Media Description for IKE in SDP

draft-saito-mmusic-sdp-ike-02

Makoto Saito
ma.saito@nttv6.jp

Dan Wing
dwing@cisco.com
Status

• Chicago:
  – MMUSIC asked SIPPING to determine applicability
  – SDP-IKE was presented in SIPPING, and there was a valid use case

• Thus, would like to go forward with this idea in MMUSIC
Purpose

- Setting up IKE and IPsec Using SIP
  - Example: VPN to a home router (or NAT device)

1. INVITE Transaction
2. IKE (Media Session)
3. Validate Fingerprint of Certificate
4. Tunnel Mode IPsec
Proposal

• Exchange Fingerprint of Self-Signed Certificate for IKE Authentication
  – Same Concept as Comedia-TLS (RFC4572) and DTLS-SRTP
    \[a=fingerprint\]
  – SIP Identity (RFC4474) can provide Integrity of SDP
Proposal

• New Media Format Description “IKE”
  \[m=\text{application } 500 \text{ UDP IKE/ESP}\]
  (IKE over UDP, then IPsec over protocol 50)
  \[m=\text{application } 4500 \text{ UDP UDP/IKE/ESP}\]
  (IKE over UDP, then IPsec over UDP)

• New Attribute “udp-setup”
  – Similar to Comedia (RFC4145)
    \[a=\text{udp-setup}:\text{active} \quad \text{(IKE Initiator)}\]
    \[a=\text{udp-setup}:\text{passive} \quad \text{(IKE Responder)}\]
Changes in -02

• Added text explaining use with ICE
• Changed media format line
MMUSIC Interest?

• Interest in describing IKE/IPsec tunnel in SDP?
Thank you

draft-saito-mmusic-sdp-ike-02
## SIP or Dynamic DNS?

<table>
<thead>
<tr>
<th>Static DNS</th>
<th>Dynamic DNS</th>
<th>SIP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name Resolution to Floating IP Address</strong></td>
<td>-</td>
<td>Support</td>
</tr>
</tbody>
</table>
| **Authentication & Authorization** | - | - | Delegate to 3rd Party  
✓ No Signed Cert  
✓ No Whitelist |
| **UDP Hole Punching (ICE) for IKE & IPsec** | - | - | Applicable |
| **Deployment** | - | - | Prompt Re-use of Provider’s Existing SIP Infrastructure |