Domain Name Assertions

Richard Barnes
Jonas Lindberg
XMPP @ IETF80
Reminder: The Problem

- When XMPP services are delegated…
- How do you verify that a server is authorized to represent a domain?
- How can the providers in the middle re-use connections for many different customers?
High-level solution

• Authentication:
  – Use DNSSEC to verify SRV records
  – Keep an list of authorized domains per server

• Connection Sharing:
  – Keep a routing table that maps domain pairs to connections
  – Add some signaling to the XMPP stream to update this routing table
DNSSEC

```
_xmpp-server._tcp.target.tld. 400 IN SRV
   20 0 5269 xmpp1.receiving.tld

_xmpp-server._tcp.target.tld. 400 IN RRSIG
```

<table>
<thead>
<tr>
<th>Connection</th>
<th>Server Domain Names</th>
<th>Delegated Domain Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX</td>
<td>xmpp1.receiving.tld</td>
<td>target.tld</td>
</tr>
<tr>
<td>YYY</td>
<td>xmpp2.receiving.tld</td>
<td>target.tld</td>
</tr>
<tr>
<td>AAA</td>
<td>paris.example</td>
<td>paris.example</td>
</tr>
</tbody>
</table>
Routing Table

I: <db:result from='sender.tld' to='target.tld' />
R: <db:result type='valid'
    from='sender.tld' to='target.tld' />

+------------------+-----------------+---------------+
| Local            | Remote          | Connections   |
+------------------+-----------------+---------------+
| sender.tld       | target.tld      | XXX, YYY      |
| laurence.example | capulet.example  | AAA           |
| laurence.example | paris.example    | YYY, AAA      |
+------------------+-----------------+---------------+
### Overall Flow

<table>
<thead>
<tr>
<th>Originating Server</th>
<th>DNS Server</th>
<th>Receiving Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRV target.tld</td>
<td></td>
<td></td>
</tr>
<tr>
<td>receiving.tld</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Look up DNSSEC-signed SRV**
- **Establish a stream between server domains**
- **STARTTLS, certificates for server domains**
- **Request permission to send for delegated domains**
- **Verify authorization to represent delegated domains**
- **Grant permission to send for delegated domains**
Status

• The current document is incomplete …
  – Needs Security Considerations
  – Needs IANA Considerations
  – Needs Operational Considerations
• … but we think the protocol spec is pretty much there
• Is this the right path?
  – Implementability?
  – Backward Compatibility?