TLSA status
IETF 80, Prague, March 2011

Paul Hoffman
Jakob Schlyter

v01

Overview

- Status of draft-ietf-dane-protocol
- Issues that have been discussed and dealt with
- Some known open issues
- Next steps
- Note: only a small amount of the interesting semantics of the protocol is covered in this presentation

Status: draft-ietf-dane-protocol-06

- Lots of discussion so far, and more is expected
- Some parts seem pretty stable
- Open issues seem to come in batches

What it looks like today

- Query: _portnum._prottype.hostname
- Response: Cert-type Hash-type Binary-blob
  - Cert-type: 1 for end entity, 2 for CA
  - Hash-type: 0 for full certificate, 1 for SHA-256, 2 for SHA-512
- May get more than one response to a query

Types of certificates in DANE

- Cert type 1 is for identifying end entities directly
  - Main goal is self-issued certs, but can also be used for ones issued by CAs not expected to be in a trust anchor store
- Cert type 2 is for specifying a particular CA to chain to
  - Main goal is CAs that are not expected to be in a trust anchor store

Certificate associations

- Associates the certificate (or hash of certificate) gotten securely from the DNS with the certificate that TLS servers must give
- End entity certs are matched exactly, CA certs are used as trust anchors
- Basic philosophy: if you can trust DNSSEC for the address you are using, you can trust it for the the certificate as well

Issues discussed and dealt with (1)

- What protocols this draft applies to #5, #17
  - TLS and DTLS over any application protocol, but not other security protocols
- Protocol specifics (format of queries and responses) #1, #3, #4, #15, #19, #20
  - See previous slide and sections 2.1 and 2.2 of the draft

Issues discussed and dealt with (2)

- Mandatory-to-implement formats and algorithms #11, #21
  - Section 4 of the draft
    - Cert-type 1 and 2
    - Hash-type 0 and 1 (none and SHA-256) are MUST, 2 (SHA-512) is SHOULD
  - Both types are extensible in an IANA registry
- Bare public keys, OpenPGP certs #14, #16
  - Not until they are standards-track for TLS

Still-open issues (1)

- How are the contents of end entity certificates to be looked at by clients? #2, #9, #13, #18
  - See next presentation
- Attacks (MITM, compromised intermediate CA, ...) #6, #10
  - Still need to work on these, maybe as Security Considerations

Still-open issues (2)

- No DNSSEC protection for last hops #8
- More complete description of error conditions #7
- Crypto questions (saying the strongest hash algorithm used, ...) #22
- Combine TLSA responses with other RRs #12
- DANE exclusivity for an entire domain #23

Next steps

- Deal with the still-open issues, particularly those from the next presentation
- Cycle the draft at least a few more times
- Get more feedback from other parties who care about DNSSEC, TLS, and so on