Authenticated Encryption with Replay prOtection (AERO)
AERO

- Authenticated Encryption algorithm
- Stateful and self-synchronizing
- Easy to use
- Robust against nonce misuse and decryption misuse
- Saves bandwidth
  - No nonce, no sequence number
- New standards contributions and research
Communication Security Goals

- Unreliable transport
  - Message loss
  - Message reorder

- Multiple senders, multiple receivers

- Adaptive chosen plaintext, chosen ciphertext attacks
  - Security against forgery
  - Plaintext indistinguishable from random
Conventional A+E with Extended SEQ

- **Header**
- **SEQ HI**
- **SEQ LO**
- **IV**
- **Ciphertext**
- **Tag**

**Message**

**AES-CBC Encryption**

**HMAC**
Conventional Decryption

- Ciphertext
- HMAC
- AES-CBC Decryption
- Message
Authenticated Encryption with Associated Data (AEAD)

<table>
<thead>
<tr>
<th></th>
<th>Header</th>
<th>SEQ</th>
<th>IV</th>
<th>Ciphertext</th>
<th>Tag</th>
</tr>
</thead>
</table>

Message

AES-GCM Encryption

SEQ HI

SEQ LO
Authenticated Encryption with Associated Data (AEAD)

 AES-GCM Encryption

Ciphertext

Message

Header | SEQ | IV | Ciphertext | Tag

Bandwidth: SEQ, IV, Tag
Authenticated Encryption with Associated Data (AEAD)

Multiple receivers awkward

Bandwidth: SEQ, IV, Tag
Authenticated Encryption with Associated Data (AEAD)

Multiple receivers awkward

IV hard to manage
Multiple senders
INSECURE if mismanaged

Bandwidth: SEQ, IV, Tag

AES-GCM Encryption

Message

Header | SEQ | IV | Ciphertext | Tag
Authenticated Encryption with Associated Data (AEAD)

- Complex to use
- IV hard to manage
- Multiple senders
- INSECURE if mismanaged
- Multiple receivers awkward
- Bandwidth: SEQ, IV, Tag

Diagram:
- Header
- SEQ
- IV
- Ciphertext
- Tag
- Message
- AES-GCM Encryption
Authenticated Encryption with Associated Data (AEAD)

- AES-GCM Encryption
- SEQ
- IV
- Tag
- Multiple receivers awkward
- IV hard to manage
- Multiple senders
- INSECURE if mismanaged
- Complex to use
- Decryption Misuse

Bandwidth: SEQ, IV, Tag
AERO Encryption

- Easy to use
- No IV to manage
- Multiple senders
- Secure if misused
- Minimal overhead
- Robust against decryption misuse
- Multiple receivers easy
AERO Encryption

Wide Pseudo Random Permutation (WPRP) Encryption

Header

Plaintext

Sequence Number

Ciphertext
Wide Pseudo Random Permutation (WPRP)

562a666ab08dae419b3 → WPRP Encryption → 0818a309a064f40a9b2
Wide Pseudo Random Permutation (WPRP)

562a666ab08dae419b3

WPRP Encryption

0818a309a064f40a9b2

562a666ab18dae419bf

WPRP Encryption

e295e324f8a7181ad927
Wide Pseudo Random Permutation (WPRP)

562a666ab08dae419b3
WPRP Decryption
0818a309a064f40a9b2

562a666ab18dae419bf
WPRP Decryption
e295e324f8a7181ad927

AES Extended Codebook (XCB) Mode of Operation
AERO Decryption

Wide Pseudo Random Permutation (WPRP) Decryption

Header

Ciphertext

plaintext

Candidate Seq Num

Return Plaintext, Update s

Check

Return FAIL

plaintext

(or)

FAIL

Return FAIL
Candidate Sequence Number Checking

- $s$: Largest sequence number accepted so far
- $r$: Last rejected candidate sequence number
- $2^{t-1}$: CSN
Likely next candidates

Largest sequence number accepted so far

Last rejected candidate sequence number
Candidate Sequence Number Checking

Largest sequence number accepted so far

Last rejected candidate sequence number
(Re)synchronization

- Largest sequence number accepted so far
- Last rejected candidate sequence number

Diagram:
- 0
- s
- r
- $2^{t-1}$
(Re)synchronization

Largest sequence number accepted so far

Last rejected candidate sequence number
Candidate Sequence Number Checking

- Reject
- Set $r$ to $s$
- Update $s$ bitmask
- Accept
- Accept
- Check bitmask
- Accept

$2t - 1$
Security of Authentication

Probability of successful forgery: \[ \frac{72}{2^t} \approx 2^{-t+7} \]
IPSec

ESP AES-GCM, AES-CCM, or AES-CTR plus HMAC-SHA1

- 4 bytes
- 4 bytes
- 8 bytes
- length of plaintext + pad
- 12 bytes

Ciphertext

ESP AERO

- 4 bytes
- plaintext length + 12 bytes

Ciphertext

- no misuse resistance
- 24+ bytes overhead per packet

- misuse resistance
- 12 bytes overhead per packet
Performance

• WPRP CPB ~ 1.5 x GCM CPB

• Inefficient on long messages
  Higher latency
  Larger memory requirements
  … but this is true of all AEAD methods …

• More efficient on short messages
  Short frames (about 100 bytes for 802.15)
    Four bytes less overhead means:
    ~ 4% less power used in transmission
    ~ 4% less power used in reception
    ~ 4% lower probability that retransmission is needed
Status

• Research
  Formalization of security models and goals
  WPRP encryption alternatives

• IETF
  
draft-mcgrew-aero-00.txt
  draft-mcgrew-srtp-aero-01.txt
  draft-mcgrew-dtls-aero-00.txt

• CAESAR
  Does not work with conventional AEAD API