DNSSEC
Roadblock Avoidance

Ólafur Guðmundsson

Wes Hardaker

Ready For WGLC?

- YES
- But there is this one issue
  - Resolver address != Single host
    - Causes: Anycast Resolvers and DNS proxies

Anycast Resolvers

- Most of the time harmless as each address has “singular service level” for DNS
    - The issues we see may cause false negatives if tests are ignorant of side effects i.e. TTL may jump around for repeated queries
    - Big issue if answer for same query differs in content
        - Some return AD bit but not all
        - Bigger issue if some return RRSIG but others do not
- Proposal for treatment → Add text explaining how to detect and the side effects and how to interpret them

DNS Proxies

- Bad Hotel Proxy advertises 3 address for resolvers that are Public Open Resolvers, one validating.
  - The three Resolvers have different DNSSEC compliance
  - Proxy DOES NOT honor address in query but Randomly sends query to one of the 3 listed
  - Proxy does not cache results
- Result: 1/3 of answers from signed zones for have AD bit set. → simplistic application of tests in draft will result misidentify the "resolvers"
- Proposed solution → document how to detect bad proxies and throw up our hands when service levels differ.