DNS Privacy/Encryption

DNSOP
IETF 89, London
March, 2014

DNSOP (DNSE II session)

Thank you for attending this second session. The main DNSOP agenda will still be addressed Friday morning. We moved this topic to Thursday night to accommodate a conflict and increase the opportunity for cross-area discussion.

Admin

This session is one hour long

- Agenda
- Note Well
- Blue Sheets

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

What is the Problem ?

- Overall Issue: Perpass considerations, applied to DNS
  - Like many current protocols, DNS leaks privacy-relevant data
  - Like many widely used protocols, DNS is hard to fix
- Summaries/assessment
  - problem statement
  - DNSE summary (including outcomes)
  - Overview of existing protocols
- Where from here?

DNSE summary

- Problem statement: DNS leaks privacy relevant data in a number of ways
  - in the query
  - on the wire
  - in servers at each step
- What to do about it?
  - applicability of TLS
  - various proposals
- Interest in doing further work seemed clear; ADs are looking to DNSOP to figure out next steps

Requirements/Tradeoffs (random sample of possible issues)

- UDP/TCP
- Middlebox Issues
- Small enough protocol changes to take only finite time
- Clarity on what we can’t do, e.g. prevent traffic analysis
- Which parts of the relationship/transaction to protect? From what threats? (priorities)
- Anycast support
- Long queries considered harmful

Solution Space

- Comparisons of solutions ala RFC 5479
  - Confidential DNS (draft-wijngaards-dnsop-confidentialdns)
  - CGA-TSIG (draft-rafiee-intarea-cga-tsig)
  - Start-TLS for DNS (draft-hzhwm-start-tls-for-dns)
  - Peter’s draft (draft-koch-perpass-dns-confidentiality)
  - Stephane's draft (draft-bortzmeyer-dnsop-privacy-sol)
- Which solutions apply to which aspects of the problem?

Next Steps

- Adopt/review problem statement
- Missing document on requirements/tradeoffs
  - who wants to write this?
- How to approach solutions?
  - How much complexity is tolerable? Can we do anything simple?
  - How much backwards compatibility is required?
- How much of the work can we do here?
  - (Charter Discussion)
- Call for shepherd for topic in the WG