Compression in IKEv2

draft-smyslov-ipsecme-ikev2-compression-01

Valery Smyslov
svan@elvis.ru

IETF 95
Advantages

- Compression of IKE_SA_INIT messages would keep their size bounded, thus saving them from IP fragmentation
- Compression of subsequent messages would make IKE fragmentation less likely
- Reducing size of IKEv2 messages would decrease power and network bandwidth consumption (important for IoT devices)
Effectiveness

- Message compressibility depends on its content and typically varies from 0% to ~30%

<table>
<thead>
<tr>
<th>Payload</th>
<th>Size</th>
<th>Compressibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA</td>
<td>Varies</td>
<td>Very good for large size</td>
</tr>
<tr>
<td>CERT</td>
<td>Large</td>
<td>Good</td>
</tr>
<tr>
<td>TS</td>
<td>Varies</td>
<td>Moderate</td>
</tr>
<tr>
<td>CP</td>
<td>Varies</td>
<td>Moderate</td>
</tr>
<tr>
<td>ID</td>
<td>Small</td>
<td>Moderate</td>
</tr>
<tr>
<td>NONCE, CERTREQ</td>
<td>Small</td>
<td>Bad</td>
</tr>
<tr>
<td>KE, AUTH</td>
<td>Average</td>
<td>Bad</td>
</tr>
</tbody>
</table>
Protocol Outline

• In IKE_SA_INIT new Compressed payload is used; it contains other payloads in compressed form
  – some payloads may be left uncompressed
  – Compressed payload has Critical bit set to allow interaction with legacy responders
  – compression algorithm can be negotiated
• In messages containing Encrypted payload compression is an extra optional step before encryption
Protocol Security

• Existing compression based attacks (CRIME, BREACH) rely on an ability for an attacker to insert arbitrary data into an encrypted stream containing secret data
  – no such possibility in IKEv2 (possibly except some EAP methods)
    • no secret information is transferred in IKE SA
    • no externally originated data is transferred in IKE SA
Protocol Security (continued)

- IKE_SA_INIT is unencrypted anyway – nothing to attack
- After IKE_SA_INIT is completed compression can be used selectively on a per-message basis
  - IKE SA messages that may contain secret data (e.g. some EAP methods) can be send uncompressed
Thanks

• Comments? Questions?
• More details in the draft
• Please review and send feedback to author