Whither DANE?

Shumon Huque

May 13th 2019

Lightning Talk

DNS-OARC 30 Workshop; Bangkok, Thailand

OARC30 discussions …

- DANE has come up several times in presentations, mic comments, and hallway discussions during this OARC workshop.
  - Bill Woodcock's talk on DNS attacks
  - SIDN incentives program
  - Also mentions from Olafur Gudmundsson, Brian Dickson, and others ..
- But is it really going to happen?

What is DANE

- The “Killer App” for DNSSEC?
- Use signed DNS records to authenticate public keys & X.509 Certificates.

```
;; QUESTION SECTION:
;_443._tcp.freebsd.org.          IN      TLSA

;; ANSWER SECTION:
_443._tcp.freebsd.org.  3600    IN      TLSA    3 1 1
31EF2A4D6E285CC29A636C5171F7DA0AC69CC44CEBAF5CD039DA8CC8 1187482A

_443._tcp.freebsd.org.  3600    IN      RRSIG   TLSA 8 4 3600 20190527013359 20190512132750 17338
freebsd.org. h6BXLidwFymOeyLyjWDfzHbsPZ5Wu7gN2LECY17Gcts4k6/rkGZdDLGu
lEOb2LXDsI3ge/NZhFsy5nXvmFDr3BZoExAH2dRotIdELT280JjrMg0J
XTJeO/izwnUER+du3k0C1r+oou81DUpfX+SFnQKOzisaXe/tKnv2NJx7
Czpz/RQ5StsjAzTBOzgkyceCNAkudXAcRTCz9YxzexJIcE0AGkXUOGEB
3e0p3Hgv6X6Y6Uy+n7H7RsKAU3R40tJ3AGi5RNvK7CMxpO2qQJS62mUP
8Sya/kk/n4gw4PtyNwRBCnM5wA0DH1DQrE/qOOA6jj8zIEC422nAvgOX pEI9kw==
```

Timeline

- RFC 6698: DANE RFC; August 2012
- RFC 7671: DANE Updates & Operational Guidance; October 2015
- RFC 7672: DANE TLS for SMTP Transport Security; October 2015
- RFC 7673: DANE for SRV; October 2015

- DANE for Web? → TLS DNSSEC Chain Extension (Unfinished)

DANE for SMTP Transport Security

- The one area to date, where DANE has had success.
- Viktor Dukhovni has been a tremendous driving force in both the protocol work, implementations, and deployment in the field.
- Updated deployment statistics from April 2019
  - https://mail.sys4.de/pipermail/dane-users/2019-May/000521.html
  - 1,122,806 domains with validatable DANE authenticated MX records

TLS DNSSEC Chain Extension

- Delivering DANE TLSA record and the entire chain of DNSSEC records needed to authenticate it in-band, so that client applications (i.e. their stub resolvers) don't have to perform these DNS queries.

- Rationale:
  - Middleboxes (the bane of the Internet!) – *WTF is a TLSA record?*
  - Reduced latency.
  - No requirement to run a validating stub (which aren't common), or to require a channel protected connection to their validating recursive servers (also not common).

- Only way web browsers were willing to implement DANE.

TLS DNSSEC Chain Extension

- Background: Adam Langley & Google
  - Stapling DANE chains in certificates
  - Aggressive opposition from the DNSSEC crowd
  - An implementation was done, later pulled; went nowhere in IETF

- 2nd try: TLS DNSSEC Chain extension
  - https://tools.ietf.org/html/draft-ietf-tls-dnssec-chain-extension-07
  - M. Shore, R. Barnes, S. Huque, W. Toorop
  - Proposed & Adopted by IETF TLS WG (the lion's den!)
  - An implementation was funded and planned for Mozilla
  - Was initially approved as a standards track document (March 2018)
  - But then a huge fight broke out and it was ultimately abandoned.

What was the fight about?

- Downgrade protection against WebPKI fraudulently issued cert attack
  - Challenging to do in an incremental deployment fashion, because the chain extension can be stripped
  - We can use WebPKI defenses to address this, like CT
- Proposal was to do pinning of DANE record existence.
  - Browser folks hate pinning (bad experiences with HPKP etc).
  - Furthermore they don't agree with the need for downgrade protection.
- Result:
  - Uncomprising sides; deadlock; hundreds of emails (DoS attack)
  - Draft abandoned.
  - **DANE is effectively dead in browsers for the foreseeable future.**
    - IETF103, major browser vendors declared that they have no plans to implement DANE ☹

My personal view

- DNSSEC/DANE advocacy requires diplomacy & compromises
- Pushing the most secure solution isn't always going to win, particularly if your target community already harbors significant antagonism to DNSSEC.
- I predicted this fight would end up in the draft dying and browsers abandoning it. That's what happened.
- Recognize legitimate arguments of DNSSEC critics:
  - DNSSEC landscape is littered with 1024-bit RSA keys for one
  - Browser folks don't see DANE as inherently superior to WebPKI
  - They also measure adoption of new features before more integration
  - Accommodate them, take baby steps, strengthen the protocol later

What's next

- Informational draft planned -> IETF independent stream
- Probably 1st use case: inband DANE authn for DNS over TLS
- Are there other use cases?
  - DANE for IMAP/POP/SMTP Submission?

- Maybe web browsers will reverse course in 5 years ..