Negotiation for Keying Pairwise Routing Protocols in IKEv2

draft-mahesh-karp-rkmp-04

Mahesh Jethanandani, Brian Weis, Keyur Patel,
Dacheng Zhang, Sam Hartman, U. Chunduri, A. Tian, Joe. Touch

IETF 86, March, 2013, Orlando, USA
Introduction

- Renamed from “TCP Authentication Option Master Key Tuple negotiation in IKEv2” to “Negotiation for Keying Pairwise Routing Protocols in IKEv2”

- Instead of only securing TCP-based pairwise Routing Protocol (RP) associations using the IKEv2 integrated with TCP-AO, aims to generate an automatic key management for unicast pairwise routing protocols,
  - Standard IKEv2 IKE_SA_INIT and IKE_AUTH Exchanges
  - Includes extensions to IKEv2 and its Security Associations to enable its key negotiation to support TCP-AO, BFD, and RSVP-TE
Support to BFD Authentication (1)

- Five types of authentication mechanisms are defined in RFC5880, Password, Keyed MD5, Meticulous Keyed MD5, Keyed SHA1, and Meticulous Keyed SHA1. Password needs not to be supported.
  - MD5 and SHA-1 is mandatory

- Two 5 types of authentication mechanisms are defined in draft-ietf-bfd-generic-crypto-auth Generic Authentication, and Generic Meticulous Authentication
  - According to draft-ietf-bfd-hmac-sha, SHA-256 is mandatory
Support to BFD Authentication (2)

- INTE Transforms are used to negotiate the algorithm to protect the message integrity.
  - INTEG transform IDs of AUTH_HMAC_MD5_96, AUTH_HMAC_SHA1_96, and AUTH_HMAC_SHA2_256_128 can be re-used.

- A new transform is defined to negotiate the authentication mechanism for BFD
## Support to BFD Authentication (3)

<table>
<thead>
<tr>
<th>INTEG Transform</th>
<th>BFD Transform</th>
<th>Authentication Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTH_HMAC_MD5_96</td>
<td>Base Authentication +</td>
<td>Keyed MD5</td>
</tr>
<tr>
<td>AUTH_HMAC_MD5_96</td>
<td>Base Meticulous Authentication +</td>
<td>Meticulous Keyed MD5</td>
</tr>
<tr>
<td>AUTH_HMAC_SHA1_96</td>
<td>Base Authentication +</td>
<td>Keyed SHA1</td>
</tr>
<tr>
<td>AUTH_HMAC_SHA1_96</td>
<td>Base Meticulous Authentication +</td>
<td>Meticulous Keyed SHA1</td>
</tr>
<tr>
<td>AUTH_HMAC_SHA2_256_128</td>
<td>Generic Authentication +</td>
<td>Generic Authentication</td>
</tr>
<tr>
<td>AUTH_HMAC_SHA2_256_128</td>
<td>Generic Meticulous Authentication +</td>
<td>Generic Meticulous Authentication</td>
</tr>
<tr>
<td>AUTH_HMAC_SHA2_256_128</td>
<td>Base Authentication +</td>
<td>ERROR</td>
</tr>
<tr>
<td>AUTH_HMAC_SHA2_256_128</td>
<td>Base Meticulous Authentication +</td>
<td>ERROR</td>
</tr>
</tbody>
</table>
Support to RSVP-TE Authentication

- MD5 is the only mandatory algorithm for integrity protection in the RSVP-TE authentication mechanism proposed in RFC2747. So, no new type INTEG transform needs to be defined.

- A RSVP-TE proposal requires a new type of transform, which indicates whether the integrity handshake (which is used to collect the latest sequence number associated with a key ID) is permitted.

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Not Allowed</td>
</tr>
<tr>
<td>1</td>
<td>Allowed</td>
</tr>
</tbody>
</table>
Notify and Delete Payloads

- A Notify Payload or Delete Payload contains a Protocol ID field.
  - The Protocol ID is set to TCP_AO (TBD1) when the message is relevant to the TCP-AO KeyID value contained in the SPI field.
  - The Protocol ID is set to BFD (TBD3) when the message is relevant to the BFD KeyID value contained in the SPI field,
  - The Protocol ID is set to RSVP-TE (TBD5) when the message is relevant to the RSVP-TE KeyID value contained in the SPI field.
IANA Consideration

- IANA is requested to add Three new Protocol Identifiers to the table:
  - Protocol Name "TCP-AO" value TBD1
  - Protocol Name “BFD” value TBD3
  - Protocol Name “RSVP-TE” value TBD5

- IANA is requested to add three new Transform Types for "Transform Type Values".
  - TBD2 for the TCP-AO transform
  - TBD4 for the BFD transform
  - TBD6 for the RSVP-TE transform
Questions?