Clarifications to the DNS Ranking Data
draft-fujiwara-dnsop-ranking-data-00

K. Fujiwara and W. Toorop
IETF 122 dnsop WG

Section 5.4.1 (Ranking data) of [RFC2181]

- assumed that information obtained from zone files, zone transfers, and name resolution will be mixed together.
- In the past, recursive resolvers would return data from referral responses, such as delegation information or glue, in the answer section of responses;
  - however, modern recursive resolvers complete name resolution with an authoritative response from an authoritative server that has authority through delegation. However, there is no clear documentation of this.
- "The Ranking Data" only indicates the priority among data, not its validity.
  - Attacks using responses that do not correspond to queries and additional data that is not required have been considered and reported, so unnecessary data should be discarded.

Proposal

1. Obsolete Section 5.4.1 (Ranking data) of [RFC2181]
2. Add new directives on how to handle the data

New Directives

1. Authoritative servers MUST NOT merge zone data. (zone data should be retrieved from a source (zone file, internal database, zone transfer)
2. Name resolution results (Answer section, or NXDOMAIN, NODATA) MUST be authoritative responses from authoritative servers that has authority through delegation.
3. Non-authoritative responses (referral/delegation responses) from authoritative servers MUST only be used to query the delegated authoritative server during the name resolution.
4. Names and IP addresses of the authoritative name servers for zones (such as the root zone) that are built-in or loaded from "hints" files, MUST only be used for priming a resolver for those zones [RFC9609].

Additional Considerations

[Further directives could be made, they may be DNS software implementation guidelines, which would be large in scale, so it is necessary to consider whether to proceed with them.]

- If a DNS server plays different roles for different namespaces (authoritative server, recursive resolver, forwarder), it MUST not merge DNS data for each role.
- The Additional Section returned as the result of name resolution MUST be exactly the same as the Additional Section that came from the authoritative response from the authoritative server, or a separate authoritative response resulting from name resolution.
- Full-service resolvers SHOULD only accept the following data from authoritative servers:
  - NS and DS RRSets (+RRSIG) in the Authority Section of the delegation response and Glue A/AAAA in the Additional Section,
  - SOA RRs (+RRSIG) in the Authority Section of authoritative NXDOMAIN and NODATA responses in response to the query,
  - the Answer Section (+RRSIG) of the authoritative response in response to the query, and
  - any additional sections allowed by type (delegated domain name),
  - and SHOULD not accept any other information

Comments

- Unbound treats DS RRSet+RRSIG in a referral response as the same as an authoritative response
- RFC 5452 updates Section 5.4.1 of RFC 2181
  - adding new text: "Full-service resolver function MUST perform section 9.1 of RFC 5452 Query Matching Rules before these directives."
- Recursive resolvers still do mix authoritative and recursive functions
  - BIND 9’s zone within recursive mode and Unbound’s local-zone changes that the server will act as an authoritative server at the specified domain name and below
- Consider RFC 8806 (Local Root)
- Directive 3: “during **the** name resolution" prevents cachg → remove “the”
- Some texts on Section 5.4.1 of RFC 2181 are necessary: “Address record” and “Glue” → “obsolete” is not good
- The word “merge” is confusing
- Consider RFC 8198 Aggressive Use of DNSSEC-Validated Cache
- Consider RPZ/DNSBL issues
- Consider mixing use of forwarders (Public Resolvers and split-horizen)

Next steps

- Authors will update the draft soon after the IETF 122 to reflect comments
  - Change “obsolete” to “update” Section 5.4.1 of RFC 2181 Ranking Data
  - many fixes
- Then, please review