- **Jason Sebranek** • 15 days ago
  Hello everyone, and welcome
  - •
  - Reply
  - •
  - Share ›

- 
  Regan Robertson Mod • 14 days ago
  Good Afternoon,
  The video will start on this page at 13:30pm, and you may have to hit play or unmute. As a reminder this site works best in a Chrome Browser. You can write in comments through this feature to continue the conversation or ask questions. Please login or sign up for a Disqus account to participate in the discussion boards.
  - •
  - Reply
  - •
  - Share ›

- 
  Gernot • 14 days ago
  Hi Yanyan, nice to see one of our alumni!
  - •
  - Reply
  - •
  - Share ›

Yanyan Shen Gernot • 14 days ago

Hi Gernot, nice to see you!

- Reply
- Share ›

Carl Nerup • 14 days ago

Good Luck - you two are the best.

- Reply
- Share ›

Nathaniel Husted • 14 days ago

I think as long as you stay away from "Hack-Proof" you're fine. *grin*

- Reply
- Share ›

Carl Nerup Nathaniel Husted • 14 days ago

LOL- Hello Katim(?)

- Reply
- Share ›

Ihor Kuz Nathaniel Husted • 14 days ago

so "un-hackable" is OK? :-)

- 1
- Reply
- Share ›

June Andronick Nathaniel Husted • 14 days ago

Sometimes staying away from saying it doesn't prevent press articles using it in titles about your work ;)

- 2
- Reply
- Share ›

Jason H Li June Andronick • 14 days ago

LOL that was some DARPA PM told me -- I never said that!

3

Reply

Share ›

Jason H Li • 14 days ago

You mentioned Samsun Knox. How do you compare with that product? Or it is an alternative competition?

Reply

Share ›

Jason Sebranek Jason H Li • 14 days ago

Knox is only a competitor in the sense that it's primarily what Gov is using now for classified phones. There is NO virtualization going on in Knox, so fundamentally the architecture is different.

Reply

Share ›

Jason H Li Jason Sebranek • 14 days ago

Right it is ARM TZ based.

Nick @ ARM talked about seL4 and TZ yesterday. Have you / will you put some thoughts along those lines?

1

Reply

Share ›

Jason Sebranek Jason H Li • 14 days ago

For sure. That was a really interesting talk and we're going to look into how/when we could incorporate that capability.

Reply

Share ›

Jason H Li Jason Sebranek • 14 days ago

I found his architecting thoughts legit. But for a product, you have to make it work and work well. Good luck!

- Reply
- Share ›

Jason Sebranek Jason H Li • 14 days ago

Thanks. I think realistically, it will be most appealing once we can find a commercial device with EL2 support in Secure World. Not common at all today.

- Reply
- Share ›

Jason H Li Jason Sebranek • 14 days ago

It wasn't common, but if it works, users don't care anyways. I'd like to see more of EL2 support of Secure World in some secure and efficient way. Messed with TZ years ago, great but not so great. I think you know the headaches too.

- Reply
- Share ›

Carl Nerup Jason H Li • 14 days ago

Knox at its heart, is a Container Solution. No driver isolation. No Nested VPN. No Double Encryption. It is better than nothing.

Reply

Share ›

Gernot • 14 days ago

What evaluation level are you aiming for?

Reply

Share ›

Jason Sebranek Gernot • 14 days ago

We're not aiming at the old deprecated EAL standard. We're strictly aiming for US Gov-SECRET under the CSfC guidelines. That amounts to evaluation against NIAP protection profiles for MDF (mobile device fundamentals), VPN, and FDE.

Reply

Share ›

Carl Nerup • 14 days ago

Imagine the 'ultimate' prove it use case. That is what this solution will be - you can just take it to a customer and show seL4 doing its magic. It will be a bit boring - but that is the point. The product just works.

Reply

Share ›

Renato Levy • 14 days ago

I agree multicore is really path critical!

1

Reply

Share ›

Jason H Li Renato Levy • 14 days ago

Totally agreed. But multi-core is really hard, especially for mission critical systems. A wise mentor once advised - single-core equivalence for multi-core is great but we need some time to apply for mission critical systems.

Reply

Share ›

Jason H Li • 14 days ago

The cons are right on. I am also academic more or less, but would love to see CoE to help some of the community issues for adoption.

1

Reply

Share ›

Gernot • 14 days ago

there'll be a talk by Ihor on the seL4 device driver framework at the very end of the Summit

Reply

Share ›

Jason Sebranek Gernot • 14 days ago

yeah, I saw that on the agenda. Looking forward to it!

- Reply
- Share ›

Aleksey Nogin • 14 days ago

Is there a specific reason why DIT and DAR are VMs, rather than "native" seL4 components?

- 1
- Reply
- Share ›

Gernot Aleksey Nogin • 14 days ago

I had the same question ;-)

- 2
- Reply
- Share ›

Jason Sebranek Gernot • 14 days ago

No specific burning reason, other than it was an easier path for us in terms of reusability from existing capability. I'd like to look at using native in future. Thanks for the question.

- Reply
- Share ›

Yanyan Shen Aleksey Nogin • 14 days ago

One reason is software reuse. For instance, building a native seL4 VPN component might take years.

- Reply
- Share ›

Regan Robertson Mod • 14 days ago

Please join us for the next session that starts now. You can either go back to agenda to get to the next session or at the bottom of the page there is a next session button.

- Reply
- Share ›

Bo Gan • 14 days ago

Can the presentation be made available offline?