Domain Name Associations

Matt Miller & Peter Saint-Andre
XMPP 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?

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

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

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?

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)

PKI Prooftype

- Verification material: PKIX certificate
- Matching rules: RFC 6125
- Source: PKI / trusted roots
- Secure DNS: nice but not necessary

Dialback Prooftype

- Verification material: token
- Matching rules: depends on implementation, but typically byte-for-byte comparison
- Source: sent over XMPP itself
- Secure DNS: needed in order to really trust the information (otherwise, weak verification)

DANE Prooftype

- Verification material: PKIX certificate
- Matching rules: SubjectPublicKeyInfo or hash
- Source: obtained from DNS
- Secure DNS: necessary

POSH Prooftype

- Verification material: PKIX certificate
- Matching rules: RFC 6125
- Source: obtained via HTTPS from well-known URI (https://im.example.com/_xmpp-client._tcp.cer)
- Secure DNS: nice but not necessary

Standalone Servers

- Use PKI as you do now
- Use DANE with secure DNS
- Use Dialback Keys, preferably with secure DNS
- POSH not needed, but OK

Virtual Hosts

- PKI is not a realistic option, so...
- Use DANE with secure DNS (preferred in the long term)
- Use POSH (not as elegant as DANE, but immediately deployable)
- Use Dialback Keys, preferably with secure DNS

Next Steps

- Get feedback on DNA framework from XMPP community
- Get feedback on DANE and POSH from security and application communities
- Experiment with implementations