arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman

2022-04-11

Recent community activity (thank you!)

- Neil Armstrong / Nordic
  - PRs for Use PSA Crypto More epic – mostly merged
  - PRs for PSA – Long Term Secrets – in review
- Archana Madhavan / SiLabs
  - PR for code-gen 1.1 (introduction of JSON driver tooling)
    - Update had a round of review, awaiting updates
- Peter Spacek / SiLabs
  - Use PSA for hashing in TLS 1.3 - assigned
- François Beerten / Silex
  - PSA driver support for entropy gathering – progressing after review
- Various (Glen Strauss / lighttpd, IoTerop, …)
  - Accessors for various fields made private in Mbed TLS 3.0 – issues, discussions & PRs
  - Majority of issues now addressed

Major activities within core team

- OpenCI
  - Ubuntu CI now publicly visible – more coming
- GitHub migration from ArmMbed to Mbed-TLS organization complete
  - Better reflect independence from Mbed OS projects / TF.org ownership
  - Easier management of GitHub (e.g., team members, CI bots, etc)
- TLS 1.3
  - Client side progress: version negotiation, Certificate Verify message completed
  - Migrating to using PSA
  - Server side functionality and PSK started
    - Community help welcomed on these!
- 3.2 – planned for Q2
  - Working on adding accessor functions for some things dropped from the public API in 3.0
  - Aim to cover most/all issues reported by community

- Storage format stabilization
  - Testing & documentation to assure stable format for non-volatile storage
- PSA Crypto
  - On-going collaboration including Arm, SiLabs, Nordic
  - Support accelerators for all crypto in TLS 1.2, 1.3, X.509
  - Isolation of long-term secrets (e.g. PSK, private keys)
- Performance
  - SHA optimisations for aarch64 crypto extensions – SHA-256, SHA-512 around 7x perf and 4.5x uplift done
  - Bignum and ECP optimization started
- Review workload
  - Struggling for review bandwidth – any assistance from the community is hugely valuable
  - Easing the general review load accelerates progress on work prioritized by the community

arm