draft-ietf-msec-ipsec-group-counter-modes-01

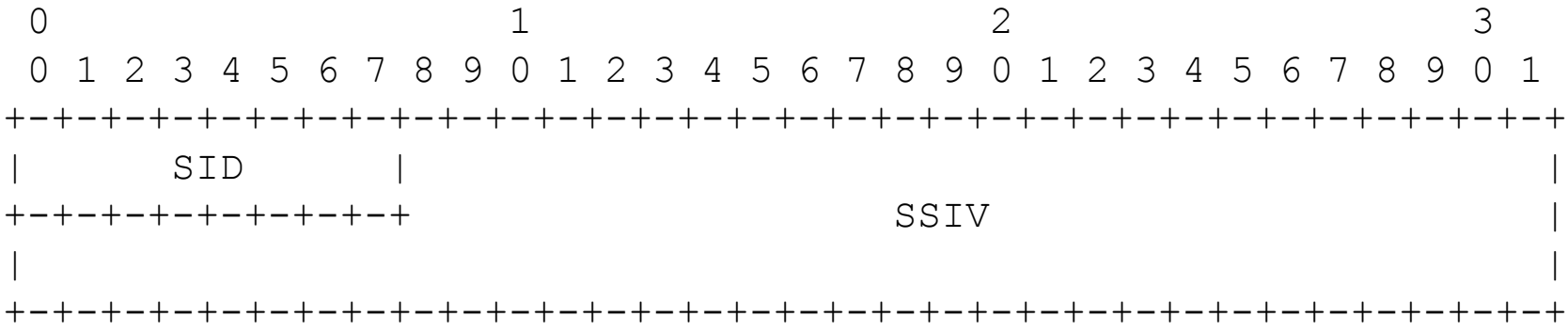
Brian Weis
David McGrew

AH/ESP AES Counter Modes

- Several AH/ESP AES counter mode transforms have been published: CTR (RFC 3686), GCM (RFC 4106), CCM (RFC 4309) and GMAC (RFC 4543)
- Counter modes require a unique IV per packet, and a counter is often used to satisfy this requirement.
  - But a counter mode used with multiple-sender group SAs puts the security of the group traffic at risk if there is no coordination of IV values between the senders.
- Counter modes provide performance and implementation advantages over other modes, which makes them valuable modes
- The goal of this I-D is to describe how to coordinate the IV values for multi-sender SAs.

Coordination of IV values

- Partition the IV field into two sub-fields
  - Sender Identifer (SID). This value is unique to a sender. Its size (e.g., 8 bits) depends on the application.
  - Sender-Specific IV (SSIV). This value is 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 into the group (“registration”).
  - If all SID values are allocated, new senders MUST not be allowed to join the group
- The 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 IV space being exhausted.
- If the GCKS does not respond before its SSIV space is exhausted, the group member is obligated to stop sending!

Next Steps

- Comments?
- Working Group Last Call?