

KARP WG

Protocol Independent Multicast-Sparse
Mode (PIM-SM) Gap Analysis



on behalf of
Manav Bhatia, Alcatel-Lucent
IETF 81, Quebec City

Current State of Security



- RFC 5796 describes how IPsec can be used to authenticate PIM-SM link local messages using ESP or optionally AH
- Mandates the use of manual keying as no automated key management currently exists that can be used



Gaps Identified

- Since it uses manual keying, no inter-connection and intra-connection replay protection mechanisms used
- Multiple PIM routers can exist on a link and setting up IPsec security associations manually is tedious
- Not all platforms support IPsec and few require an extra license for using IPsec

Result



- Because of operational complexity and license issues nobody is using IPsec to protect PIM-SM
- Most major vendors don't support IPsec protection for PIM
- Other issues detailed in the draft

So, what does the draft propose (1/2)



- In order to encourage deployment of PIM security we must provide an alternate authentication mechanism
- This will be similar to what was done for OSPFv3, where an Authentication Trailer is appended to the OSPFv3 packet, instead of relying on IPsec (as few folks were deploying that)

So, what does the draft propose (2/2)



- As part of KARP design guide phase 1, provide an authentication mechanism that uses manual keying
- Solution **MUST** provide inter and intra replay protection
- Solution **MUST** work for unicast and multicast PIM exchanges



Next Steps

- Currently only covers PIM-SM. It should be updated to include other flavors as well.
- Take this as the starting point for PIM gap analysis which falls within KARP WG's charter
- More discussion on the KARP and PIM mailing lists