what you were looking for from the document I referred you to, I will be doing a bit more inside on this and let me get you the right answer on this meanwhile our server gurus would also be pitching in and giving their insight on this. Let's get you to resolution

--

Warm Regards,

Javed Lodhi

[Intel Go Green, Save The Environment!](#)

[TxT-VT-d_Noob](#) 5 posts since

Jun 9, 2009 2. **Re: TXT and VT both required for Measured Launch?** Jun 30, 2009 6:24 PM

Hey There,

Re: TXT and VT both required for...

It's been a couple of weeks and I noticed no one else has commented on my thread I inserted. Probably because it looks like Javed answered my question. However, I'm still trying to understand what TxT and VT-d give me if I am not using Virtualization at all. If I am using a TPM, can't I have a measured launch of a regular system that's not using any virtual OSes? I've been told that VT-d gives you nothing extra if you're not using virtualization. Does the same apply for TxT? Is TxT required for a Measured Launch?

Thanks again!

Noob