Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2024-11-04

Recent community activity (thank you!)

- #9421 mfil - Implement TLS-Exporter
- merged: #9118 jetm - Backport 3.6: ssl_client2: Add Host to HTTP GET request
- merged: #9105 jetm - ssl_client2: Add Host to HTTP GET request
- #6556 polhenarejos - XChaCha20 and XChaCha20-Poly1305 support.
- #5824 polhenarejos - Add support to Ed448 in EdDSA
- #5823 polhenarejos - Add support for SHA-3 KMAC
- #5822 polhenarejos - SHA-3 cSHAKE128 and cSHAKE256 support
- #5821 polhenarejos - SHA-3 SHAKE128 and SHAKE256 support
- #5819 polhenarejos - Add support for EdDSA with ed25519 curve (pure ed25519, ed25519ctx and ed25519ph)
- #7977 ivq - Fix doc on GCM API
- #9489 rsaxvc - Optimize software gcm_mult() routines on strictly-aligned systems
- #9127 nbfalcon - constant_time.h: add #ifdef __cplusplus guard
- merged: #9711 ThePassionate - net/mbedtls_net_connect: Preventing double close problem
- merged: #9714 ThePassionate - [Backport 3.6] net/mbedtls_net_connect: Preventing double close problem
- merged: #9715 ThePassionate - [Backport 2.28] net/mbedtls_net_connect: Preventing double close problem

Recent community activity (thank you!)

Valerio (Nordic)

- #9562 valeriosetti - md: allow dispatch to PSA whenever CRYPTO_CLIENT is enabled
- #9371 valeriosetti - psasim: use shared memory as messaging system for client-server communication
- merged: #9728 valeriosetti - [Backport 3.6] Revert & fix #9690 workarounds
- merged: #9703 valeriosetti - Revert & fix #9690 workarounds
- merged: #9302 valeriosetti - PSA: use static key slots to store keys
- merged: #9448 valeriosetti - [Backport 3.6] PSA: use static key slots to store keys

Major activities within core team

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

- TF-PSA-Crypto — main focus in Q4
  - Splitting files, reworking some interfaces (configuration, platform, …)
  - https://github.com/Mbed-TLS/TF-PSA-Crypto
  - Will become upstream source for crypto in Mbed TLS
- Mbed TLS 4.0
  - PSA_CRYPTO_C / CLIENT always on
  - Consume TF-PSA-Crypto repository as source of PSA and crypto code
  - Remove some legacy interfaces & features
- Mbed TLS 3.6.2
  - Security fix release (CVE-2024-49195)
- Open for SPAKE2+ reviews (tasks defined on backlog board)

Reminder: please do not submit security patches directly on GitHub

- If you think you have found an Mbed TLS security vulnerability, then please send an email to the security team at mbed-tls-security@lists.trustedfirmware.org.
- We keep pending security issues and patches private until we can make a release with the fixes.

Release Timeline

- 4.0 currently aiming for first half of 2025
- 3.6 LTS supported until early 2027
    - 3.6.1 (Aug 2024): mostly fixes related to TLS 1.3
    - 3.6.2 (Oct 2024): security fix
    - 3.6.3 (TBA): will support a PSA key store in builds without malloc
- 2.28 LTS ends supported life end of 2024

TF-PSA-Crypto 1.0 + Mbed TLS 4.0 highlights

- TLS 1.2: removing finite-field DH, static ECDH, PKCS#1v1.5 RSA encryption, ~~CBC~~
- Crypto: removing PKCS#1v1.5 RSA encryption, DES, EC curves smaller than 250 bits
- Removing all crypto ALT (use PSA drivers instead)
- Removing low-level crypto APIs (use PSA APIs instead)
  - Removing cipher.h; Keeping parts of md.h and pk.h partially as transition layers
  - Removing direct access to bignum/ECC arithmetic
  - Removing direct access to DRBG

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה

ధన్యవాదములు