The EDNS(0) „padding“ Option

Alexander Mayrhofer

July 24 2015, IETF 93, Prague

Motivation

- Disclaimer: I‘m a TLS noob!
- Size-based correlation of encrypted DNS messages
  - Affects DNS over TLS
  - As well as DNS over DTLS
- See Haya Shulman talk
  - Message size analysis „assists“ correlation
- Sidenote: Figures on distribution of DNS message sizes?b

Possible Solutions

- TLS WG: DK Gillmor proposing „padding“ option for TLS
- Hallway discussion yesterday noon
- Padding „closer“ to application is preferred
  - Easier to control from the DNS application
- „Bogus“ RR in the additional section (TXT?)
- EDNS0!

draft-mayrhofer-edns0-padding

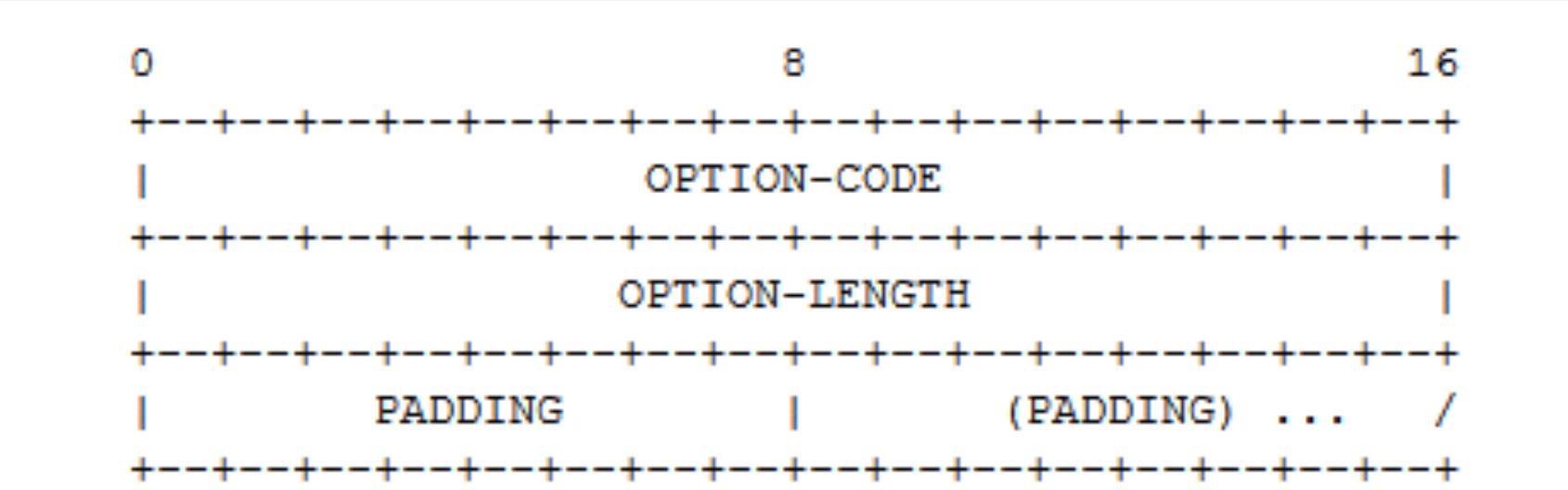

Figure 1

Next steps / discussion

- Is this useful?
- „Toolbox“ for both DNSoD and DNSoTLS
- Padding „contents“
  - 0x00? Compression „attack“?
- Actual padding sizes?
  - ~~Fixed length padding~~
  - Queries: „Classes“ of 96 / 192 / 384 bytes?
  - Random padding (1 < x < 32)?
  - Needs more work on stats
- dnsop or dprive?