EDNS Padding Policy

draft-ietf-dprive-padding-policy-01

Alex Mayrhofer – 2017-07-18 – IETF99 – Prague, CZ

Document Status & Changes

- Status
  - -00 expired in June (completely my fault)
  - -01 posted two weeks ago
- Changes
  - Recommended Strategy
  - Some editorial changes
- Feedback to -01
  - Add „Pad to maximum message size“ strategy (Hugo)
  - „Wording seems fine“ (Paul)
  - Packet counts is important, not size (Shane)
  - Private Feedback: Why not random padding? Prevent analysis on „block counts“?

Recommended Strategy
(credits Daniel K. Gillmor's – big thanks!)

5. Recommended Strategy

Based on empirical research performed by Daniel K. Gillmor [dkg-padding-ndss], EDNS Padding SHOULD be performed as follows:

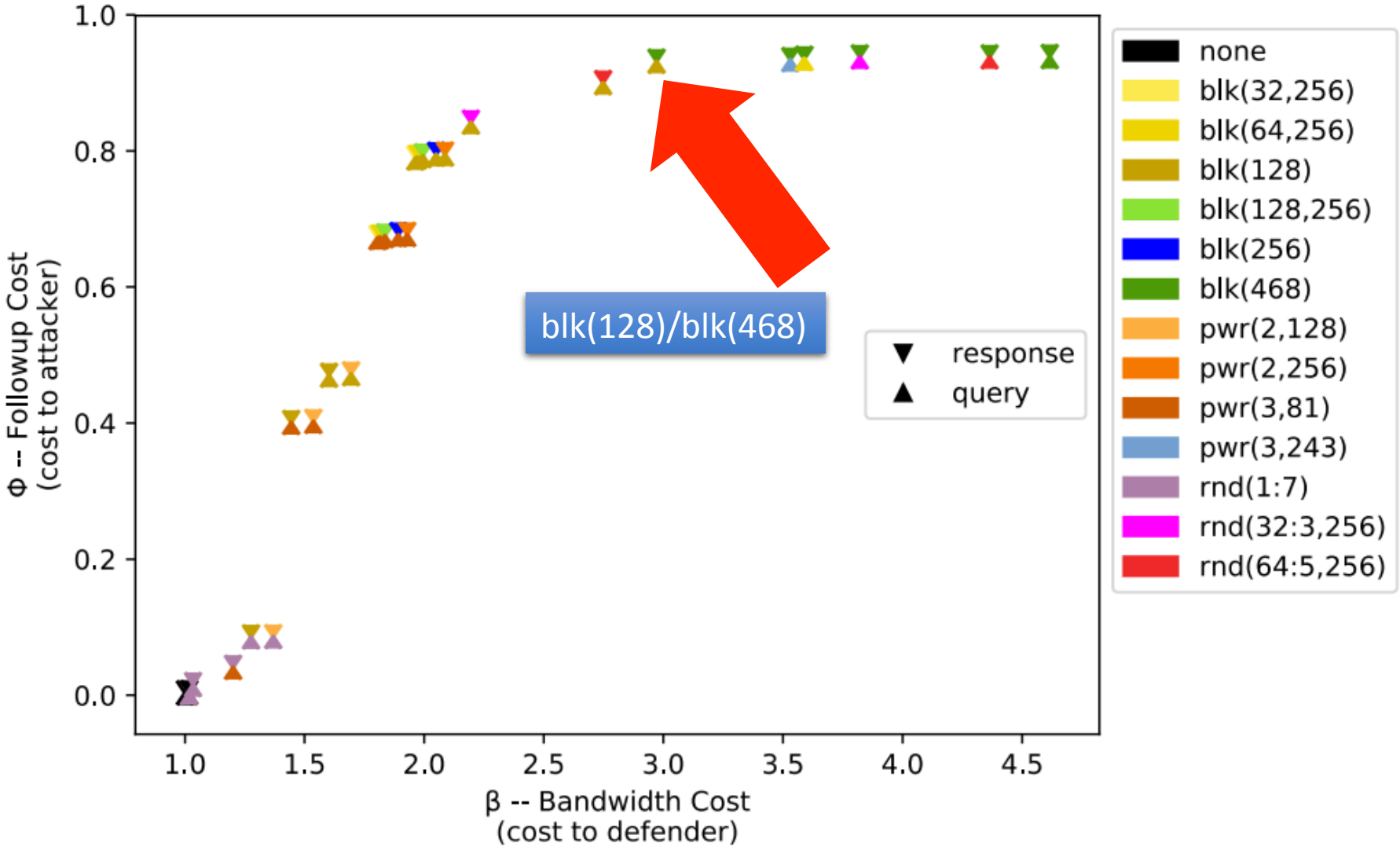
(1) Clients should pad **queries** to the closest **multiple of 128** octets.

(2) If a Server sees padding in a query, it should pad its **response** to a **multiple of 468** octects.

(3) TODO: recommend to not pad when query was unpadded?

https://dns.cmrg.net/ndss2017-dprive-empirical-DNS-traffic-size.pdf

Background Recommended Strategy



Next Steps / Questions

- Are we happy with the recommendation (128/468)?
  - More research? (Cost functions, „sweet spot“, other field data)
  - Document Status: „Experimental“ if we‘re unsure?

- Keep the description of strategies?

- As always: Reviewers, please!

- *And…. „Why 468“?*
  - We need text to explain this (if we go for that option)