arm

TF-M Profile

David Wang

19 Dec 2019

Why?

- Dramatic variation in device capabilities and use cases
  - Secure software takes significant portion of hardware resources
  - Diverse use-cases with differing security requirements
- PSA vision is to raise the bar on security and make security easier
  - Is the market ready to pay the price for security?
- All use cases don’t need same level of security
- ALL use cases don’t need ALL of the security
- TF-M current memory usage poses a challenge for usage in ultra constrained devices

Profile Proposal

- Predefined list of base profiles
- Targeted towards use-cases with different hardware constraints
- Proven to work, tested in CI
- Alignment with PSA specifications and certification requirements

Profile 1 Features (Proposal)

- Lightweight boot
  - Rollback protection, Single binary (SPE+NSPE)
- Lightweight Framework
  - L1 isolation, Library/SFC mode, Buffer sharing allowed (need to check the usage in SP carefully)
  - Single secure context
- Storage
  - eFlash available, Internal Trusted Storage (ITS), No encryption
  - No internal transient buffers, client buffers used, No rollback protection
- Crypto
  - Symmetric (say AES), Cipher Suite for PSK TLS (AES128-CBC-SHA256).
- Attestation
  - Compile time generated token structure, Only IAT
  - HMAC based authentication.

arm

Profile 2 Features (Proposal)

- Lightweight boot
  - Rollback protection, Single binary (SPE+NSPE)
- Lightweight Framework
  - L1/L2 isolation, buffer sharing allowed in L1 (need to check the usage in SP carefully)
  - Multiple secure context
- Storage
  - eFlash available, ITS, No encryption, Protected Storage (Optional)
  - Scalable internal transient buffers, No rollback protection
- Crypto
  - Symmetric & Asymmetric, Cipher Suite for TLS1.2 (say AES-128-GCM/CCM, ECDSA, RSA,ECDH,SHA-256,HMAC)
- Attestation
  - Compile time generated token structure, Only IAT

arm

Profile 3 Features (Proposal)

- Profile 2 +
- Level3 Isolation
- Audit Log
- Everything else

arm

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
תודה