Security HC Meeting

August 17, 2023

Agenda

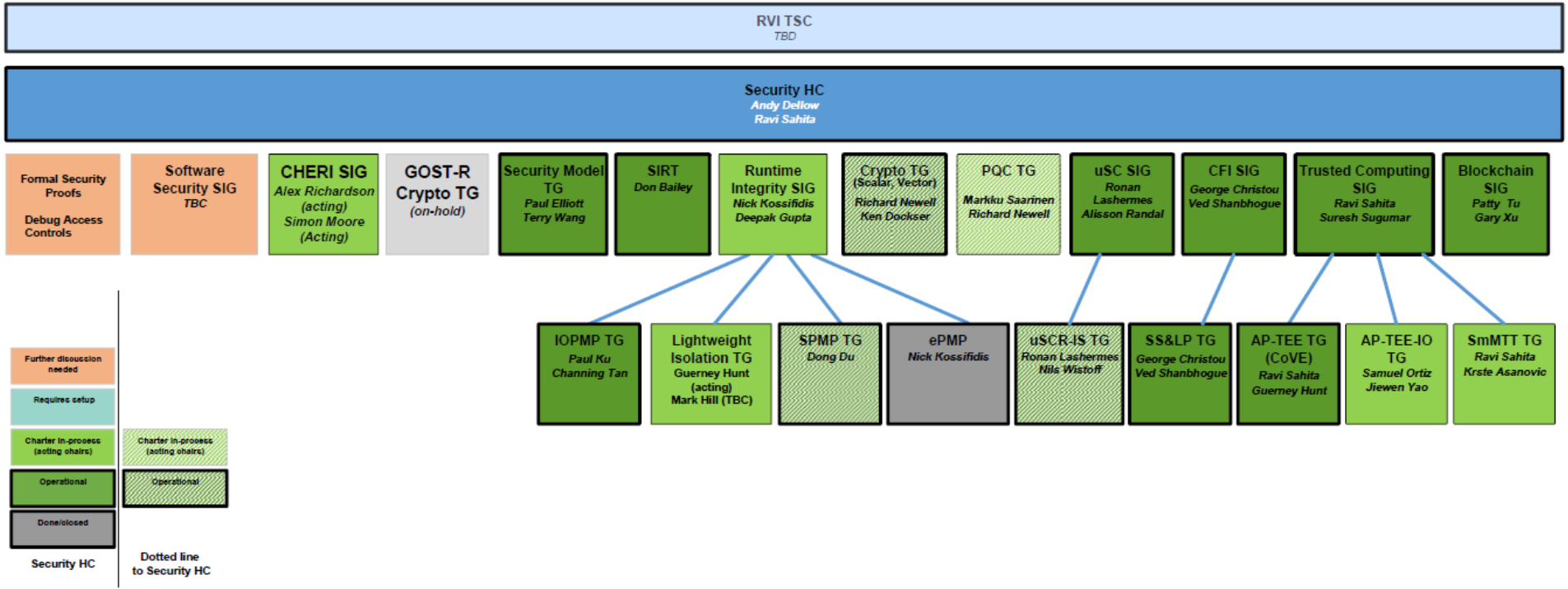
- PQC TG status –
  - Markku to fwd the autogenerated email. Andy to send the call
- Svadu extension fast track ratification.
  - Hardware updating of PTE A/D bits

  Ravi has reviewed, Guerney will also review and comment.
- Work Group Status
  - A few corrections - Smmtt is dotted line
  - App tee IO and IOPMP to present their plans at next chairs meeting
  - Lightweight iso TG – guerney and mark to meet to discuss next steps end of august
  - Crypto – Vector TG will remain active to push last two instructions as fast track
  - High Assurance Crypto TG - Richard will define candidate quals ready for call for candidates
  - Security Model – slow progress due to holidays since restructuring of the doc.

- Discussion topics Status
  - Andy to ask nick to start a gap analysis and strategy doc, linking back to SIG charter goals.
  - Idea is to agree on gaps and optimal solutions, to avoid multiple solutions diluting effort
    - Alisson, Ravi, Gurney, Andy all agreed to assist

  - Debug – low security attendance to the DTPM meeting, but agreement that dtpm should own the solution. Security team tol define the security issues gap and requirements to the debug. Nvidia already has most of that in their slides.
  - Andy to align with the DTPM chair.

Working groups Status



Discussion Status

- RTI SIG
  - HFI
  - Pallete Memory
  - Memory Tagging, Pointer Masking
  - Interactions with lightweight Isolation TG

- Debug
  - Proposals being discussed, but we need gap analysis, Charter 1st