draft-ietf-dprive-dns-over-tls-01

IETF 94, Yokohama

November 2, 2015

Major Changes since IETF 93

- Since we last presented, major changes were:
  - STARTTLS contents entirely removed, based on the WG consensus
  - Draft name changed to dns-over-tls from start-tls-for-dns
  - Added strong references to RFC 7525 (BCP 195), Recommendations for Secure Use of TLS and DTLS
  - We succeeded in the early allocation request and we added port 853 to the IANA Considerations

Status

- Pre-WGLC issues all addressed
- A few WGLC issues:
  - Align language with final 5966bis text
  - Clarify the authentication profiles section
  - Publish profiles and authentication mechanisms draft separately
- Implementation has progressed further
  - Implementation updates on later slides
  - Very busy hackathon!

Draft Status

Align with 5966bis

- 5966bis has completed its WGLC
- Comment identified one section in this draft that isn't aligned
  - Fixed when the submissions window re-opens

Confusion on Authentication Profiles

- Section 4 states that two authentication profiles are specified, and others are possible
  - Opportunistic Privacy Profile (4.1)
  - Pre-Deployed Profile
- Question was asked what fields in cert are matched in Pre-Deployed
  - Pre-Deployed was intended to be certificate-level not field-level
  - Both need work, so we now suggest moving these to the separate profiles and authentication draft

Proposed Clarifications

- Explicitly state that an upcoming document will define further authentication profiles
  - Draft in development, will be submitted ASAP
- This draft will document Opportunistic and briefly cite the risk-benefit for it
- This draft will provide a brief sketch of authentication in the case where there is a two-way active relationship between the client and the server (e.g. enterprise)

Implementation Status

Current Implementation Status

- Unbound
  - supports port-based DNS-over-TLS since 1.4.14, configurable to port 853. Use 1.5.6 for strict TLS.
- ldns, drill, NSD patched to do TLS
  https://portal.sinodun.com/wiki/display/TDNS/DNS-over-TLS+patches
- digit (USC/ISI tool)
- getdns (client)
  - Active and ongoing development (next release within this week)
  - Now uses port 853
  - Implements API with ordered list of transports (TLS only, or possible fallback) and proof-of-concept authentication option

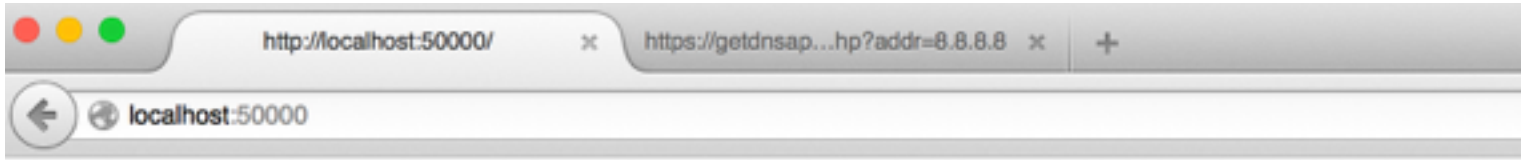
Proof of Concept in Development

- getdns implements Opportunistic Privacy Profile
- getdns has a PoC for authentication
  - Authentication Profile 1 (Out of Band)
  - An additional profile with hostname matching for CA certificates – experimentation, not ready for the draft
- Also exploring other privacy-related proposals

DNS Team Hackathon Projects

- DNS Privacy topics
  - getdnsapi extension (call debugging) implemented with changes so user learns transport/privacy results
  - edns0-client-subnet privacy election
  - edns0-padding option (client side is done)
  - Check TLS at Recursive - node.js application
- DNSSEC topics
  - DNSSEC roadblock avoidance - proposed new extension for getdnsapi
  - CDS/CDNSKEY -

  …



Check TLS at Recursive

Target Resolver: 185.49.141.38

Recursive's Hostname in Certificate:getdnsapi.net

Checking for:

1. Successful TCP connection

2. Successful TLS connection

3. Successful TLS Authentication

4. Opportunistic TLS with fallback to TCP available

Note: This webpage is created with node.js bindings of getdns, in the expressjs framework

Source code will be available at https://github.com/getdnsapi/checkresolvertls

✔✔✔ Result: Authentication Succeeds!

Discussion

Discussion Areas

- Does WG support the move of most profiles and authentication to a new draft?
- DNS-over-TLS draft to be published with pared-down guidance that will avoid “baking in” profiles at this stage
- DNS-over-TLS draft not dependent on separated out profiles and authentication draft.

WGLC will complete Nov 12

- Are there any last issues with the draft?
  - Not already covered in these slides
- Any questions on the implementations?
  - Draft includes an implementation section
- We plan to submit -02 ASAP

DNS Hackathon Team

- Dickinson, Sara
- Kahn Gillmor, Daniel
- Mankin, Allison
- Shore, Melinda
- Toorop, Willem
- Wicinski, Tim
- Včelák, Jan
- Cathrow, Andy
- Dickinson, John
- Huque, Shumon
- Miller, Matt
- Tomofumi Okubo
- Overeinder, Benno
- Seltzer, Wendy
- Visweswaran, Gowri