Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath
2025-01-13

Recent community activity (thank you!)

- #9872 rojer - Defragment incoming TLS handshake messages
- #9876 winterheart - Mbedtls 3.6 subslotting
- #9797 NadavTasher - Added minimal TLSv1.3-only client configuration
- merged: #9798 NadavTasher - Added debug print in tls13 ssl_tls13_write_key_share_ext
- #8458 yuhaoth - Improve readability of random bytes generator on tls12 server hello
- #6280 yuhaoth - TLS 1.3: PSK: Add psk ephemeral test generate scripts
- merged: #9777 hughsie - Add a SBOM file in CycloneDX format
- #8795 winterheart - Allow install headers to different location
- #8800 winterheart - Allow install headers to different location (mbedtls-3)

Recent community activity (thank you!)

Valerio @Nordic

- #9863 valeriosetti - Move most of min_requirements.py to the framework
- #9864 valeriosetti - [Backport 3.6] Move most of min_requirements.py to the framework
- #9888 valeriosetti - Move pkgconfig.sh to the framework
- #9889 valeriosetti - [Backport 3.6] Move pkgconfig.sh to the framework
- merged: #9853 valeriosetti - Move tests/scripts/check_names.py to the framework
- merged: #9854 valeriosetti - [Backport 3.6] Move tests/scripts/check_names.py to the framework
- merged: #9826 valeriosetti - [3.6] Move "easy" basic checks scripts to the framework
- merged: #9825 valeriosetti - Move "easy" basic checks scripts to the framework

Major activities within core team

https://github.com/orgs/Mbed-TLS/projects/18

- TF-PSA-Crypto
  - https://github.com/Mbed-TLS/TF-PSA-Crypto
  - It is now the upstream source for crypto in Mbed TLS
  - The CI currently still pulls in Mbed TLS
  - Work is being done to remove this dependency
- 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
  - Focus is on re-planning and investigation
- Mbed TLS 3.6.3/2.28.10
  - Last release for the 2.28 LTS branch
  - MBEDTLS_PSA_STATIC_KEY_SLOTS feature in 3.6.3

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 (25Q1): will support a PSA key store in builds without malloc
- 2.28 LTS ends supported life after one last release in 25Q1

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