Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman

2023-10-23

Recent community activity (thank you!)

- Valerio Setti @Nordic
  - Clarify driver handling of ALG_STREAM and ALG_ECB
  - Fix error reporting in driver testing parity
  - ~~Improve location of MD_CAN macros~~
  - ~~Fix dependencies of mbedtls_pk_ec_ro and mbedtls_pk_ec_rw~~
  - Add test component with all ciphers and AEADs accelerated only
  - ~~Change accel_aead component to full config~~
  - Create Cipher light
  - Make CTR-DRBG use cipher.c when available
  - Make PEM use cipher.c when available
  - PSA crypto should not depend on the cipher module

- Misc
  - Add CodeQL Workflow for Code Security Analysis – b4yuan
  - Use CMAKE_C_SIMULATE_ID when available to determine compiler - daantimmer
  - Fixes "CSR parsing with critical fields fails" - mschulz-at-hilscher
  - Fix compiling AESNI in Mbed-TLS with clang on Windows – sergio-nsk
  - Backport 2.28: Fix compiling AESNI in Mbed-TLS with clang on Windows – sergio-nsk
  - Remove trailing whitespace on grep command in prepare_release.sh – mcagriaksoy
  - Add ignoring return value casting and Fix non-uniform cast – mcagriaksoy
  - Rename local variable in aes.c - kasjer
  - [Backport 2.28] Rename local variable in aes.c – kasjer
  - Add missing casting size_t to int on ssl_tls13_keys.c – mcagriaksoy
  - Fix C++ build issue when MBEDTLS_ASN1_PARSE_C is not enabled – kloolk
  - Restore Windows XP platform support – irwir
  - Fix doc on GCM API - ivq
  - ssl: fix critical extension handling regression – askourtis
  - Support compilation using CLang on Windows - SlugFiller
  - Add AES encrypted keys support for PKCS5 PBES2 – zvolin
  - Comply with the received Record Size Limit extension – kloolk
  - Guard ticket specific TLS 1.3 function with macro - inorick

Major activities within core team

https://github.com/orgs/Mbed-TLS/projects/1

- TF-PSA-Crypto
  - https://github.com/Mbed-TLS/TF-PSA-Crypto
  - Currently, read-only preview
  - Will become upstream source for crypto in Mbed TLS
- TLS 1.3 early data
- Driver-only cipher & AEAD
  - AES, GCM, CCM, ChachaPoly
- Thread-safe PSA

- Planning Mbed TLS 4.0 – Q3 2024?
  - PSA_CRYPTO_C / CLIENT always on
  - Consume TF-PSA-Crypto repository as source of PSA and crypto code
  - Remove some legacy interfaces & features
- TF-PSA-Crypto – productization
- CI
  - Testing on Arm coming soon
- Planning Mbed TLS 3.6 LTS - early 2024
  - TLS 1.3 early data, record size limit
  - PSA multi-threading support
  - Accessor functions for fields made private in 3.0
  - Driver-only cipher and AEAD

arm

Release Plans

- **3.5 – October 5**
  - Size optimization (including driver-only ECP, bignum)
  - p-256m – reduce code size for SECP256R1 ECDH and ECDSA
  - SHA-3
  - AES performance
  - PBKDF2 CMAC and HMAC
  - TLS 1.3 FFDH
  - TLS 1.3 server-side version negotiation

- **3.6 LTS – early 2024**
  - TLS 1.3
    - Finish support for early data
    - Record size limit extension
    - Key export
  - Driver-only cipher
  - PSA thread safety
  - Review private fields, add missing accessors
  - Final 3.x release

- **Timeline**
  - 3.5 end of September / early October
  - 3.6 LTS early 2024
  - 4.0 second half of 2024