Object Security of COAP

draft-selander-ace-object-security-03

Göran Selander, Ericsson
John Mattsson, Ericsson
Francesca Palombini, Ericsson
Ludwig Seitz, SICS Swedish ICT

IETF 94 COSE WG, Yokohama, November 3, 2015

Context

- One design goal of Constrained Application Protocol (CoAP): “keep message overhead small, thus limiting the need for fragmentation.”
- Where does the energy go? … **Communication**!
- 6LoWPAN L2 packets are limited to 127 bytes including various overheads

Examples

- Integrity Protection only
  - MAC → HMAC-SHA256
  - Signature only → ECDSA with 64 bytes signature
- Integrity Protection and Encryption
  - AEAD → AES-CCM
  - Symmetric Encryption Asymmetric Signature (SEAS) → AES-CTR + ECDSA

Information Elements

Integrity Protection Only	Encryption & Integrity Protection
› Sequence Number › Context Identifier	
› CoAP Payload	› Ciphertext
› Signature / MAC	

COSE Profile: MAC

- Sequence Number
- Context Identifier

CoAP Payload	Ciphertext

- Signature / MAC

```
[
  msg_type,
  protected: alg, seq,
  unprotected: -
  payload
  MAC,
  [                              #recipients:
    [                            #recipient:
      protected: -
      unprotected: alg:dir, cid
      ciphertext: -
    ]
  ]
]
```

Suggested Modification for COSE

1. “Flattened out” structure: no recipients, no multiple signatures
2. Security context defines uniquely the cipher suite: no alg parameter
3. All parameters should be protected when possible : no “unprotected” field
4. Define key/label values for the introduced parameters and algorithms

COSE modified profile: MAC

- Sequence Number
- Context Identifier

CoAP Payload	Ciphertext

- Signature / MAC

```
[
  msg_type,
  protected: cid, seq,
  payload,
  MAC
]
```

Message Overhead Example

- HMAC-SHA256

Scheme	seq+cid	MAC	Total Size	Overhead
COSE	11 B	16 B	53 bytes	26 bytes
mod-COSE	11 B	16 B	37 bytes	10 bytes
bound	11 B	16 B	32 bytes	5 bytes

- ECDSA with 64 bytes signature

Scheme	seq+cid	SIG	Total Size	Overhead
COSE	11 B	64 B	100 bytes	25 bytes
mod-COSE	11 B	64 B	86 bytes	11 bytes
bound	11 B	64 B	81 bytes	6 bytes

The message size is calculated without payload

Message Overhead Example

- AES-CCM

Scheme	seq+cid	TAG	Total Size	Overhead
COSE	11 B	8 B	44 bytes	25 bytes
mod-COSE	11 B	8 B	29 bytes	10 bytes
bound	11 B	8 B	24 bytes	5 bytes

- AES-CTR-ECDSA

Scheme	seq+cid	SIG	Total Size	Overhead
COSE	11 B	64 B	134 bytes	59 bytes
mod-COSE	11 B	64 B	86 bytes	11 bytes
bound	11 B	64 B	81 bytes	6 bytes

The message size is calculated without payload

ERICSSON

Thank you!

Comments/questions?

COSE profile: Sig

- Sequence Number
- Context Identifier

CoAP Payload	Ciphertext

- Signature / MAC

```
[
  msg_type,
  protected: seq,
  unprotected: -
  payload
  [                              #signatures:
    [                            #signature:
      protected: alg, cid
      unprotected: -
      SIG
    ]
  ]
]
```

COSE profile: Sig

- Sequence Number
- Context Identifier

CoAP Payload	Ciphertext

- Signature / MAC

```
[
  msg_type,
  protected: cid, seq
  payload,
  SIG
]
```

COSE profile: AEAD

- Sequence Number
- Context Identifier

CoAP Payload	Ciphertext

- Signature / MAC

```
[
  msg_type,
  protected: alg, seq,
  unprotected: -
  TAG: -
  [                          #recipients:
    [                        #recipient:
      protected: -
      unprotected: alg:dir, cid,
      ciphertext
    ]
  ]
]
```

COSE profile: AEAD

- Sequence Number
- Context Identifier

- CoAP Payload
- Ciphertext

- Signature / MAC

```
[
  msg_type,
  protected: cid, seq,
  ciphertext,
]
```

COSE profile: SEAS

- Sequence Number
- Context Identifier

CoAP Payload	Ciphertext

- Signature / MAC

```
[
  msg_type,
  protected: seq,
  unprotected: -
  payload: COSE_encryptData
  [                #signatures:
    [              #signature:
      protected: -
      unprotected: alg:dir, cid
      SIG
    ]
  ]
]
```

```
[
  msg_type,
  protected: -
  unprotected: -
  TAG: -
  [            #recipients :
    [          #recipient:
      protected: alg, cid
      unprotected: -
      ciphertext
    ]
  ]
]
```

COSE profile: SEAS

- Sequence Number
- Context Identifier

CoAP Payload	Ciphertext

- Signature / MAC

```
[
  msg_type,
  protected: cid, seq,
  ciphertext,
  SIG
]
```