ECS support detection and birthday attack hardening

Ralph Dolmans
ralph@nlnetlabs.nl
ECS birthday attack

- Multiple in-flight queries for same QNAME/QTYPE/QCLASS
- Answers without ECS record are accepted
- RFC7871, section 11.2
  - States issue, but no solution
Limit ECS queries, but how..?

- ECS support signaling by nameservers
  - Does not exist :(
- RFC7871, section 12
  - Whitelist
  - Probing
Probing proposal

• Always include ECS record
• Set prefix scope to /0 on first query
  – No ECS in response → accept answer
  – ECS in response → send new query containing client’s address in ECS record
Probing proposal - cont.

• No extra queries for non-ECS zones
• No ECS to root and TLDs
  – QNAME minimisation
• Dropping queries containing unknown EDNS options → mark as “EDNS lame”
  – No DNSSEC
Birthday attack hardening

• Require ECS response when probing query shows ECS support
  – Re-query without ECS otherwise

• Also probe before forwarding ECS!
  – Exception possible when incoming query has /0 prefix (don’t probe the probing query)
Please share your opinions!

• Can the whitelist approach be (operationally) workable?
• Do we need a signaling specification?
• Should we do probing? Is this the correct way?