TLS DNSSEC Chain Extension

draft-ietf-tls-dnssec-chain-extension

(remaining issues)

Presenting: Shumon Huque & Willem Toorop
(Co-authors: Melinda Shore & Richard Barnes)

March 21st 2018

TLS Working Group, IETF101 Meeting, London, U.K.

IESG evaluation: DISCUSS & COMMENTs

- Almost all (we believe) have been resolved on list.
- Write-up in new draft (-07) almost done.

- DISCUSS issues (Alexey):
  - “DNAME chains SHOULD omit unsigned CNAME records” – what are the implications if they aren’t omitted?
  - TLS 1.3 needs to be a normative reference.

- DISCUSS issues (Eric):
  - Chain data format insufficiently specified. Elaborate.
  - “The domain name” associated with an IP address – not unambiguous.
  - Discussion of cases: DANE validates but PKIX doesn’t and vice versa.

TLS 1.2 vs 1.3 keyword discrepancy

3.1. Protocol, TLS 1.2

[…]

Servers receiving a "dnssec_chain" extension in the ClientHello and which are capable of being authenticated via DANE **MAY** return a serialized authentication chain ..

?

3.2. Protocol, TLS 1.3

[…]

Servers receiving a "dnssec_chain" extension in the ClientHello, and which are capable of being authenticated via DANE, **SHOULD** return a serialized authentication ..

New Issue: 1 of 2

- **Data format in the chain extension**:
  - Raised by Paul Wouters.
  - Format is suggested to be: complete DNS message rather than sequence of wire format DNS Resource Record sets.
  - **Resolved:** Paul has been persuaded that full message isn't needed.

New Issue: 2 of 2

- **Vulnerability to downgrade to PKIX-only attacks**:
  - Raised by Viktor Dukhovni.
  - This issue was known by the authors, and documented in the draft with possible mitigations.
  - Fundamentally tied to the fact that the protocol does not provide authenticated denial of existence.

  - Viktor suggests that we need a more robust defense (he will elaborate later)

PKIX downgrade attack

- TLS server has valid DANE TLSA record.
- Attacker has fraudulently obtained valid PKIX credentials.
- Attacker manages to get TLS client to connect to it, ignores the dnssec_chain extension, and offers PKIX authentication.

- (Note: this attack applies only to incremental deployment of DANE in an existing PKIX environment. Not relevant to green field DANE applications, or applications that require explicit client configuration.)

Preventing this attack

- Was not an original design goal of this draft.
- Early debate about semantics of TLSA record with web people.
  - Is it a policy signal that DANE must be used? Or is DANE use always a local policy decision by the TLS client?
- So the extension provides a mechanism to enable DANE authentication, but has no facility to mandate it.

- Client-side behavior or configuration can mandate DANE:
  - Trust on First Contact, then pin knowledge of DANE existence for some period of time.
  - Whitelist known DANE servers.

Other possible mitigations

- Use PKIX defenses to protect against PKIX attacks, e.g.
- Certificate Transparency Logs

- Checking CT is probably necessary anyway, in an incremental deployment environment:
  - TLS server supports both DANE and traditional PKIX
  - Even if TLS server only supports DANE, it may want to make sure that attackers cannot masquerade the service to DANE unaware clients.

In-protocol commitment to DANE

Viktor Dukhovni:

Perhaps this draft should go back to the working group, to consider a new protocol element, by which the server commits to support the extension for a time that is substantially longer than the underlying DNS TTLs. During this time (suggested to be weeks or months, when in production after initial testing), the server MUST support the extension and respond with EITHER a valid TLSA RRset chain, or with a valid denial of existence.

(Note: this is still vulnerable to attack on first contact.)

Viktor suggests that no-one will deploy this extension without a robust in-protocol defense against PKIX downgrade attacks ..