draft-ietf-tls-dnssec-chain-extension

the past and the future
Sean Turner (WG Chair Hat On)
Questions

just to level set

Who is reading their email?

Who knows what DANE is? DNNSEC?

Who has read the draft?

Who has followed the list discussions?

Who read this presentation?

Who is planning to implement?

Who is planning to deploy?
Agreed Use Case!

Timeline

20150630 Initial Posts: thread_1 & thread_2 (20)
Primarily aimed at making DANE practical for HTTPS, where last-mile considerations on the client end are a significant part of the adoption barrier.

Think of it as “DANE stapling”.
20150630  Initial Posts: thread_1 & thread_2 (20)
20150722  IETF 93 Presentation / Meetecho @ 1:37
20160407  IETF 95 Presentation / Meetecho @ 1:55
20160425  WG Call for Adoption (10)
20160604  -00 Version
20160707  -01 Version
20170111  -02 Version
20170117  IETF 97 Presentation / Meetecho @ 0:32
20170322  Comments on -02 (14)
20170327  -03 Version
20170328  IETF 98 Presentation / Meetecho @ 1:28
20170601  -04 Version
20170621  WGLC comments: thread_1 & thread_2 (29)
20171029  -05 WG Version
Timeline

20150630 Initial Posts: thread_1 & thread_2 (20)
20150722 IETF 93 Presentation / Meetecho @ 1:37
20160407 IETF 95 Presentation / Meetecho @ 1:55
20160425 WG Call for Adoption (10)
20160604 -00 Version
20160707 -01 Version
20170111 -02 Version
20170117 IETF 97 Presentation / Meetecho @ 0:32
20170322 Comments on -02 (14)
20170327 -03 Version
20170328 IETF 98 Presentation / Meetecho @ 1:28
20170601 -04 Version
20170621 WGLC comments: thread_1 & thread_2 (29)
20171029 -05 WG Version
20180123 -06 WG Version / Publication Requested / IETF LC (0)
“Downgrade” re-identified as an issue.

But, now it is a SHOWSTOPPER!

Timeline

20150630 Initial Posts: thread_1 & thread_2 (20)
20150722 IETF 93 Presentation / Meetecho @ 1:37
20160407 IETF 95 Presentation / Meetecho @ 1:55
20160425 WG Call for Adoption (10)
20160604 -00 Version
20160707 -01 Version
20170111 -02 Version
20170117 IETF 97 Presentation / Meetecho @ 0:32
20170322 Comments on -02 (14)
20170327 -03 Version
20170328 IETF 98 Presentation / Meetecho @ 1:28
20170601 -04 Version
20170621 WGLC comments: thread_1 & thread_2 (29)
20171029 -05 WG Version
20180123 -06 WG Version / Publication Requested / IETF LC (0)
20180207 GENART (3) / IESG: Adam (5 msgs), Mirja (15), Eric (52), Alexey (4), Ben (2)
“Downgrade” Attack

tl;dr: DANE needs downgrade resistance against PKIX attacks.

Absent whitelists, a client misdirected to a server that has fraudulently acquired a public CA-issued certificate for the real server's name, could be induced to establish a PKIX verified connection to the rogue server that precluded DANE authentication.
Approved after resolving final DISCUSS point.
But, was the issued raised during the DISCUSS addressed properly?
Not Surprising.
Consensus to publish as-is or address issues in WG?
Consensus Call

Do you support publication of the document as is, leaving these two issues to potentially be addressed in follow-up work?

Issues:

1. Recommendation of adding denial of existence proofs in the chain provided by the extension
2. Adding signaling to require the use of this extension for a period of time (Pinning with TTL)

If no then what should the WG work on:

A) Recommendation of adding denial of existence proofs in the chain provided by the extension
B) Adding signaling to require the use of this extension for a period of time (Pinning with TTL)
C) Both

(added later)

D) Remove pinning paragraph from draft.
Participated in the thread.
Answered the 1st question directly.
Answered the 2nd question.

(And, it wasn’t the same 10).
Split decision. But, the chairs determined there was consensus for A) and enough discussion to recommend that the AD return the draft to the WG.
But, we never told the authors to merge text related to DoE. (more on this later)
Message Count

- Viktor: Up to WGLC - 20, After - 60
- Shumon: Up to WGLC - 40, After - 20
- Nico: Up to WGLC - 10, After - 30
- Paul W: Up to WGLC - 15, After - 15
- Melinda: Up to WGLC - 10, After - 10
- ekr: Up to WGLC - 5, After - 5
- Richard: Up to WGLC - 15, After - 15
- Willem: Up to WGLC - 10, After - 10
- Ben: Up to WGLC - 5, After - 5
- Joe: Up to WGLC - 5, After - 5
- Kathleen: Up to WGLC - 5, After - 5
- ilari: Up to WGLC - 5, After - 5
- Tom H: Up to WGLC - 5, After - 5
- Jim R: Up to WGLC - 5, After - 5
- Sean: Up to WGLC - 5, After - 5
Text Proposals
(will come back to this)

20180321  IETF 101 Presentation / Meetecho @ 0:44 / -07 WG Version / Proposed text (2) / Approved
20180326  Offlist Appeal Threats
20180404  Consensus Call (126)
20180425  Proposed text for draft (29)
20180427  Precluding Bilateral opt-in for Downgrade Protection (13)
20180428  Draft updates (13)
20180516  Consensus Speak Up (24)
20180604  Security Considerations (25)
20180716  IETF 102 Presentation / Meetech @ 0:30 / Meetecho @ 0:00 / Side Meeting
20180718  Response to concerns raised @ IETF 102 (10)
20180809  Draft returns to WG
20180821  Offlist proposals (22)
20180912  Proposed text for Interim (12)
### Timeline

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>20180321</td>
<td>IETF 101 Presentation / Meetecho @ 0:44 / -07 WG Version / Proposed text (2) / Approved</td>
</tr>
<tr>
<td>20180326</td>
<td>Offlist Appeal Threats</td>
</tr>
<tr>
<td>20180404</td>
<td>Consensus Call (126)</td>
</tr>
<tr>
<td>20180425</td>
<td>Proposed text for draft (29)</td>
</tr>
<tr>
<td>20180427</td>
<td>Precluding Bilateral opt-in for Downgrade Protection (13)</td>
</tr>
<tr>
<td>20180428</td>
<td>Draft updates (13)</td>
</tr>
<tr>
<td>20180516</td>
<td>Consensus Speak Up (24)</td>
</tr>
<tr>
<td>20180604</td>
<td>Security Considerations (25)</td>
</tr>
<tr>
<td>20180716</td>
<td>IETF 102 Presentation / Meetech @ 0:30 / Meetecho @ 0:00 / Side Meeting</td>
</tr>
<tr>
<td>20180718</td>
<td>Response to concerns raised @ IETF 102 (10)</td>
</tr>
<tr>
<td>20180809</td>
<td>Draft returns to WG</td>
</tr>
<tr>
<td>20180821</td>
<td>Offlist proposals (22)</td>
</tr>
<tr>
<td>20180912</td>
<td>Proposed text for Interim (12)</td>
</tr>
<tr>
<td>20180914</td>
<td>Virtual Interim / Paul W’s Notes</td>
</tr>
<tr>
<td>20180925</td>
<td>Offlist arguing re: next steps (25) / re: pinning risks (79)</td>
</tr>
<tr>
<td>20181009</td>
<td>Notes and next steps (15)</td>
</tr>
</tbody>
</table>

---

!fun!/!great/!MIGA
Timeline

20150630  Initial Posts: thread_1 & thread_2 (20)
20150722  IETF 93 Presentation / Meetecho @ 1:37
20160407  IETF 95 Presentation / Meetecho @ 1:55
20160425  WG Call for Adoption (10)
20160604  -00 Version
20160707  -01 Version
20170111  -02 Version
20170117  IETF 97 Presentation / Meetecho @ 0:32
20170322  Comments on -02 (14)
20170327  -03 Version
20170328  IETF 98 Presentation / Meetecho @ 1:28
20170601  -04 Version
20170621  WGLC comments: thread_1 & thread_2 (29)
20171029  -05 WG Version
20180123  -06 WG Version / Publication Requested / IETF LC (0)
20180207  GENART (3) / IESG: Adam (5 msgs), Mirja (15), Eric (52), Alexey (4), Ben (2)

20180321  IETF 101 Presentation / Meetecho @ 0:44 / -07 WG Version / Proposed text (2) / Approved
20180326  Offlist Appeal Threats
20180404  Consensus Call (126)
20180425  Proposed text for draft (29)
20180427  Precluding Bilateral opt-in for Downgrade Protection (13)
20180428  Draft updates (13)
20180516  Consensus Speak Up (24)
20180604  Security Considerations (25)
20180716  IETF 102 Presentation / Meetecho @ 0:30 / Meetecho @ 0:00 / Side Meeting
20180718  Response to concerns raised @ IETF 102 (10)
20180809  Draft returns to WG
20180821  Offlist proposals (22)
20180912  Proposed text for Interim (12)
20180914  Virtual Interim / Paul W's Notes
20180925  Offlist arguing re: next steps (25) / re: pinning risks (79)
20181009  Notes and next steps (15)
20181107  IETF 103

You are here!
And now for some housekeeping
(aka CYA for the chairs)
**Consensus Call (during SecCon thread)**

1. Do you support the working group taking on future work on a pinning mechanism (based on the modifications or another approach)?

2. Do you support the reserved bytes in the revision for a future pinning mechanism?

3. Do you support the proof of denial of existence text in the revision?

4. Do you support the new and improved security considerations?
Participated in the thread.
1. Do you support the working group taking on future work on a pinning mechanism (based on the modifications or another approach)?

2. Do you support the reserved bytes in the revision for a future pinning mechanism?

3. Do you support the proof of denial of existence text in the revision?

4. Do you support the new and improved security considerations?
Direction
Direction for 24-part commit

Merge:

- Editorial commits
- DoE-related commits:*
  - Reconfirmed consensus to adopt DoE text.
  - Authors to identify which commits* are DoE related.
  - Merge text.
- Security Considerations related:*
  - Confirmed consensus to adopt updated Security Considerations.
  - Authors to identify which commits are Security Considerations related.
  - Merge text.

Publish new version.
Observation
So now what!?

We have been circling for a while.

Fewer participants.

So, we can:

a) Publish the consensus document, i.e., without pinning or reserved field.
b) Have it gracefully die because there is no consensus to add pinning or reserved bytes.
Agreed use case!

Downgrade re-identified as an issue. Now it is a shop stopper!