Using Counter Modes with ESP and AH to protect Group Traffic

draft-ietf-msec-ipsec-group-counter-modes-05

mcgrew@cisco.com

Initialization Vectors

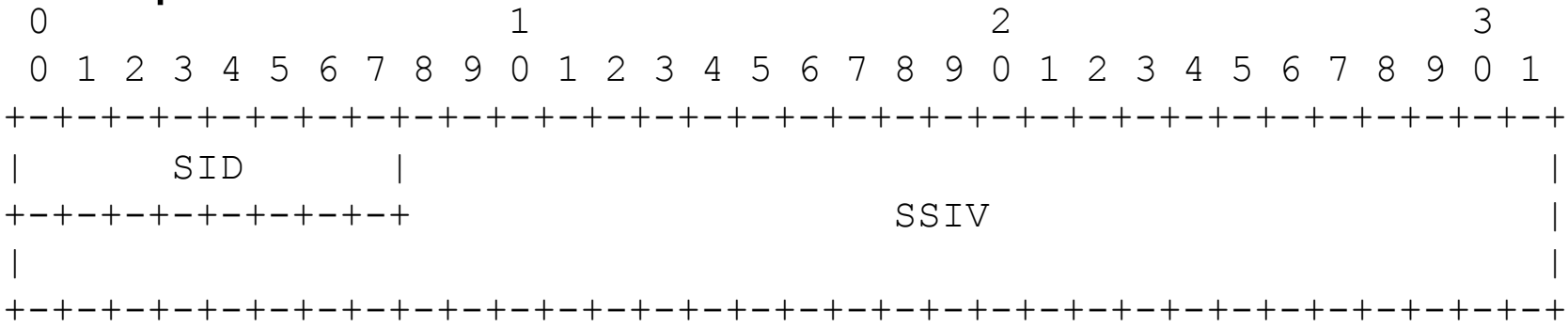
- ESP/AH CTR (RFC3686), GCM (RFC4106), CCM (RFC4309), GMAC (RFC4543) use 8-byte distinct IVs

```
IV in packet 1: 0000000000000001
IV in packet 2: 0000000000000002
IV in packet 3: 0000000000000003
IV in packet 4: 0000000000000004
IV in packet 5: 0000000000000005
IV in packet 6: 0000000000000006
IV in packet 7: 0000000000000007
```

Sender free to choose any IV values as long as they are distinct

Coordination of IV values

- Partition the IV field in two
  - Sender Identifer (SID) - unique to each sender, for all senders sharing the same SA
  - Sender-Specific IV (SSIV) - unique for each IV constructed by a particular sender for use with a particular SA



Example

a800000000000001	3e00000000000001	4400000000000001
a800000000000002	3e00000000000002	4400000000000002
a800000000000003	3e00000000000003	4400000000000003
a800000000000004	3e00000000000004	4400000000000004
a800000000000005	3e00000000000005	4400000000000005
a800000000000006	3e00000000000006	4400000000000006
A800000000000007	3e00000000000007	4400000000000007
. . .	. . .	. . .

MSEC Architecture

- Group Controller/Key Server (GCKS) responsible for managing SID values
  - Allocation during registration
  - Creates new SAs before SSIV exhaustion
- Group Member uses assigned SID
  - SHOULD notify GCKS prior to SSIV exhaustion

Status

- WG last call on -02 was Dec 2008
  - All comments addressed
  - January 2010 comment: I-D should cover ciphers other than AES as well
    - -02 addresses this point
- Ready for IETF Last Call