TCP Authentication Option Master Key Tuple negotiation in IKEv2

draft-mahesh-karp-rkmp-02

Mahesh Jethanandani, Brian Weis, Keyur Patel, Dacheng Zhang, Sam Hartman, Uma Chunduri, Albert Tian

IETF 85, Nov. 2012, Atlanta, USA
Introduction

- Combines the work of “draft-chunduri-karp-using-ikev2-with-tcp-ao-02”

- Instead of generating an automatic key management for pairwise routing protocols, aims only to secure TCP-based pairwise Routing Protocol (RP) associations using the IKEv2 integrated with TCP-AO

  - Standard IKEv2 IKE_SA_INIT and IKE_AUTH Exchanges
  - Includes extensions to the Security Association payloads to enable its key negotiation to support TCP-AO.
  - Uses standard IKEv2 TS payloads to represent the traffic selectors for the routing protocol that will use the TCP-AO MKT (e.g., BGP or LDP).
Transforms Substructures (1)

- In order for IKEv2 to negotiate TCP-AO policy, a new Security Protocol Identifier needs to be defined in the IANA registry for "IKEv2 Security Protocol Identifiers".
  - This memo proposes adding a new Protocol Identifier to the table, with a Protocol Name of "TCP_AO" and a value of TBD1.

- Two MAC algorithms are supported in TCP-AO
  - HMAC-SHA-1-96 and AES-128-CMAC-96
  - Re-use the existing INTEG transform IDs of AUTH_HMAC_SHA1_96 and AUTH_AES_CMAC_96 respectively.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Mandatory Types</th>
<th>Optional Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-AO</td>
<td>INTEG, TCP</td>
<td>D-H</td>
</tr>
</tbody>
</table>
Transforms Substructures (2)

- No KDF algorithm is negotiated
  - In TCP-AO, the use of each INTEG algorithm implies the use of a specific KDF (deriving session keys from a master key)

- a new type of transform is defined, which describes whether TCP options are to be protected by the integrity algorithm.

```
+-----------------------------+
| Number | Name                      |
+-----------------------------+
| 0      | Options Not Integrity Protected |
| 1      | Options Integrity Protected   |
+-----------------------------+
```
Example of SA Payloads for TCP-AO

- The TCP-AO KeyID that is sent in the SPI field of an IKEv2 proposal.
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 a notify message is relevant to the TCP-AO KeyID value contained in the SPI field.
Questions?