DANE Vocabulary

Ólafur Guðmundsson

ogud@ogud.com

IETF-87 Aug 2013

Goals

- Extract the principles in defining DANE extension to an protocol.
- Create common vocabulary to simplify specification

Service definition names

- ***Service Specification Records***
  - where is the service specified in DNS ?
    - Name and RR Type
      - SRV, NAPTR, A/AAAA, other ?
- ***Service Authentication Record***
  - Location/name and type
- ***Service Address Records***
  - Location/name

DNS

- ***DNS Navigation***
  - DNS control plane records used to get to the names of interest
    - Tree: NS
    - Direction change: CNAME, DNAME
- ***DNS Integrity***:
  - DNS records used by DNSSEC validators to verify correctness
    - Existence: DNSKEY, RRSIG and DS
    - Non-existence: NSEC/NSEC3

DNS Complications

- If the DNS navigation includes CNAME or DNAME traversal
  - bar.example.de xNAME foo.example.is
    - Both bar.example.de and foo.example.is MUST be validated by DNSSEC or DNS Integrity does not apply.
    - May affect name presented to server and acceptable CERT's
- NAPTR: an application level redirection
  - should be treated either
    - like xNAME if it requires additional lookup to e.g. SRV lookup
    - Or NAPTR + SRV combined is Service Definition

What needs DNS Integrity?

- DNS Navigation Records
- Service Specification Records
- Service Authentication Records

Server address records SHOULD NOT require DNS Integrity as the presence of Service Authentication SHOULD be sufficient??
Note: If Authentication Records are stored at or below Address Records the Address records are covered by DNS Integrity

Example: TLS

- Service Specification:
  - <name> A or AAAA
- Service Authentication:
  - _443._tcp.<name> TLSA [RFC6698]
- Service Address:
  - Same as Service Specification

Example: SSH

- Service Specification:
  - <name> A or AAAA
- Service Authentication:
  - <name> SSHFP [RFC4255]
- Service Address:
  - Same as Service Specification

Example: SMTP

- Service Specification: (in preference order)
  - <name> MX <preference> <target>
  - <name> A or AAAA
    - In this case <name> == <target>
- Service Authentication:
  - _25._tcp.<target> TLSA
- Service Address:
  - <target> A or AAAA

Example: IMAP

- Service Specification:
  - _imap._tcp.<name> SRV <a> <b> <port> <target>
- Service Authentication:
  - _<port>._tcp.<target> TLSA
- Service Address:
  - <target> A or AAAA

What's next?

- Is this useful?

- Do I need guidelines on definition of alternate Authentication types ?
  - CERT, Finger print, raw key, other
- Better understanding and description of NAPTR + SRV service Specification.