Outline

- Issues with TCP MD5
- Replacement Goals
- TCP-AO
- Status
TCP MD5 (RFC2385)

- Header just stores MAC:

<table>
<thead>
<tr>
<th>KIND=19</th>
<th>LEN=18</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>MD5 MAC (128 bits)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Not much else specified
Issues with TCP MD5

- MD5 weakness as a MAC
- Algorithm rigidity
- Does not specify intra-conn. rekeying
  - Doesn’t prohibit, but loses packets/window
- No replay protection
- Does not require per-conn. keys
- Underspecified w.r.t TCP
Replacement Goals

- Algorithm agile
- Allows rekeying
  - Without loss or window impact
  - Without requiring multiple tries (DOS issue)
- Replay protection
- Per-connection keys
- Supports manual and auto. keying
  - KMI agnostic
- **OBSOLETE TCP MD5**
TCP-AO

- Header includes KeyIDs:

<table>
<thead>
<tr>
<th>KIND=??</th>
<th>LEN=var</th>
<th>KeyID</th>
<th>RNExtKID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Various HMACs (curr. 96 bits)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- KeyID = current key for this HMAC
- RNExtKeyID = “ready” to receive key ID
TCP-AO Features

- Loss-free rekeying – KeyID
- Loss-free sync. use of new key – RNextKID
- Per-connection keys
  - Master key + ISNs -> conn. Key
- Replay protection
  - Via sequence number extensions
- Master key tuple (MKT) includes parameters
  - Conn. key alg., HMAC alg., TCP option incl. flag
- Fully specified w.r.t. TCP states/events
## TCP-AO Summary

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm agile</td>
<td>MKT indicates alg. Algs. specified separately.</td>
</tr>
<tr>
<td>Allows rekeying, esp. efficiently</td>
<td>KeyID for current segment MKT. RNextID for return path sync.</td>
</tr>
<tr>
<td>Replay protection</td>
<td>Ext. sequence numbers maintained, used in HMAC.</td>
</tr>
<tr>
<td>Per-connection keys</td>
<td>Derived keys using KDF.</td>
</tr>
<tr>
<td>Man/auto KMI agnostic</td>
<td>MKT treated as external. Parameter changes require MKT changes.</td>
</tr>
</tbody>
</table>
TCP-AO Future Plans

- NAT support
  - Currently a separate I-D
- Key management protocol
  - No current plans
Current Status

- In TCPM last call:
  - draft-ietf-tcpm-tcp-auth-opt – Touch/Mankin/Bonica
    - Explains probs. with TCP MD5, IPsec
    - Describes AO
  - draft-ietf-tcpm-tcp-ao-crypto – Lebovitz/Rescorla
    - Describes HMAC and KDF algs.

- In TCPM for discussion:
  - draft-touch-tcp-ao-nat – Touch
    - Describes NAT-compatible configuration
    - Requires MKT add a flag that modifies HMAC calc.