COSE: AES-CTR and AES-CBC

draft-ietf-cose-aes-ctr-and-cbc-01

Russ Housley and Hannes Tschofenig

Background

- The SUIT WG is using CBOR and COSE
- The SUIT WG is working on firmware encryption scheme, which is also expected to be used in TEEP
    - https://datatracker.ietf.org/doc/html/draft-ietf-suit-firmware-encryption-09
- IETF 114: Explained need for ciphers without integrity protection
    - Existing bootloaders use AES-CTR for firmware encryption
    - Lack of encryption expansion makes the job much easier
    - Signature over plaintext payload provides integrity protection
- This draft registers AES-CTR and AES-CBC
    - Only allowed in combination with a separate integrity mechanism
    - COSE WG adopted the draft on 11 Oct. 2022

Proposed Algorithm Registrations

Name	Value	Key Size	Description	Recommended
A128CTR	TBD1	128	AES-CTR w/ 128-bit key	Deprecated
A192CTR	TBD2	192	AES-CTR w/ 192-bit key	Deprecated
A256CTR	TBD3	256	AES-CTR w/ 256-bit key	Deprecated
A128CBC	TBD4	128	AES-CBC w/ 128-bit key	Deprecated
A192CBC	TBD5	192	AES-CBC w/ 192-bit key	Deprecated
A256CBC	TBD6	256	AES-CBC w/ 256-bit key	Deprecated

Concerns about AES-CTR and AES-CBC

- Signature Stripping
- AES-GCM to AES-CTR authentication key compromise attack
- AES-GCM to AES-CTR malleability attacks
- AES-GCM to AES-CBC plaintext recovery attacks

Security Considerations text for each of these was proposed on the mail list

Possible Ways Forward

Options:

1. Proceed with the proposed security considerations text
2. Drop AES-CBC; proceed with the proposed AES-CTR security considerations text
3. Stop working on this document –
    a. Tell SUIT WG to figure out a way to use an AEAD
    b. At least some bootloaders will not use the SUIT solution