draft-weis-esp-group-counter-cipher-00

Brian Weis
David McGrew

AM/ESP AES Counter Modes

- Several AH/ESP AES counter mode transforms have been published

  RFC 3686 ESP: Counter Mode (CTR)

  RFC 4106 Galois/Counter Mode (GCM)

  RFC 4309 Counter with CBC-MAC Mode (CCM)

  RFC 4543 Galois MAC Mode (GMAC)

- Counter modes require a unique IV per packet, and a counter is often used to satisfy this requirement.
  - But uses of a counter provides performance and implementation advantages over other modes.

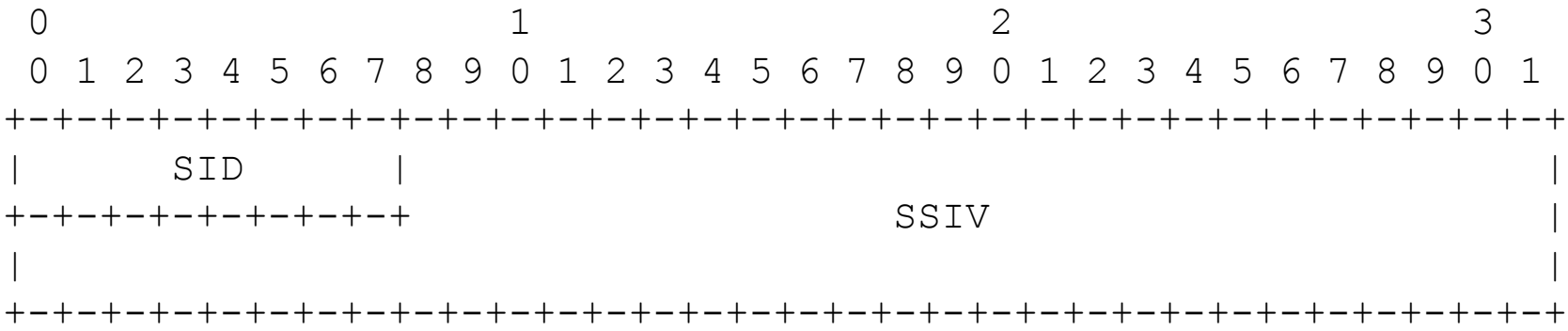
Applying counter mode to group SAs

- The requirement for a unique IV currently restricts counter modes to single-sender group IPsec Sas
- But multi-sender SAs used with Many-to-Many applications could benefit from counter mode benefits too.

This draft describes a method for supporting counter modes with multi-sender IPsec SAs

Proposed Method

- Partition the IV field into two sub-fields
  - Sender Identifer (SID). This value is unique to a sender (e.g., 8 bits).
  - Sender-Specific IV (SSIV). This value is unique for each IV constructed by a particular sender for use with a particular SA.



SID Allocation

- The Group Controller/Key Server (GCKS) is responsible for allocating a unique SID for each sender
  - For simplicity, the SID SHOULD be a sender attribute used with all group SAs
  - The GKCS can re-allocate a SID if and only if the previous sender is no longer part of the group, and after deleting all SAs on which the previous sender may have sent packets.
  - If all SID values are allocated, new senders MUST not be allowed to join the group

Effect of a shorter SSIV

- The group member is obligated to stop sending after its SSIV space is exhausted! A group member should not be leve without a replacement key.
  - A simple method of enforcement is for the GCKS to set SA lifetimes as a function of the expected or maximum packets/second rate from senders
- This method is not new -- even with non-counter modes it might not be safe to use the key for the entire set of valid IVs, and this can be enforced using SA lifetimes.
- However, the draft does propose some explicit actions as well.

Explicit GKM actions for avoiding an overused key

- Group member actions
  - A group member SHOULD notify the GCKS in advance of its IV space being exhausted.
- GCKS actions
  - A GKCS SHOULD support a group member notifying the GCKS that its IV space will soon be exhausted and requires a new SA to be distributed
  - A GCKS MAY choose to ignore this notification based on policy (e.g., if the group member appears to be asking for new SAs so frequent as to negatively affect group communications).

Discussion

- Should this draft become a working group draft?
- If not, how will the working group address these newer modes of operation?