In-Band Authentication Extension for Protocol Independent Multicast (PIM)

draft-bhatia-zhang-pim-auth-extension-00

Manav Bhatia
manav.bhatia@alcatel-lucent.com
Dacheng Zhang
zhangdacheng@huawei.com

Problem Statement

- Existing PIM security mechanisms mandate to use IPsec to provide message authenticity and integrity.
  - No suitable key management mechanism is provided to support multicast.
  - Extremely difficult to use and configure - as a result nobody uses it today.
  - When manual keying is used, the replay protection of IPsec does not work.
  - Replay attacks can seriously disturb the normal operations of PIM
    - For instance, when a PIM router received a hello message with a changed GenID and an re-initialized sequence number, it is difficult for the receiver to distinguish this message from a replay attack.

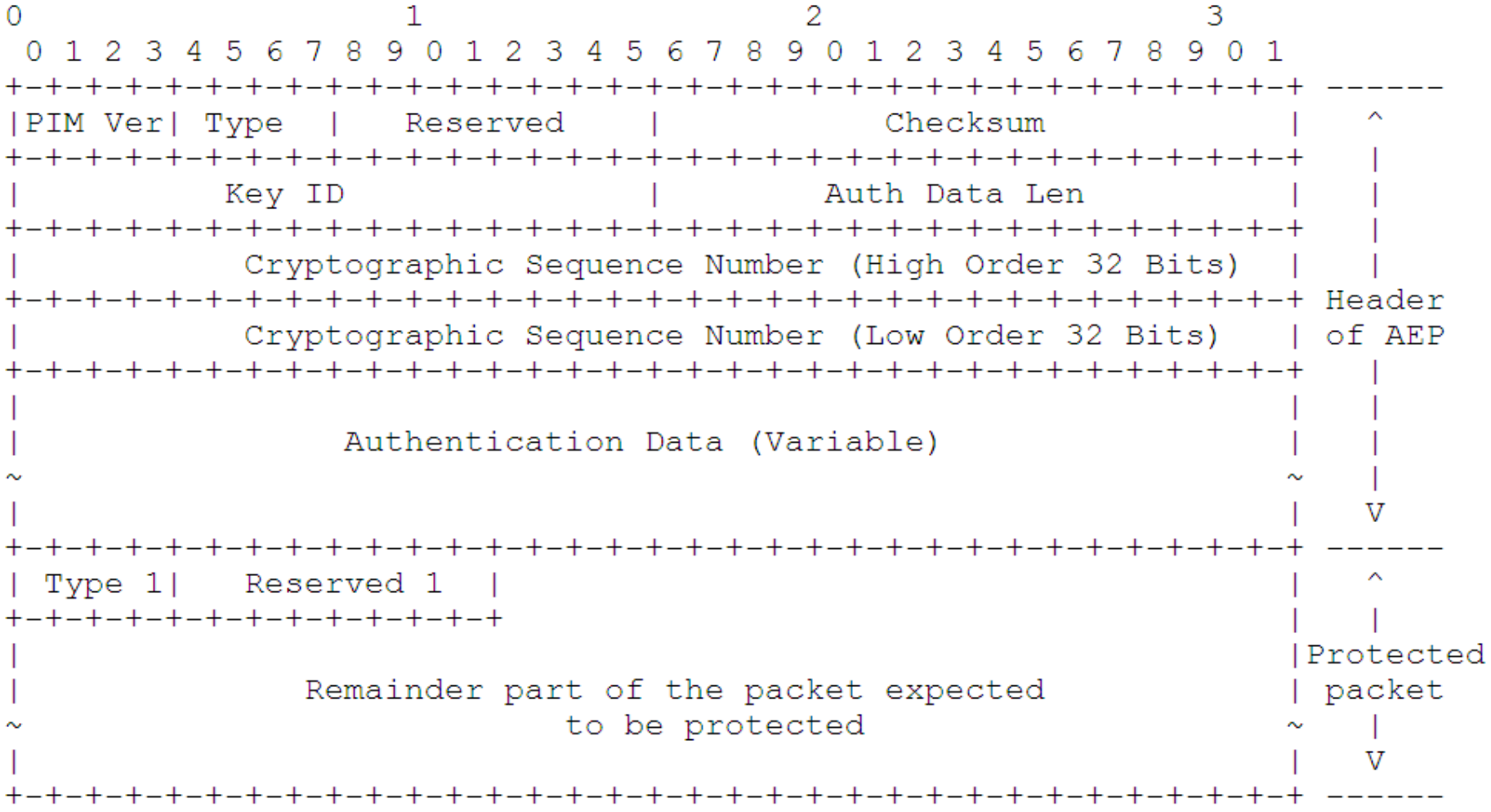
Related Work

- The issues raised by using IPsec to protect OSPFv3 have been discussed in both the KARP and OSPF WGs.
  - The analysis is proposed in *draft-ietf-karp-ospf-analysis*
  - An in-band security approach is proposed in *draft-ietf-ospf-auth-trailer-ospfv3*
- Applying similar principles in PIM
  - The analysis is done in *draft-bhatia-karp-pim-gap-analysis*

Solution

- Define an in-band security solution to replaces IPsec to provide message authenticity, integrity, and freshness.
  - A new type of PIM message is defined that encapsulates and secures other types of PIM messages.
  - Manual keying is assumed
  - The solution does not preclude the possibility of supporting automated keys in future.

Packet Format



Resistance on Replay Attacks:

- Protection against intra-connection replay attacks:
  - A monotonically increased sequence number is provided
  - The space of the sequence number should be big enough
- Protection against inter-connection replay attacks:
  - The base solution is subject to inter-connection replay attacks.
  - By using the approach proposed in *draft-ietf-ospf-security-extension-manual-keying*, this problem can be addressed
    - The first 32 bits of the sequence number is used to count the reboot times which is maintained in non-violated memory

Question?