Strict Transport Security in DNS

Paul Hoffman, VPN Consortium

v. 1

Overview

- HSTS specifies “I always do HTTP over TLS” in HTTP headers
- There is discussion of “I always do Foo over TLS” in DNS
- Where do these things overlap? Where is the synergy?

HSTS

- draft-hodges-strict-transport-sec
- “a HTTP response header field is used to convey site policy to the UA”
- Effects:
  - All insecure ("http") connections to a HSTS Server are redirected by the HSTS Server to be secure connections ("https").
  - The UA terminates, without user recourse, any secure transport connection attempts upon any and all secure transport errors or warnings, including those caused by a site presenting self-signed certificates.
  - UAs transform insecure URI references to a HSTS Server into secure URI references before dereferencing them.

Strict transport security in the DNS

- Has been discussed for years
- Only (?) current draft is draft-hallambaker-esrv
- Could also be done as a single DNS resource record
- Probably should not be done as part of a KIDNS record because it could lead to silly states

High-level differences in the DNS-based proposals

- Applies to all application protocols, not just HTTP
- Can be seen by the client before the protocol is run the first time
- Is (hopefully) protected by a different type of security

Implications of running STS-in-DNS without security

- With STS-in-DNS not under DNSSEC, a MITM who can alter DNS queries can prevent the client from seeing the message
- This leads to the utility of having STS both in the DNS, which leads to the client getting to the right server, and in the protocol itself (in case the MITM can only alter HTTP, not the client’s DNS queries)

Synergies

- If both HSTS and STS-in-DNS are deployed, the client will probably get conflicting information about how long to believe the “must do TLS” assertion
- ...but that is irrelevant: they’ll pick the longer one, which is still valid
- There don’t appear to be any conflicts yet, but STS-in-DNS is much less mature than HSTS

Overlap of semantics

- The semantics associated with STS-in-DNS should be the same as HSTS; otherwise, the overlap will lead to confusion
- This will require coordination of drafts
- Have to evaluate if the HTTP semantics apply to other application protocols that run under TLS

More to be done

- Start listing all the protocols that use TLS
- Line up the semantics
- Choose how to put this in the DNS
- . . .