DANE Deployment Observations
draft-york-dane-deployment-observations

Dan York

DANE WG, IETF 91

November 12, 2014

DNSSEC

DANE

Motivation

- If you want…

- you need…

DANE Success Stories

- SMTP
  - 330+ SMTP servers with TLSA records
  - http://www.tlsa.info/
- XMPP (Jabber)
  - 229 servers
  - client-to-server & server-to-server
  - https://xmpp.net/reports.php#dnssecdane
- Advertisements!

Fundamental Question

- As we are seeing active DANE deployment and usage, are we learning anything about DANE deployment challenges that can be addressed within the IETF?

Keeping in mind…

1. There are actions the IETF can take within the standards development process.

2. There are actions **OUTSIDE** the IETF that need to be taken within the operator, hosting, registrar, registry and other communities.

Potential Outcomes Today

1. Nothing for DANE WG or any other WG to do (beyond finish existing drafts). All required actions are external.

2. Nothing for DANE WG to do but actions for other WGs (ex. DNSOP), plus external actions.

3. Actions for DANE WG and potentially other WGs, plus external actions.

Observations in -00 draft

- Lack of awareness of DANE
- Perception that DANE is only for self-signed certificates
  - "why do I need it when I have my EV-SSL cert?"
- Challenges creating TLSA records
- **Inability to enter TLSA records at DNS hosting operators**
- Availability of developer libraries
- Performance concerns
  - multiple round trips
  - DDoS amplification attacks
- Cryptographic concerns

Additional Observations

- Stéphane Bortzmeyer:
  - Distrust of domain name industry by some people
  - Lack of TLSA monitoring solutions
- Viktor Dukhovni
  - Operational issues:
    - Forgetting to update TLSA RRs when keys are rotating.
    - Forgetting to updates TLSA RRs when a new certificate is issued.
    - Getting the usage or selector wrong.
    - Domains using elliptic curve DNSKEY RRs not yet supported by validating resolvers (and so they appear unsigned)

Additional Observations

- Michael Ströder
  - Lack of DNSSEC support is major blocker.
  - Concerns about DNSSEC auto-signing
  - Security of registry web interfaces
  - Doesn't like inventing a bunch of DNS RR types for different purposes

Keeping in mind…

1. There are actions the IETF can take within the standards development process.

2. There are actions **OUTSIDE** the IETF that need to be taken within the operator, hosting, registrar, registry and other communities.

Potential Actions

- Most challenges seem to be in operational area or awareness
- Actions DANE WG can take?
  - Updates to draft-ietf-dane-ops?
  - Guidance around minimizing new RR types?
    - i.e. so that more don't need to be added to web interfaces
  - Performance guidance? (or is this DNSOP? or external?)
  - Cryptographic concerns?

Questions for Discussion

- What roadblocks are people running into with implementing DANE? Are there lessons we can feed back into our process of developing DANE-related standards?
- Are there more “Using DANE with <foo>” types of documents that we can or should create? (And who is willing to do so?)
- Are there some good examples/case studies of DANE implementations that we could perhaps capture as informational RFCs?
- Are there places where it would be helpful if there were reference implementations of DANE support? For example, DANE for email got a boost when support was added to postfix. Are there other commonly-used open source projects where the addition of DANE support would help move deployment along?
- Are there test tools that need to be developed? Or existing ones that need to be better promoted? Are there interop tests we can arrange?

Thank You!