TF-M Profile Proposal

01-Nov-19

Why?

- Dramatic variation in device capabilities and usecases
  - 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 usecasesdon’t need same level of security

- ALL usecasesdon’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

Memory Usage Today on MuscaB1e

@10 Sept 19
TF-M Master

Build Config	Compiler	Code + RO Data	RW + ZI Data	Comments
ConfigCoreIPCTfmLevel2 (Level2 Isolation, IPC)	ARMCLANG	122k	64k	Audit Log Secure Partition Not Present. Separate Stack for each partition.
	GCC	127kB	64K	
ConfigDefault (Level1 Isolation, Lib Mode)	ARMCLANG	124k	49k	
	GCC	129K	49K	

Memory Usage Today on MuscaB1e

Partition	Code + RO Data	RW + ZI Data
TF-M Core	24K	13K
Crypto	88K	36K
Secure Storage	6K	12K
Attestation	4K	3K
Total	**122k**	**64k**
Secure Boot	20K	22K

@10 Sept 19

TF-M Master

Profile 1

- Lightweight boot
  - No rollback protection, Single binary (SPE+NSPE)
- Lightweight Framework
  - L1 isolation, Library/SFC mode, Buffer sharing allowed
  - Single secure context, Secure stack defined at initialization
- Storage
  - eFlash available, ITS, No encryption
  - No internal transient buffers, client buffers used, No rollback protection
- Crypto
  - Symmetric (say AES), Cipher Suite for PSK TLS (say HMAC, SHA-256). Leverage HW Crypto
- Attestation
  - Compile time generated token structure, Only IAT
  - HMAC based authentication.

Profile 2

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

Profile 3

- 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