DANE + XMPP

(draft-miller-xmpp-dnssec-prooftype-02)

Matt Miller & Peter Saint-Andre

DANE WG

IETF 84, Vancouver

Two Problems

- First: Am I connecting to the right server? This is a matter of *secure delegation*.
- Second: Is the server who it claims to be? This is a matter of *identity verification*.
- In essence: Is it legitimate to associate a given domain name with this XML stream?

2

Delegation

- In XMPP, for discovery we use SRV records: *_xmpp-server._tcp.im.example.com 5269 hosting.example.net*
- But for identity verification we check the source domain (e.g., im.example.com), not the delegated domain (e.g., hosting.example.net)
- This is OK for standalone servers, but it's a big problem for virtual hosting environments

3

DNSSEC Helps...

- Request *_xmpp._tcp.im.example.com*
- Get *5269 hosting.example.net*
- If signed, can trust the delegation (if not, fallback to normal XMPP methods)
- Then check cert for hosting.example.net instead of im.example.com

4

Identity Verification

- What is the verification material? (Certificate, key, token, etc.)
- What are the matching rules? (e.g., RFC 6125)
- Where do you get the material? (PKI, DNS, etc.)
- Do you need secure DNS to trust the material?

5

Prooftypes

- The entity asserting its identity needs to *prove* the association using a recognized "prooftype"...
  - PKI (RFC 6120 + RFC 6125)
  - Dialback keys (RFC 3920 / XEP-0220)
  - DANE (draft-miller-xmpp-dnssec-prooftype)
  - "POSH" (draft-miller-xmpp-posh-prooftype)

6

DANE Prooftype

- Here, we care about the DANE prooftype...
  - Verification material: PKIX certificate
  - Matching rules: SubjectPublicKeyInfo or hash
  - Source: obtained from DNS
  - Secure DNS: necessary

7

Virtual Hosting

- Standard PKI prooftype (RFC 6120 + RFC 6125) doesn't work for virtual hosting environments
- DNSSEC for secure delegation plus DANE for identity verification solves the problem neatly and is the preferred long-term solution
- For service providers who can't deploy it right now, fallback is draft-miller-xmpp-posh-prooftype

8