XMPP DNA Options

Richard Barnes

July 25, 2011

Overview of the DNA problem

- XMPP outsourcing providers don't want to have to hold certificates with their clients' domain names in them.
  - Risk of key compromise, hijacking other services, masquerading, etc.
- The current XMPP server-to-server connection model requires $2N_1N_2$ connections between providers, which doesn't scale.
  - Need a way to multiplex many domain pairs onto a single connection.

Outline of draft-ietf-xmpp-dna-01

- Instead of CA signing a cert, domain holder signs SRV
- Use dialback (XEP-0220) plus DNSSEC checks to support secure multiplexing

Is there a problem here?

- Ekr: Most certificate risks are mitigated if the certs the outsourcing provider can only be used for XMPP
  - No `CommonName` or `dNSName`
  - Only `XmppAddr` or `sRVName` (including `_xmpp-server._tcp.`)
- Dialback already supports multiplexing, just need to fold in security

Solution outline

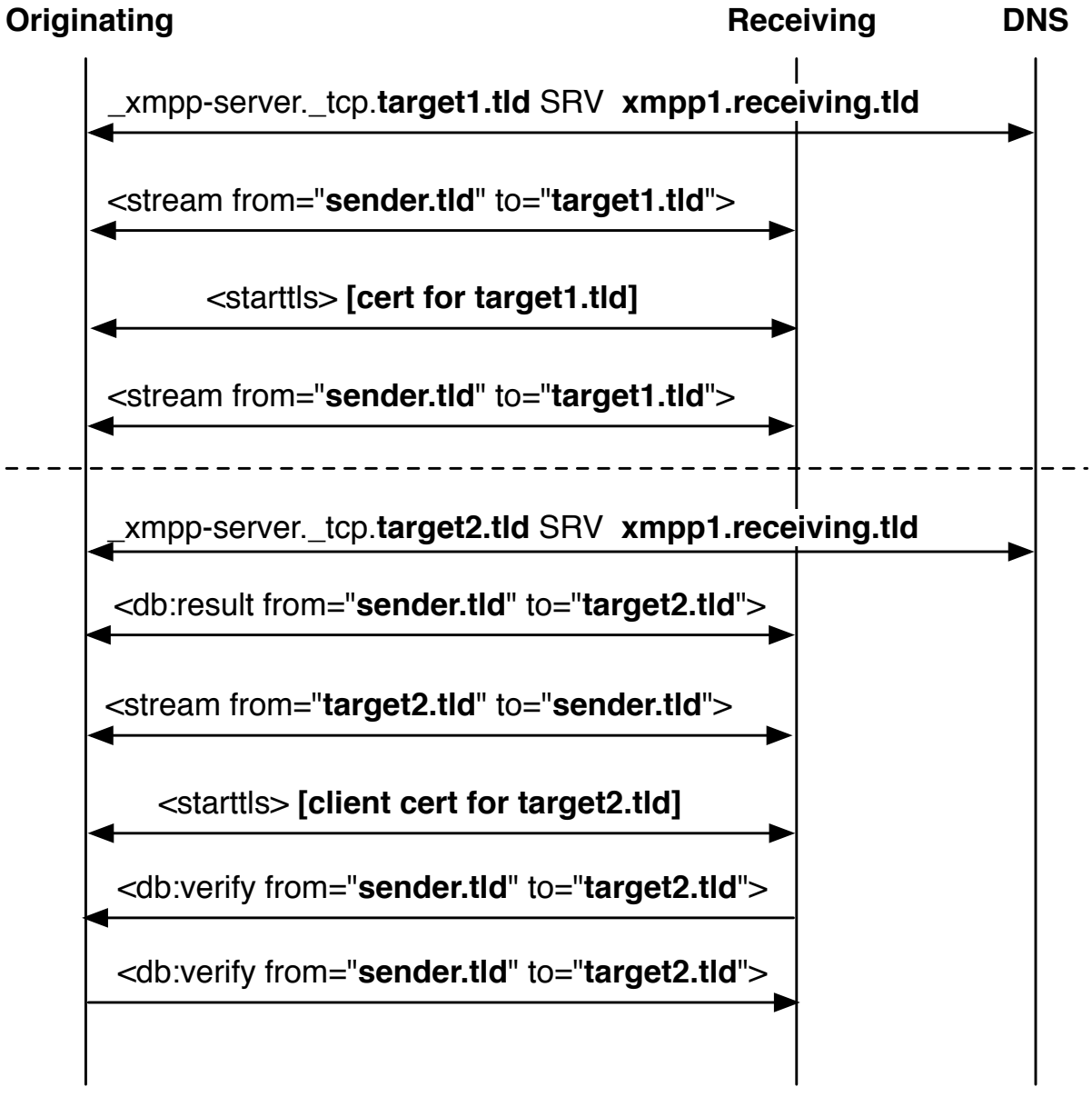
sender — originating — receiving — target1, target2

On first connect...

- SRV: target1.tld → xmpp1.receiving.tld
- Start a stream from sender.tld to target1.tld
- STARTTLS, server presents cert for target1.tld

On subsequent connect...

- SRV: target2.tld → xmpp1.receiving.tld
- `<db:result from='sender.tld' to='target2.tld'>`
- `<db:verify from='sender.tld' to='target2.tld'>`
- STARTTLS, client and server present certs


Originating
Receiving
DNS
_xmpp-server._tcp.target1.tld SRV xmpp1.receiving.tld
<stream from="sender.tld" to="target1.tld">
<starttls> [cert for target1.tld]
<stream from="sender.tld" to="target1.tld">
_xmpp-server._tcp.target2.tld SRV xmpp1.receiving.tld
<db:result from="sender.tld" to="target2.tld">
<stream from="target2.tld" to="sender.tld">
<starttls> [client cert for target2.tld]
<db:verify from="sender.tld" to="target2.tld">
<db:verify from="sender.tld" to="target2.tld">

Trade-offs

- Issuance: Issuing certs vs. signing zones
- Validation: PKIX validation vs. validating DNSSEC
- Revocation: PKIX revocation (OCSP, CRLs) vs. DNSSEC expiry
- Muxing: TLS latency vs. DNSSEC latency

What to do?

- Do we still need a document?
- PKIX-based or DNSSEC-based or both?
- Overview of the whole connection process?
- What else?