Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman
2022-07-18

Recent community activity (thank you!)

- Glenn Strauss
  - X.509 code-size and memory-size PRs
- EdDSA
  - Community contribution of SHA-3, SHAKE, CSHAKE, KMAC Ed25519 and Ed448 (legacy interface)
  - Review steadily progressing through 2022
  - Community interest in merging this
- Misc
  - make dependency tidy-up – in progress
  - make – shared library naming improvement
- François Beerten / Silex
  - PSA driver support for entropy gathering #5437
    - Design review complete
    - Francois working on testing (currently paused)
- Archana Madhavan / SiLabs
  - PR for code-gen 1.1 (introduction of JSON driver tooling) #5396
  - Going through cycle of review & updates, progressing towards resolution
- SecureMark-TLS / Cuno Pfister
  - Support for PSA Crypto using Mbed TLS 3.1 added

Major activities within core team

- Mbed TLS 3.2.1 released July 12
  - 3.2.1 is a bug-fix for 3.2.0
    - restores a file that was missing (no functional change)
    - no need to upgrade if 3.2.0 works for you
  - Address most 3.0 API issues reported by community
    - Adds many accessor functions – address issues caused by making various fields private in 3.0
    - Thanks to Glenn Strauss for many of these
  - TLS 1.3
    - Client authentication by server
    - Server HelloRetryRequest
    - Client-side version negotiation
    - Build with TLS 1.3 but without TLS 1.2 support
    - Server support (ephemeral key only)
  - PSA
    - USE_PSA_CRYPTO causes almost all crypto in TLS and X.509 to use PSA
    - Exceptions: EC J-PAKE, FFDH, RSS-PSS signature verification
  - Performance
    - SHA-256 and SHA-512 have Arm aarch64 optimized implementations (7.5x and 4.5x faster than Mbed TLS 3.1)

- Website
  - tls.mbed.org went down
  - Pointed at the new website, but some old content is missing
  - Currently restoring old content via ReadTheDocs

- OpenCI
  - Running well, expect to fully transition to this soon
  - Windows coming very soon – currently FreeBSD / Ubuntu
  - Please let us know your feedback

- Q3 plans – focus on
  - PSA code-size optimisations
  - Bignum performance optimization
  - TLS 1.3 PSK
  - PKCS #7

- 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