RISC-V External Debug Security TG

Meeting notes – 11/15/2023

Disclaimer

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

Agenda

- Introduction
- Review TG charter
- Goal for Nov
- Discuss arch opens

Introduction

- Acting chair – Joe Xie @nVidia
- Acting vice-chair – Gokhan Kaplayan @Imgtec
- Contributor - Aote Jin @nVidia
- Enrico @Intel
- Beeman @Rivos
- Robert @Individual
- Paul @Ventana
- Erick @NXP
- Yann @SiFive
- Vicky @IMG

TG Charter Review (No Change)

- TG Charter Draft

- Status
  - Had two rounds of reviews with related SiG/HC (RTI, DTPM, SOC, Security)

- Last changes
  - Include trace spec to the scope for TG
  - Make authentication mechanism future considerations (originally out-of-scope)

Goal for Nov

- TG
  - Get TSC to review and approve TG charter
  - TG chair and vice-chair ellection

- Spec (https://github.com/joxie/riscv-debug-security/blob/main/spec/Secure%20Debug%20Proposal.md)
  - Create ratification plan and status checklist
  - Create spec github repo, and move proposal draft to offical spec github repo

Dev Spec Status (Aote)

- Keepalive should be either ignored for all debug privilege levels or at least for sub-machine mode privilege levels.
- Relaxedpriv must be hardwired to 0x0
- The fields in dcsr require sufficient privilege level to access, otherwise the fields will be masked by 0x0 (mutiplexed to read-only zero if privilege not suffice and switched back to be configurable fields if granted sufficient privilege).
- Debug PC (dpc) and Debug Scratch Register (dscratch0, dscratch1)The CSR dpc, dscratch0 and dscratch1 is accessible when the hart enter a debuggable privilege level.
- Triggers with action = 1 (enter debug mode) will only match/fire if debug is enabled for the privilege level where the hart hits the trigger.
- In debug mode:
  - - triggers (action = 0/1) cannot be enabled for privilege levels higher than the one specified in mdbgsec.dbgprv/mdbgsec.dbgv.
  - - triggers (action = 2/3/4) cannot be enabled for privilege levels higher than the one specified in mdbgsec.trcprv/mdbgsec.trcv.
  - - triggers (action = 8/9) cannot be enabled if mdbgsec.extrigdis is zero.

Arch Opens & Issues

- https://github.com/joxie/riscv-debug-security/blob/main/spec/Secure%20Debug%20Proposal.md
- External Trigger of Core Trigger Module

Meeting notes and Actions

- Charter discussion
  - Joe / Gokhan to start offical approval process right now, don’t have to wait

- Spec (https://github.com/joxie/riscv-debug-security/blob/main/spec/Secure%20Debug%20Proposal.md)
  - Async triggers can be weaponized by low priv mode to attack high priv mode
    - AI – Aote to open a new issue – Aote
  - How to handle trigger match when debug is disabled
    - https://github.com/riscv-admin/external-debug-security/issues/2
  - Clarify the relationship between debug enable and authentication bits
    - AI – Aote to open an issue
  - Clarify system protections (WG / IOPMP or similar checker mechanism)
    - Open a new issue
    - https://compass.sustech.edu.cn/nailgun/ (ARM nailgun attack, we should provide some guidance to help implementation to avoid such kind of attack in RISC-V world)
  - How does debug security spec interact with m-mode isolation extension?
    - AI – Aote to check M mode isolation spec

Backup Slides