Using Counter Modes with ESP and AH to protect Group Traffic

draft-ietf-msec-ipsec-group-counter-modes-02

David McGrew
Brian Weis

Initialization Vectors

- ESP AES CBC (RFC 3602) uses 16-byte unpredictable IVs

```
IV in packet 1: 0307522f68fff3f0d28f24d694990532
IV in packet 2: 4a651cc9238b6984ac6cd35962d8c437
IV in packet 3: dbd0fd2449516adbafbfd7e3813f7636
IV in packet 4: cb69c75b94ba9458ee7fb1d8415d1026
IV in packet 5: 62ac2bbc2a736153aa38ed8fe9ac2602
IV in packet 6: 3e39be141c19cbfb815e17dce03ab4c8
IV in packet 7: 2bcdbf177ddf01f96a09c2eba3821d1e
```

Initialization Vectors

- ESP/AH CTR (RFC 3686), GCM (RFC 4106), CCM (RFC 4309), GMAC (RFC 4543) 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
```

Initialization Vectors

- ESP/AH CTR (RFC 3686), GCM (RFC 4106), CCM (RFC 4309), GMAC (RFC 4543) 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

Problem

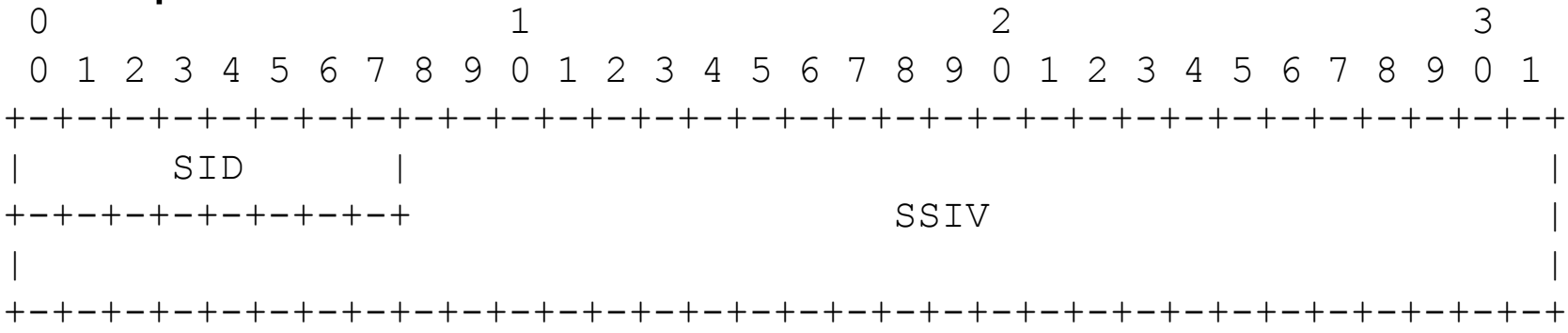
- AH/ESP AES modes requiring distinct IVs all have significant performance advantages
  - Suite B (RFC 4869)
- But when multiple senders use the same key, they need to ensure IV uniqueness
  - **Failure here voids security guarantees**

Solution

a800000000000001	3e00000000000001	4400000000000001
a800000000000002	3e00000000000002	4400000000000002
a800000000000003	3e00000000000003	4400000000000003
a800000000000004	3e00000000000004	4400000000000004
a800000000000005	3e00000000000005	4400000000000005
a800000000000006	3e00000000000006	4400000000000006
a800000000000007	3e00000000000007	4400000000000007

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



GCKS Responsibilities

- Group Controller/Key Server (GCKS) is responsible for managing SID values
  - Allocation of SIDs to group members during admission/registration into group
  - If all SID values are allocated, new senders MUST NOT be admitted
- GCKS will generate new SAs when a group member reports that it is in danger of exhausting its SSIV space

Group Member Responsibilities

- A group member SHOULD notify the GCKS in advance of its SSIV space being exhausted.
- If the GCKS does not respond before its SSIV space is exhausted, the group member MUST stop sending!

Status

- Comments welcome
  - Have some editorial feedback
- Ready for Working Group Last Call
  - Was ready after IETF70, but is dependent on draft-ietf-msec-ipsec-extensions-09
- Should be MSEC priority to ensure secure use of RFCs 3686, 4106, 4309, and 4543