RISC-V®

Security HC meeting

November 11, 2022

Agenda

- Vice Chair – progress update
- Open signoffs –
  - Ratification-Ready Milestone for RV32E-64E package
  - Ratification-Ready Milestone for Ztso package

- Security Model – Call for Chair
- CHERI SIG – status
- Runtime Integrity SIG – Nick - status update
- Lightweight TEE – Nick ?
- AP-TEE – Ravi - progress update, next steps

- Any other Updates from TGs + SIG

Security HC Vice Chair

A few candidates

Some new to the group so interviews ongoing

Hope to propose to the TSC this week

Open signoffs

- Any comments on
  - Ratification-Ready Milestone for RV32E-64E package
  - Ratification-Ready Milestone for Ztso package

- *Agreed to set up subcommittee to better manage future review requests*
- *Nick, Guerney, others agreed to look at Ztso (ch.25 total store ordering), and the rv32e-64e and comment by Monday*

Security Model

- Really Critical TG
- Call for Chair

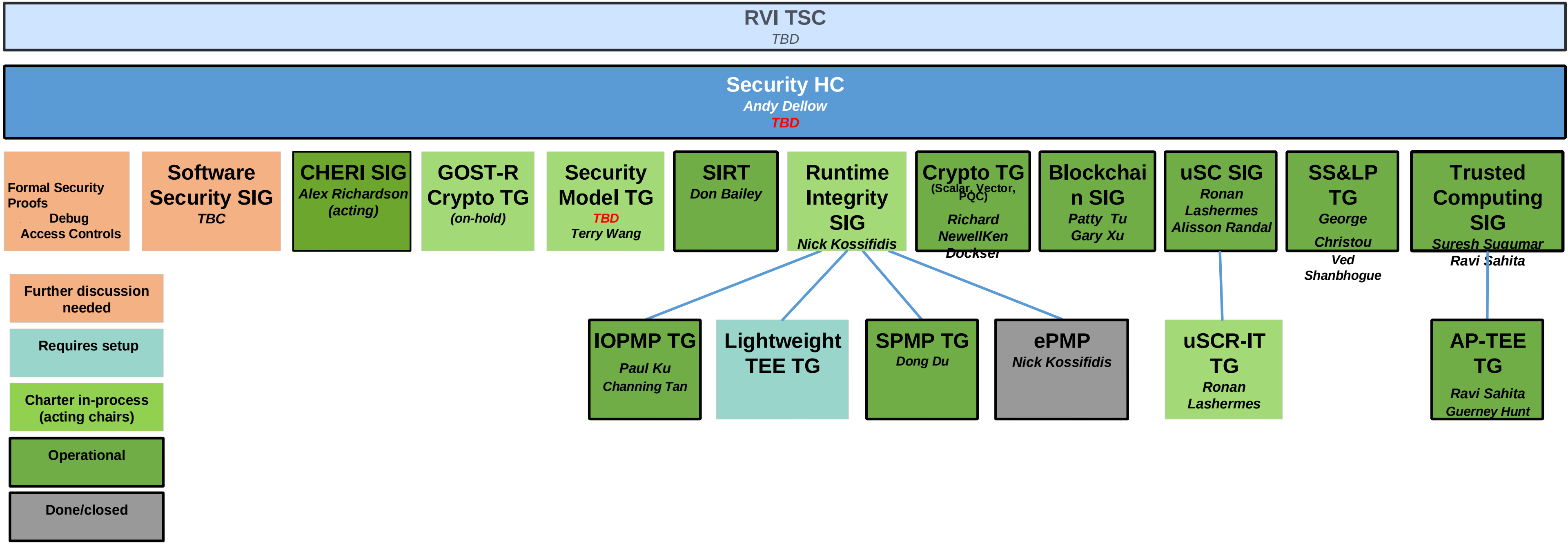
- *Please offer up / volunteer as candidate for chair. This is a critical TG*

others

- CHERI SIG – status
  - *Alex on honeymoon so on hold with set up until his return. Cambridge may yet offer vice chair but unable to attend today*
- Runtime Integrity SIG – Nick - status update
  - *Charter done, Jeff will help set up the infrastructure and formally begin the steps to have an approved sig*
- Lightweight TEE – Nick ?
  - *May be called m-mode isolation*
  - *Overlap with confidential compute requirement for isolated attestable TCB*
  - *Agreed a call between the sig and TG chairs and vice chairs to define the functional split and next steps.*
  - *Guerney offered to chair as he is close to AP-TEE as well.*
- AP-TEE – Ravi - progress update, next steps
  - *Scheduling clash, Ravi had to leave early. Will add to agenda for next time.*

- Any other Updates from TGs + SIG
  - *Nick reported on memory tagging draft.*

Current Organisation



RVI TSC
TBD

Security HC
Andy Dellow
TBD

Formal Security Proofs
Debug
Access Controls

Software Security SIG
TBC

CHERI SIG
Alex Richardson (acting)

GOST-R Crypto TG
(on-hold)

Security Model TG
TBD
Terry Wang

SIRT
Don Bailey

Runtime Integrity SIG
Nick Kossifidis

Crypto TG
(Scalar, Vector, PQC)
Richard NewellKen Dockser

Blockchain SIG
Patty Tu
Gary Xu

uSC SIG
Ronan Lashermes
Alisson Randal

SS&LP TG
George Christou
Ved Shanbhogue

Trusted Computing SIG
Suresh Sugumar
Ravi Sahita

IOPMP TG
Paul Ku
Channing Tan

Lightweight TEE TG

SPMP TG
Dong Du

ePMP
Nick Kossifidis

uSCR-IT TG
Ronan Lashermes

AP-TEE TG
Ravi Sahita
Guerney Hunt

Further discussion needed

Requires setup

Charter in-process (acting chairs)

Operational

Done/closed