RISC-V®

RISC-V External Debug Security TG

Meeting notes – 12/11/2023

Disclaimer

- https://docs.google.com/presentation/d/1LNhpuNwU54TgwGfcl-Fgf4HUFxCxh0AztPaeqMuRQRw/edit#slide=id.p1

Agenda

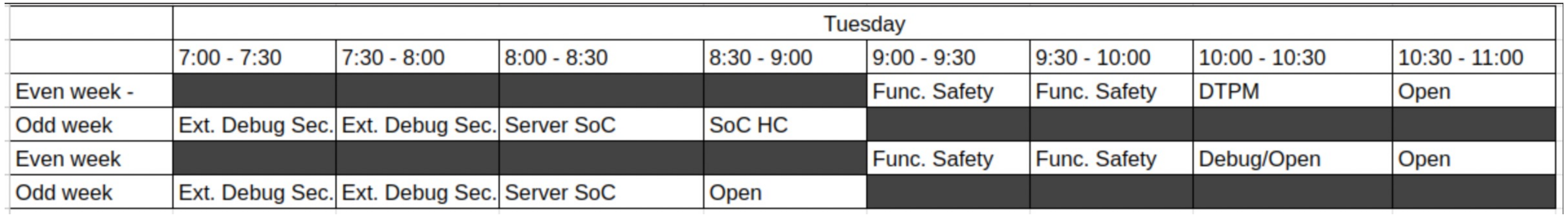
- TG update
  - Meeting time
  - Charter update
- Discuss arch opens
  - https://github.com/riscv/riscv-smmtt/issues/11

Introduction

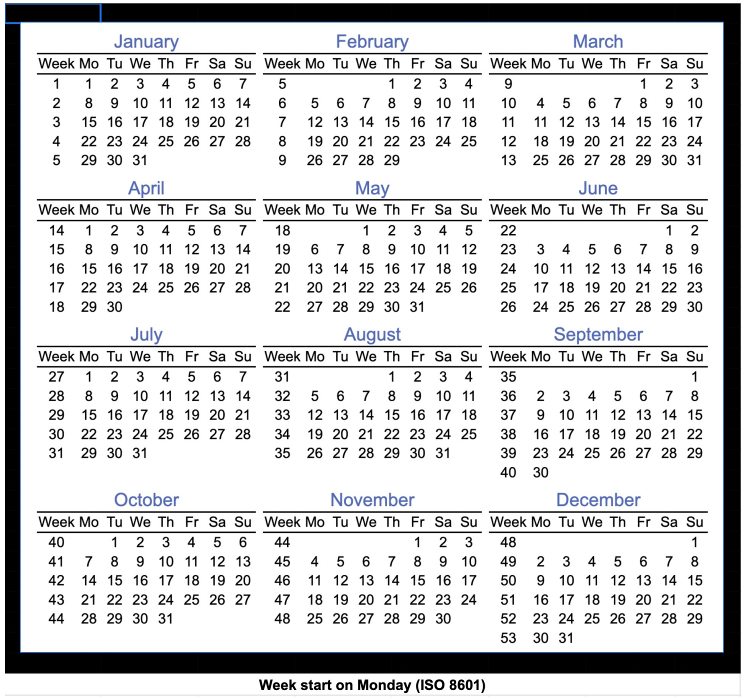
- Welcome to TG meeting
- Feel free to raise your hand and introduce yourself

New meeting time

- Foundation shuffle all TG meetings to avoid conflict
- Ext. Debug sec. TG meeting time assigned to new time, see below
- Next TG meeting likely 1/15/2024



	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
Even week -	■	■	■	■	Func. Safety	Func. Safety	DTPM	Open
Odd week	Ext. Debug Sec.	Ext. Debug Sec.	Server SoC	SoC HC	■	■	■	■
Even week	■	■	■	■	Func. Safety	Func. Safety	Debug/Open	Open
Odd week	Ext. Debug Sec.	Ext. Debug Sec.	Server SoC	Open	■	■	■	■



January

Week	Mo	Tu	We	Th	Fr	Sa	Su
1	1	2	3	4	5	6	7
2	8	9	10	11	12	13	14
3	15	16	17	18	19	20	21
4	22	23	24	25	26	27	28
5	29	30	31				

February

Week	Mo	Tu	We	Th	Fr	Sa	Su
5				1	2	3	4
6	5	6	7	8	9	10	11
7	12	13	14	15	16	17	18
8	19	20	21	22	23	24	25
9	26	27	28	29			

March

Week	Mo	Tu	We	Th	Fr	Sa	Su
9					1	2	3
10	4	5	6	7	8	9	10
11	11	12	13	14	15	16	17
12	18	19	20	21	22	23	24
13	25	26	27	28	29	30	31

April

Week	Mo	Tu	We	Th	Fr	Sa	Su
14	1	2	3	4	5	6	7
15	8	9	10	11	12	13	14
16	15	16	17	18	19	20	21
17	22	23	24	25	26	27	28
18	29	30					

May

Week	Mo	Tu	We	Th	Fr	Sa	Su
18			1	2	3	4	5
19	6	7	8	9	10	11	12
20	13	14	15	16	17	18	19
21	20	21	22	23	24	25	26
22	27	28	29	30	31		

June

Week	Mo	Tu	We	Th	Fr	Sa	Su
22						1	2
23	3	4	5	6	7	8	9
24	10	11	12	13	14	15	16
25	17	18	19	20	21	22	23
26	24	25	26	27	28	29	30

July

Week	Mo	Tu	We	Th	Fr	Sa	Su
27	1	2	3	4	5	6	7
28	8	9	10	11	12	13	14
29	15	16	17	18	19	20	21
30	22	23	24	25	26	27	28
31	29	30	31				

August

Week	Mo	Tu	We	Th	Fr	Sa	Su
31				1	2	3	4
32	5	6	7	8	9	10	11
33	12	13	14	15	16	17	18
34	19	20	21	22	23	24	25
35	26	27	28	29	30	31	

September

Week	Mo	Tu	We	Th	Fr	Sa	Su
35							1
36	2	3	4	5	6	7	8
37	9	10	11	12	13	14	15
38	16	17	18	19	20	21	22
39	23	24	25	26	27	28	29
40	30						

October

Week	Mo	Tu	We	Th	Fr	Sa	Su
40		1	2	3	4	5	6
41	7	8	9	10	11	12	13
42	14	15	16	17	18	19	20
43	21	22	23	24	25	26	27
44	28	29	30	31			

November

Week	Mo	Tu	We	Th	Fr	Sa	Su
44					1	2	3
45	4	5	6	7	8	9	10
46	11	12	13	14	15	16	17
47	18	19	20	21	22	23	24
48	25	26	27	28	29	30	

December

Week	Mo	Tu	We	Th	Fr	Sa	Su
48							1
49	2	3	4	5	6	7	8
50	9	10	11	12	13	14	15
51	16	17	18	19	20	21	22
52	23	24	25	26	27	28	29
53	30	31					

Week start on Monday (ISO 8601)

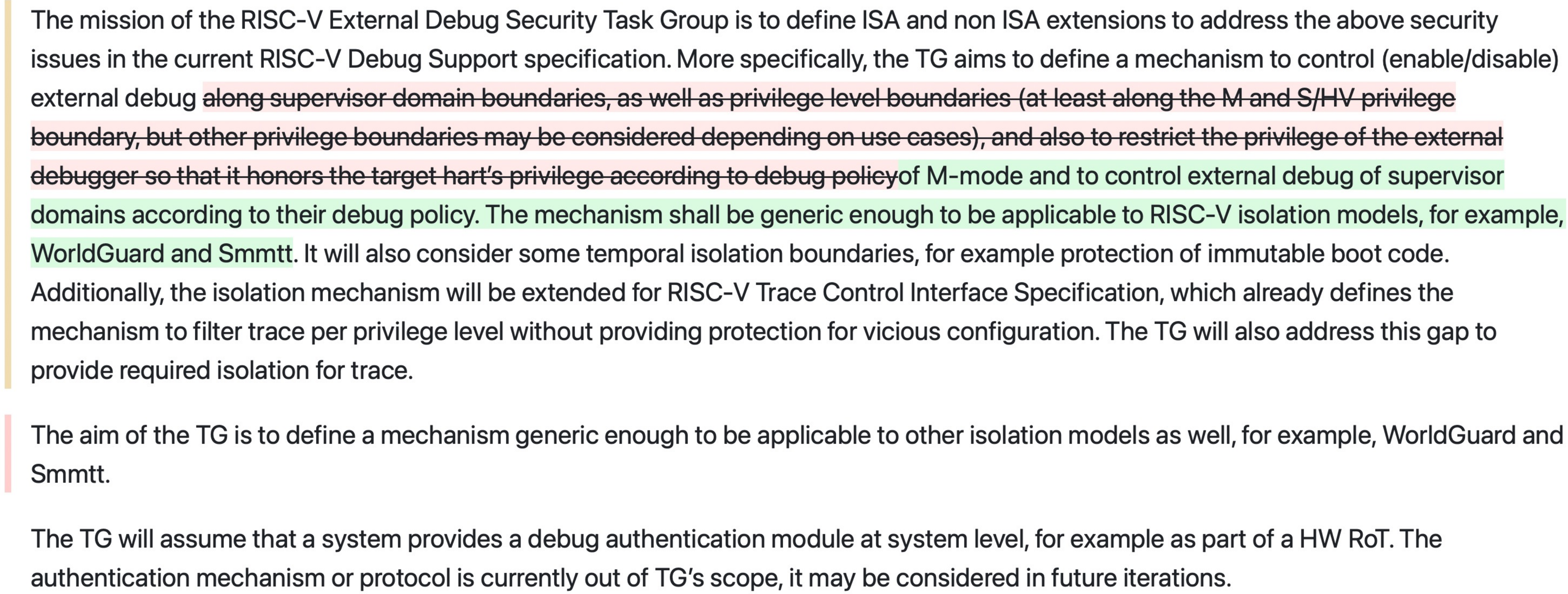
TG Progress (Updates in blue)

- Charter
  - Made minor change accroding to new feedback

- Chair & Vice chair election (Updates in blue)
  - Create ”call for candidate” ticket in github - Done (Ticket)
  - Governing and Dotted-line Chairs to review the required qualification
    - Blessed by Security HC chair (Andy), waiting for SOC HC chair (Ved)
  - Governing HC/IC chair send call-for-candidate email – Need to update charter according to new feedbacks
  - Collect candidate list, interview – Pending
  - Nominee & approve – Pending

Charter update

- https://github.com/riscv-admin/external-debug-security/pull/5



The mission of the RISC-V External Debug Security Task Group is to define ISA and non ISA extensions to address the above security issues in the current RISC-V Debug Support specification. More specifically, the TG aims to define a mechanism to control (enable/disable) external debug ~~along supervisor domain boundaries, as well as privilege level boundaries (at least along the M and S/HV privilege boundary, but other privilege boundaries may be considered depending on use cases), and also to restrict the privilege of the external debugger so that it honors the target hart's privilege according to debug policy~~of M-mode and to control external debug of supervisor domains according to their debug policy. The mechanism shall be generic enough to be applicable to RISC-V isolation models, for example, WorldGuard and Smmtt. It will also consider some temporal isolation boundaries, for example protection of immutable boot code. Additionally, the isolation mechanism will be extended for RISC-V Trace Control Interface Specification, which already defines the mechanism to filter trace per privilege level without providing protection for vicious configuration. The TG will also address this gap to provide required isolation for trace.

The aim of the TG is to define a mechanism generic enough to be applicable to other isolation models as well, for example, WorldGuard and Smmtt.

The TG will assume that a system provides a debug authentication module at system level, for example as part of a HW RoT. The authentication mechanism or protocol is currently out of TG's scope, it may be considered in future iterations.

Meeting notes

- Charter

- https://github.com/riscv/riscv-smmtt/issues/11
  - Agreed to remove M mode control from proposal
    - Allow M mode to enable debug for itself is a security concern
    - Hierachical security control - RoT enables debug for non-RoT hart, RoT BR enables debug for its M mode via hardware (e.g. life cycle FSM) out of hart
  - Agreed to simplify the proposal to remove per priv level control
  - Agreed to split debug control to separate extension, TBD on which CSR to use

Call for candidate – Chair/Vice Chair

- Required Technical Qualifications
  - Knowledgeable in RISC-V debug architecture, RISC-V external debug spec and trace spec
  - Knowledgeable in RISC-V security architecture, isolation model and related specs
  - Experience with threat modeling and security architecture analysis
  - Experience in platform/SOC/CPU security architecture and aspects related to debug security

- Community Charter
  - https://github.com/riscv-admin/external-debug-security/blob/main/CHARTER.md

Information & Logistic

- TG Charter
  - https://github.com/riscv-admin/external-debug-security/blob/main/CHARTER.md

- TG Meeting notes
  - https://github.com/riscv-admin/external-debug-security/tree/main/meetings

- Draft
  - https://github.com/joxie/riscv-debug-security/blob/main/spec/Secure%20Debug%20Proposal.md (Stable version)
  - https://github.com/joxie/riscv-debug-security/blob/dev/spec/Secure%20Debug%20Proposal.md (Dev branch)
  - https://github.com/joxie/riscv-debug-security/issues (Open issues)

Backup Slides