Security HC

12/07/2023

Agenda

- Disclosures, opens, and updates
- Meeting time updates
- TG and SIG updates
- New/emerging use cases and architectural gaps – discussion

- Meeting Notes in RED

Meeting time updates

BOD requested streamlining of TG/SIG meeting times

- Avoid overlapping meetings to facilitate better attendance
- Carry out most work offline - emails and Github
- Use meeting time for matters that need active discussion for resolution

Initial proposed calendar for **Security HC meetings** - starting in 2024

- All times in Pacific TZ; additional PM slots available if needed
- SIGs should plan and announce ahead on how to use their slots and avoid overlaps

	Tuesday							
	7:00 - 7:30	7:30 - 8:00	8:00 - 8:30	8:30 - 9:00	9:00 - 9:30	9:30 - 10:00	10:00 - 10:30	10:30 - 11:00
Odd week					Crypto*	Crypto*	CHERI TG/SIG	RI SIG+
Even week	TC SIG**	Sec. Model	Crypto*	Crypto*				
Odd week					Crypto*	Crypto*	CHERI TG/SIG	TC SIG**
Even week	RI SIG+	HC	Crypto*	Crypto*				

**CoVE, CoVE-IO, Smmtt TGs

+sPMP, IOPMP, LIso, Memsafety, Compart

*CETG+FstTrk HACTG, PQCTG
Asking to switch to ISA unpriv slots

Alternative

	Tuesday							
	7:00 - 7:30	7:30 - 8:00	8:00 - 8:30	8:30 - 9:00	9:00 - 9:30	9:30 - 10:00	10:00 - 10:30	10:30 - 11:00
Odd week					Crypto* ?	CHERI TG/SIG	RI SIG+	
Even week	Sec Model	Crypto*?	TC SIG**					
Odd week					Crypto* ?	CHERI TG/SIG	TC SIG**	
Even week	RI SIG+	Crypto* ?	HC	HC				

**CoVE, CoVE-IO, Smmtt TGs

+sPMP, IOPMP, LIso, Memsafety, Compart

*CETG+FstTrk HACTG, PQCTG
Asking to switch to ISA unpriv slots

CONFIRMED Crypto are asking to move to ISA unpriv so we have more slots

Noted that this is a 4 week cycle where we likely need 2.

Any and Ravi to collect requests and constraints and send new proposal

Updates

- **Security Model TG (assignee HC)**
  - Plan revised September 2023
  - Spec → LINK v0.1
  - Next steps → release spec v0.2 by EOY'23 with usage models documented; v0.3 in Jan with crypto recommendations.
- **CoVE TG (assignee TC SIG)**
  - Ratification plan (revised) approved February 2023
  - Spec → ABI v1.0 documented at LINK
    - Updates to sync with supervisor domains terminology is in progress -> freeze review
  - Next Steps → Freeze criteria deliverables
    - [RFC 00/48] RISC-V CoVE support
    - [RFC kvmtool 00/10] RISC-V CoVE support
    - TSM code that implements the ABI has been released at https://github.com/rivosinc/salus
    - Wiki for running tests on POC using QEMU: https://github.com/rivosinc/cove/wiki/CoVE-KVM-RISCV64-on-QEMU

Updates

- **Cove-IO TG (assignee TC SIG)**
  - Ratification plan approved on October 2023
  - Spec → LINK
  - PoC - vfio-user based TEE-IO device on top of a QEMU emulated CoVE platform
  - Next Steps → Spec and POC Development
- **Smmtt TG (assignee TC SIG)**
  - Ratification plan approved September 2023
  - Spec→ LINK
  - Next step → address open issues to complete spec. Development in Q1'24
- **SSLP TG (assignee CFI SIG)**
  - Ratification plan approved Aug 2022
  - Spec → LINK: Completing Architectural Committee review
  - Next Steps
    - psABI definition making progress in the TG github; several issues resolved
    - Acceptance criteria deliverables being worked upon

Updates

- **sPMP TG (assignee RI SIG)**
  - Ratification plan approved on Aug 2022
  - Spec → LINK in AR review
  - PoC status - ?
  - Next Steps → complete ARC ARs, resource sharing
- **IOPMP TG (assignee RI SIG)**
  - Ratification plan approved on July 2022
  - Spec → LINK
  - PoC status - ?
  - Next Steps → resolve direction vis-a-vis WG non-ISA
- **Lightweight Isolation TG (assignee RI SIG)**
  - Charter revision ? Charter revision planned this year
  - Need to answer the WG question ASAP – this has likely taken too long so fast track request will be made to the IC
- **CHERI TG (assignee CHERI SIG)**
  - Charter proposed – set up request will be made to priv IC, security HC happy to manage if priv ic wants to delegate but this may be run by priv IC
  - Ratification plan WIP

Updates

- **Memory Safety and Compartmentalization (assignee RI SIG)**
  - In strategy and gaps discussion phase in the SIG
- **Secure Debug (dotted line)**
  - Charter in progress **-** smmtt are looking at debug. Any requested folks think about their debug scenarios and comment, particularly around multple trust chains