Security HC Meeting

June 22nd, 2023

Agenda

- SIG and TG announcements made – CHERI, Runtime Integrity, AP-TEE-IO
- Source-ID generation, AKA Domain IDs. *what and where*
- Lightweight Isolation TG – *volunteers, charter, issues*
- Full round AES TG – *what and why*
- Vector Crypto Wrap up – *Fast Track ?*
- Debug control by role, per domain – *next steps*
- Others –
  - EU Legislation implications on open source
  - Office Hours
    Read Me on Github

Domain ID generation

- Nomenclature - source-ID, aka world ID will be named Domain ID -agreed
- Final Domain IDs will compound IDs, and may be implementation specific - agreed
- Supervisor Domain ID
  - We are proposing defining Supervisor Domain ID in the SmMTT TG. - agreed
  - Will be set by M-Mode. This may be a root domain manager, but could also be a simpler security monitor. Should be generic CSRs to set the SDID to allow other use cases outside of confidential VMs. Need to consider inputs from lightweight isolation TG.
  - SDID can be carried on the bus
- Need a Semi Static option to set the Root Domain ID
  - CSR format to match SDID
  - Propose lightweight isolation TG to include this aspect – a lot of discussion, Mark gave additional options, but decided it should be between the SmMTT and the Lightweight Isolation TG, most likely the lightweight isolation TG. TBC in the runtime integrity SIG

Lightweight Isolation TG

- Acting chair Guerney
- Vice Chair - Mark Hill
- Charter Update – Guerney and Cark to look at charter
- Issues to look at
  - De-priviledging approach:
    - SW implications, action - co-ordinate with the SW HC, confirm depriv approach is suitable
    - Performance on switching
    - PMP reuse – cant add SPMP in lightweight systems, too expensive
      - delegate individual PMP entries to S-mode ? Lightweight MTT ?
    - Secure Function Calls, S-S, S-M
      - supported in ARM TZ-M
    - Interrupts and exception handling – minimal TCB, FW reuse
      - Low latency interrupt to s-mode RTOS (blocked when in M-mode)
  - Root Domain ID – likely to be discussed in this group
- Other issues understood, and to be discussed in the TG once formed. SW agreement and Charter are next steps

Full Round AES TG

- Why –
  - Robustness – SCA resistant implementation
  - Key Management
    - Key handles
      - Setting and usage by privilege level, domain

- Do we agree this is needed ? Some discussions on how this seems to overlap with an embedded SE, but actually the approach is common and widely used on intel CPUs (bitlocker etc). Markku sent a link. Agreed this is needed. To follow up with Richard et al.
- Volunteers ?

others

- Vector Crypto Wrap up – *Fast Track* ? - yes
- Debug control by role, per domain – *next steps – raise with SoC infra*
- Others –
  - EU Legislation implications on open source
    - Allison asked for interested parties to contact her, there is a discussion starting, and a meeting imminently
  - Office Hours

    Read Me on Github - added