Security Tech Talk Chat Transcript
May 3, 2022

00:14:22 Archna Haylock: please mute yourself if you are not speaking. You are welcome to post questions in this chat and we will get to them as soon as we can. Thanks!

00:15:02 Kali Burdette: And thank you so much to our sponsor GOOGLE for making this Tech Talk happen!

00:27:41 Mary A: Thanks for the presentation

00:34:48 Bill-OCP: What is the MCTP bus?

00:35:11 Eric Mann (Intel): Its a typo :)

00:36:51 Jeff Hilland (HPE): https://en.wikipedia.org/wiki/Management_Component_Transport_Protocol

00:36:55 Nilesh Narayan: is MCTP over I3C needed for PFR?

00:39:35 Eric Mann (Intel): (is audio down?)

00:39:44 Eric Eilertson: I think so.

00:40:28 jrquaran: Can you clarify the interaction between Caliptra and TPM

00:40:30 Bill-OCP: Thanks Jeff.

00:53:50 Silviu Vlasceanu (Huawei): is the SRAM buffer for SoC FMC inside the Caliptra boundary?

00:54:13 Bharat Pillilli: It is inside Caliptra boundary

00:54:31 Silviu Vlasceanu (Huawei): thanks

00:55:04 Tsippy Mendelson: How is the rest of the code beyond FMC measured?

00:56:00 Lohith Rangappa: Will Caliptra services for attestation based on SPDM or a new standard ? also what is the communication medium (SMBus, I2C ?)

00:57:59 Huijun Xie: After dual signing, can the manufacturer only signed firmware still run?

00:58:16 Eric Mann (Intel): is there an upper bound defined on the authentication process - as add-in devices such as nics must typically meet PCI initialization requirements of 100msec after PERST# deassertion ,Ä¶where is the fuse controller to pull keys? who controls updates to revoke and update auth keys? does the design comprehend fuse-based anti-rollback controls? does the design comprehend international security standards such as FIPS and SMx - complete with CAVPs & CMVPs - or is this a vendor issue to resolve?

01:00:16 Bharat Pillilli: "Will Caliptra services for attestation based on SPDM or a new standard ? also what is the communication medium (SMBus, I2C ?)" -> SPDM. The MCTP stack and thereby physical layer stops in an appropriate SOC management engine

01:00:47 Bharat Pillilli: "After dual signing, can the manufacturer only signed firmware still run?" -> Yes, as long as the dual signing/cosigning passes

01:03:22 Bharat Pillilli: "is there an upper bound defined on the authentication process - as add-in devices such as nics must typically meet PCI initialization requirements of 100msec after PERST# deassertion ,Ä¶" -> in general yes, but the issue is device key generation, but that 100ms is rarely a real requirement in DCs. Infact the requirement truly is PCIe link being ready for the config write than PERST# itself because many devices start on PERST# or after 3.3V is applied (unlike NICs/aux devices)

01:04:08 Bharat Pillilli: "where is the fuse controller to pull keys? who controls updates to revoke and update auth keys? does the design comprehend fuse-based anti-rollback controls?" -> Fuse registers are exposed with properties for SOC to populate at boot time because each SOC/company have different fuse controller IP/logic on how they do

01:04:40 Varun Sampath (NVIDIA): what about boot media controller? Must be Caliptra SPI?

01:04:59 Eric Mann (Intel): Typically the PCIe EP ROM must be patch from authenticated NVM to be able to start link training ,Ä¶ so it still applies ,Ä¶ there is CRS# which can delay theoretically config cycles by 1sec ,Ä¶ however it sounds like OCP doesn't consider PCI-SIG compliance required ,Ä¶.?

01:05:22 Tsippy Mendelson:Could other HW be used that conforms to Caliptra - or it is expected that this open sourced block be used?

01:05:32 Silviu Vlasceanu (Huawei): will Caliptra be CC and FIPS 140-3 friendly?

01:05:34 Bharat Pillilli: "what about boot media controller? Must be Caliptra SPI?" -> No, full spec will provide better information but we will allow the SOC level block to read and issue data into SRAM

01:05:59 Eric Mann (Intel): presuming PQC requirements on authentication flows would be a vendor issue? or in-scope for this?

01:06:18 Bharat Pillilli: so the media can be different - this is primarily because in multi-socket systems the flash may be located in various places and behind different sources

01:07:40 Bharat Pillilli: "does the design comprehend international security standards such as FIPS and SMx - complete with CAVPs & CMVPs - or is this a vendor issue to resolve?" -> Good question, goal is to be CAVP (and potentially FIPS) compliant open HW but I will let Andres/Bryan/Prabhu answer

01:09:00 Silviu Vlasceanu (Huawei): do you expect any sort of TPM-like PCRs or will all measurements bind in DICE fashion? How would the measurement principle extrapolate to the boot process after FMC (BL, kernel etc.)? DICE all the way up or leveraging TPM for host side?

01:09:06 Bharat Pillilli: "presuming PQC requirements on authentication flows would be a vendor issue? or in-scope for this?" -> Since there is no final NIST compliant PQC yet, its not a goal for first revision but we would love to have folks contribute for potential algorithms

01:09:40 Bing Zhu: Caliptra IP only allows RISC-V? how about other architectures?

01:10:17 Bharat Pillilli: Since Andres is taking questions, will stop answering :-)

01:10:30 Elaine Palmer (IBM Research): Will OCP's royalty-free licensing terms be applied to Caliptra,Äôs RTL contribution?

01:10:44 Matt King (Nvidia): Can you expand on how transparency/openness will be used? Unlike software, silicon artifacts are inherently non-inspectable.

01:12:57 Ismael Rangel (OCI): if vendor X was to implement this, what changes in the main SoC HW, boot ROM and Runtime FW are needed to interact with / be 'Caliptra aware'?

01:13:12 Elaine Palmer (IBM Research): Are you anticipating reproducible builds across all devices using Caliptra?

01:13:48 Bharat Pillilli: "Typically the PCIe EP ROM must be patch from authenticated NVM to be able to start link training ,Ä¶ so it still applies ,Ä¶ there is CRS# which can delay theoretically config cycles by 1sec ,Ä¶ however it sounds like OCP doesn't consider PCI-SIG compliance required ,Ä¶.?" -> I would be incorrect to say PCIe SIG compliance is accounted for but nothing in the definition is disallowing the compliance since it depends on the speeds of FW fetch & authentication

01:15:11 Bill-OCP: Can a device w/ Caliptra still work in a system that has not implemented RoT.

01:15:47 Eric Mann (Intel): XMSS is still a PQC compliant algo ...

01:16:48 Bill-OCP: It is safe to assume that the goal is to have Caliptra embedded in all mutable devices within a system? If so, is there a timeframe or goal to achieve this?

01:17:47 Silviu Vlasceanu (Huawei): does OCP intend to run a Caliptra compliance or logo program?

01:20:17 Christine Severns-Williams: Open source HW is not a common way to build chips. Can you comment on your vision for WHAT this really means? What is really open source from this? Or is it really a spec that must be build to?

01:20:29 Lohith Rangappa: Will Cliptra be confined to RTM ? Or it will grow to be source for RTU (Root of Trust for Update) and RTRec (Root of Trust for Recovery)

01:22:10 Silviu Vlasceanu (Huawei): Is Google moving away from OpenTitan to Caliptra?

01:23:41 Simon Ramage: recalling Bryan's comment about avoiding (or being cautious of?) coupling Manageability concepts into Caliptra, and seeing the included peripherals into Caliptra, would these be primarily for internal communications/debug within the SoC, or for direct SPDM communications into Caliptra, or otherwise? curious to hear more of your thoughts on the tradeoffs at play here, including the potential for security exposures with the peripherals being there.

01:24:15 Matt King (Nvidia): RE: DICE - will Caliptra act as a DICE protection module?

01:27:05 Ismael Rangel (OCI): I'm thinking about those control signals

01:27:41 Silviu Vlasceanu (Huawei): In the first slides there was a mention of RTM doing measure, verify and attest. Will calyptra do verifications (i.e. Secure Boot for FMC of SoC)?

01:29:41 alberto: What is the (or is there a) relationship between Caliptra and TCG DPE?

01:29:50 Eric Mann (Intel): Does Caliptra continue to run as an ongoing service or does it terminate after performing the SoC runtime fw measurement collection (?)

01:30:48 James Zhang (NVDA): Do you guys expect to have different measurement for different Caliptra implementation or do you still all vendor to actually have the same Caliptra TCB measurements without modification of the OS FW at all?

01:31:32 Eric Mann (Intel): .. or ,Ä¶ does Caliptra expect to exclusively own the manageability interfaces in which to exchange the SPDM measurement messages?

01:33:03 alberto: How do you prevent manufacturers from "adding value" to the Caliptra open source version in their own releases?

01:33:52 Christian Maldonado (WDC): Will the threat model that this is built based on be open source as well?

01:36:18 Huijun Xie: Does OCP enforce I3C as physical layer for SPDM binding?

01:37:08 Silviu Vlasceanu (Huawei): regarding international crypto - perhaps crypto agility in all caliptra data structures should be considered early on

01:37:47 Jeff Andersen: "RE: DICE - will Caliptra act as a DICE protection module?,Äù

01:38:05 Jeff Andersen: ,ÄúWhat is the (or is there a) relationship between Caliptra and TCG DPE?,Äù

01:39:02 Jeff Andersen: DPE being an in-progress TCG spec we probably can,Äôt discuss much by way of specifics, but we do want to have Caliptra offer DICE-as-a-Service via a well-defined standard.

01:42:10 Silviu Vlasceanu (Huawei): thank you, amazing talk

01:42:40 Andres LC : thank you all!

01:44:06 Lee: Hello all, I missed the earlier portion of the call. Is there a recording I can access later on?

01:45:01 Bryan Kelly: yes, calls are being reccorded

01:45:09 Bryan Kelly: link will be sent later

01:45:28 Lee: Hi Bryan, thanks. where can I go access later on?

01:46:02 Archna Haylock: this call is being recorded, the slides and video will be available by end of week on the OCP Past Events Page here: https://www.opencompute.org/events/past-events

01:47:18 Lee: thank you all

01:53:32 Eric Mann (Intel): Re: Circular economy - it is very common for multiple "OEMs" (aka ODM1->ODM2->ODM3...) to be involved in the manufacturing process - the point of which "end of manufacturing lockdown" is a bit vague and often fraught with errors ...

01:59:51 Lohith Rangappa: Do we need both Owner key and Vendor key to be immutable ? e.g. eFUSE mapped

02:00:43 Eric Mann (Intel): This seems generally at odds to zeroization requirements (in particular fuse-based ones)

02:02:42 Eric Mann (Intel): Just industry feedback - we (Intel) have had several CSPs ask to sign the bootstage firmware, not Intel (vendor), which presumes owner-provisioned keys ,Ä¶

02:03:58 Varun Sampath (NVIDIA): I'd challenge the assertion that devices with only vendor-managed configuration don't need ownership transfer. Ownership transfer authorizes that configuration without necessarily authoring it. An owner may want that authority to restrict the set of configurations beyond what the vendor does. Attestation is an alternative but doesn't cover all cases due to time-of-check-time-of-use

02:05:18 Eric Mann (Intel): And I promise my last question -- is reselling really a thing in the industry? I recall several counter-examples of purchases from large, online resale sites which were used as a vector to supply counterfeit material ,Ä¶ hence discouraged ,Ä¶ if a customer cares about security, will they want to start with a 70% lifetime product from an intermediary clearinghouse (?)

02:07:41 Eric Mann (Intel): *or* is this just a refactoring of vendors supplying on-prem equipment to hybrid cloud rollouts?

02:10:05 Ned Smith: RFC8995 defines some of the ownership transfer flow. Does OCP notion of OT align with RFC8995?

02:20:18 Varun Sampath (NVIDIA): Does this imply that the Caliptra BootROM will sit in a spinloop waiting for a key to be loaded?

02:20:19 Bryan Kelly: different to RFC8995, as it is not requiring manufacturer to be in the middle

02:21:36 Bryan Kelly: no spinloop for key, it's blended into identity

02:22:05 Silviu Vlasceanu (Huawei): slightly off-topic: will Caliptra do all asymmetric DICE operations at every boot or do you plan some optimizations?

02:24:47 Silviu Vlasceanu (Huawei): bumping this up from the Caliptra talk as related to ownership verifications:In the first Caliptra slides there was a mention of RTM doing measure, *verify* and attest. Will Caliptra do such ownership verifications (i.e. Secure Boot) for the SoC FMC or will it stick to measure only?

02:26:26 Bryan Kelly: on caliptra, ownership authentication is included in the RTM capabilites

02:27:12 Silviu Vlasceanu (Huawei): so also for the SoC FMC, not only for Caliptra FMC, is this correct?

02:27:46 Bryan Kelly: correct, ownership transfer applies to all SOC firmware.

02:28:02 Silviu Vlasceanu (Huawei): got it

02:28:40 Bryan Kelly: manufacturer signs soc firmware and makes it authentic, owner signs the same manufacturer signed authentic firmware and makes it authorized on their device.

02:31:25 Daniil Egranov: As I understand, the history of ownership is not preserved. Will it be important to have device verifiable chain of ownership for a device security?

02:32:54 Silviu Vlasceanu (Huawei): perhaps this could be tracked external to the device, if necessary :)

02:38:29 Ned Smith: It,Äôs important to think about ownership transfer as being fine-grained / multi-grained as each DICE layer can have a different loadable ownership key. The idea that a top-level owner coexists with finer gained owners isn,Äôt a contradiction, but can be complex to model in a circular economy context.

02:46:23 Thomas Bowen (Intel): Has Common Criteria security evaluations been considered for security audits? are there deficiencies to Common Criteria security evaluations that necessitate CSPs doing their own audit?

02:52:57 Bryan Kelly: CSPs do their own audits today, but those shouldn't be exclusive to the few large CSPs. CSPs audit to approximately the same criteria, why not just standardize it and do it once for everyone to benefit, including the author/manufacturer of that firmware.

02:54:15 Bryan Kelly: instead of it being a CSP audit, it can be a 3P security auditing company that meets requirements for auditor.

02:56:11 Eric Hibbard (Samsung): Does OCP envision developing cPPs?

02:56:43 Thomas Bowen (Intel): Common Criteria already defines evaluation assurance levels could those be leveraged?

02:57:45 Eric Hibbard (Samsung): Note the ISO/IEC is on the cusp of releasing the new 5-part ISO/IEC 15408 standard

03:09:49 Thomas J. Blau: Thank you.

03:10:04 Elaine Palmer (IBM Research): Thank you, Google!