DNS Resolver Information

draft-ietf-add-resolver-info-06

T. Reddy (Nokia) & M. Boucadair (Orange)

Document Status

- Successfully passed WGLC

Comments Raised Since Then

- Tommy Jensen raised DDR-related comments during document shepherd review
  - RESINFO response from an attacker
  - DNSSEC cannot be used with DDR; DNSSEC protection is not possible with "resolver.arpa"

DNSSEC validation is possible with DNR and IKEv2 configuration for Encrypted DNS.

The “sig” Approach for DDR

- Added “sig” attribute: signature of RESINFO RR
- Signature will be calculated by Encrypted DNS resolvers using the private key of the certificate
- Clients will validate signature using the public key in the DNS resolver's certificate
- “sig” attribute only required with DDR

Objections from Ben Schwarz

- Not deployable in architectures that separate TLS termination from DNS logic
  - Clear text traffic between the TLS terminator and DNS server.
  - Goes against zero-trust security framework

Some Observations

- No defense against resolver lying about the attributes “qnamemin”, “exterr” and “inforul” in RESINFO.
  - The resolver can provide inaccurate information, but data origin authentication will verify that the data has been generated by the resolver itself
  - Explicit tests possible on some of the attributes, such as ‘exterr’
  - ‘infourl’ is for troubleshooting purpose only
  - Future, new attributes that can possibility be attested or verified

Other Possible Solutions

- RESINFO MUST NOT be used with DDR
  - Cons: Reduces the scope of the specification

- RESINFO can be used where the client has out-of-band agreement with the server to comply with the claims
  - Cons: Significantly reduces the scope of the specification

Other Possible Solutions

- Move metadata into EDNS, but …
  - DNS forwarders without caching capability can forward unknown EDNS
  - EDNS is unauthenticated information and not protected by DNSSEC
  - Why lose the advantage of DNSSEC provided to DNR and IKEv2 configuration for Encrypted DNS?

Other Possible Solutions

- Relax the rule to validate the "sig" attribute from "MUST" and "SHOULD" for DDR

- Explain when the SHOULD can be safely ignored
  - In cases where the "sig" attribute is not provided, clients can process the response if and only if they have an out-of-band agreement with the server operator to support RESINFO

Next Steps ?

- Which approach should we follow here:
  1. Current approach in the draft: MUST ‘sig’ for DDR
  2. Relax MUST to “SHOULD + out-of-band agreement”
  3. EDNS
  4. Exclude DDR
  5. RESINFO where client has an agreement with the DNS server

- The Authors recommend to maintain the current design (1) in the I-D