Expecting Larger Records When TLSA Is Deployed

Paul Hoffman, VPN Consortium
OARC 2011 Spring Workshop
Overview

• What is DANE/TLSA
• What a TLSA request and resource record will probably look like
• Expectations for timing and amounts
DANE WG in the IETF

• Problem: TLS certificates currently need to be rooted by one of the hundreds of “trusted” CAs
• It would be good to be able to put the trust of “this cert is associated with this domain name” in the DNS itself
• Solution: let the DNS publish the certificate associations (RRtype is currently called TLSA)
• Requirement: DNSSEC
Hasn’t this already been done?

• Not for TLS
  – SSH has SSHFP (RRtype 44, RFC 4255)
  – IPsec has IPSECKEY (RRtype 45, RFC 4025)
  – SSHFP and IPSECKEY are barely used in practice

• However, there seems to be a lot of interest in DANE for TLS
Likely request format

- `_443._tcp.www.example.com IN TLSA`
- `_25._tcp.mail.example.com IN TLSA`
- Also can expect `_udp` for DTLS
- Some requests can get multiple responses
  - When first rolling out, if the mandatory-to-implement requirements are not clear
  - Some large TLS sites have multiple certs (but usually only one CA)
  - We really don’t know
Likely resource record format

- Certificate type (1 octet), reference type (1 octet), data (lots of octets)
- Certificate type is an end-entity certificate or a CA certificate
- Reference type is 0 for “unhashed”, with other values for the type of hash
Response length

- If hashes are used, the record length will be <100 octets
- If hashes are not used, the records will be much longer
  - Cert type of RSA1024, signed with SHA1: ~600 octets
  - Cert type of RSA2048, signed with SHA256: ~720 octets
Operational issues

• It is not at all clear whether people will prefer to use unhashed or hashed, but that has a fairly large operational impact
• For end-entity certificates, hashed should be just fine
• For CA certificates, hashed only makes sense for limiting the CA that can issue certs, so most use of TLSA for CA certs will be unhashed
What’s next

- More work to be done in the DANE WG
- Hopefully will have this finished by this summer (but you know the IETF)
- Already have browser implementers who are coding for this
- But what do we do for assuring the data is covered by DNSSEC?
- DANE WG might add a similar record for S/MIME after TLSA is done