draft-ietf-dane-ops(-05)

Wes Hardaker
Viktor Dukhovni

Overview

- Who has read -05?
- Change in purpose
- Changes in Text

BCP → Standards Track

- Discussed at IETF89
  - Many WG decisions needed to be normative
  - E.G. type DANE-EE(3) ignores CN/SAN checks
- New title:
  - "**Updates to** and Operational Guidance for the DANE Protocol"
- Goal timeline
  - Get this soon
  - DANEbis eventually

BCP → Standards Track

- Update vs Guidance?
  - Confusion potential in the text
- Solution:
  - Section 12 is “Summary of Updates to RFC6698”
  - Please review!

Updates To RFC6698 List

- 3: Requires at least TLS 1.0
- 4.1: DANE-EE(3) ignores X.509 names and times
- 4.1: Raw public OOB keys discussed
- 4.2: DANE-TA TLS servers MUST send the TA
  - (within the handshake)
- 4.*: PKIX-EE/TA vs DANE-EE/TA
- 6: Use the validated CNAME for TLSA base
- 7: Rollover and parameter change reqs
- 8: Digest agility protocol

Important Components To Review

- Everything in the previous list!!

- CNAME following
  - Generally agreed upon and discussed before
- Algorithm Agility
  - No objections raised
  - Not sure of people that have read it
- Discuss “opportunistic”
  - Protocols that may or may not use TLS

Protocol Guidance: PKIX-* vs DANE-*

- For non-PKIX protocols
  - Treat PKIX-TA and PKIX-EE as unusable
  - There is no purpose in using them
  - They add impossible to implement bits

Protocol Guidance: PKIX-* vs DANE-*

- For PKIX protocols
  - Understand the ramifications of using all 4 types
    - If someone can insert DNSSEC records, then an attacker can just insert a DANE-EE record to work around PKIX.
    - DANE-* types function trump PKIX verification.
      - (By design)
    - (everyone knows this already)
- 4.3 functionally says:
  - If using a PKIX protocol, require only PKIX-*

Protocol Guidance: PKIX-* vs DANE-*

Thus:

- PKIX-protocol?
  - Use only PKIX-TA and PKIX-EE
- Non-PKIX protocol?
  - Use only DANE-TA and DANE-EE
- Switching from one to the other?
  - Probably the only case to use both

Digest Agility

- When you need to change parameters
  - Section 7 should be followed
  - Functionally:
    - Client gets to pick their favorite algorithm
    - Server side doesn't know which clients support which
    - Server must publish all algorithms they deem ok
    - Client algorithm ordering SHOULD be configurable
    - Matching Type Full(0) neither trumps not
  - When rolling certificates:
    - MUST publish records for every parameter set used
    - Don't mix and match
    - If using 311 for cert1, you must publish 311 for cert2

Questions?

Referral and CNAME Processing and TLSA Base Domain Preferences