Security HC Meeting

Feb 2nd, 2023

Agenda

- Security Roadmap update. Yesterday we presented the security roadmap to the Chairs, we will represent here for the wider group. – Presented roadmap. James (qualcomm) suggested TMP table based PMP, Ravi noted this was already considered in the AP-TEE ISA TG, to be discussed in the Confidential Compute TG. James also suggested there may be a need for a security domains TG (similar to world guard). As this is yet to be published, discussion deferred until the details are clearer.
- Paper from Mark **- A cross-process Spectre attack via cache on RISC-V processor with trusted execution environment** https://www.sciencedirect.com/science/article/pii/S0045790622007613

Agenda

- Next steps on confidential compute/TEE/ lightweight TEE use case, assumptions and requirements. (process discussion rather than technical discussion)

Agreed on a call with smaller sub group of interested parties on Monday 6th at 15:00 UST, using the security HC zoom link.

Security Roadmap

- https://docs.google.com/presentation/d/1D57J1vEvliUNJHB-wjUFuo2SXLAdfyEyMDBc0esTC7w/edit#slide=id.p2