Phase 2 Requirements

DPRIVE Milestone – „unpublished document"

Alex Mayrhofer & Benno Overeinder, IETF 104, Prague

History

- DPRIVE Charter Work Item: ***"Develop requirements for adding confidentiality to DNS exchanges between recursive resolvers and authoritative servers"*** (unpublished document)

- IETF 103: DPRIVE WG session cancelled

- Creation of a Wiki document (now moved to https://github.com/DPRIVE/dprive-v2-ms-and-reqs/blob/master/dprive-v2-ms-and-reqs.md)

- First review at DPRIVE interim

- Updates since then

What's in the GitHub document?

- Existing / Previous Work
- Three "Requirement Perspectives"
  - User
  - Operator
  - Software Vendor
- Functional Breakdown
  - Privacy Protection Mechanism
  - Authentication
  - Performance and Efficiency
  - Detection of Availability
  - End User Policy Propagation

https://github.com/DPRIVE/dprive-v2-ms-and-reqs/blob/master/dprive-v2-ms-and-reqs.md

Current Status & Direction

- Currently more a description of Options / Areas to work on
- Rather than a "List of Requirements"

- How shall we proceed?
- Three "essential" questions
- Please review! Please comment!

Question 1: "Hard Requirements"?

- Document is currently a description of Options / functional Areas to work on

- Rather than a "List of Requirements"

Q: Shall we modify the document to list "hard" requirements? (eg. "MUST", "SHOULD")

If yes, what are these?

Question 2: "Are we set with DoT"?

- Document lists Transport Protocol as one of the dimensions in the Design Space

- DoT is baked, there are other options

Q: "Do we want to settle on DNS-over-TLS as the Transport Protocol of choice for Phase 2"?

If yes, do we need any modifications (besides a new "Profile")?

If no, what else do we use?

Question 3: "End User Signaling"?

- Currently, the privacy properties of the (multi-hop) "upstream" connections are opaque to the stub resolver / user

- Like in many other protocols where some form of "proxying" takes place (some with indications, eg. SMTP headers)

Q: "Do we want/need signaling to the Stub Resolver whether (all?) upstream communication was privacy enabled?"

(seems complicated..)

Discuss!

- Q1: "Hard Requirements"?
- Q2: "DoT, or something else"?
- Q3: "Stub Resolver signalling"?

- Qn: Other questions *not* touched upon?

Further Steps for the document?
  - gap analysis
  - relate activities and drafts with perspective and requirements (Venn diagram)