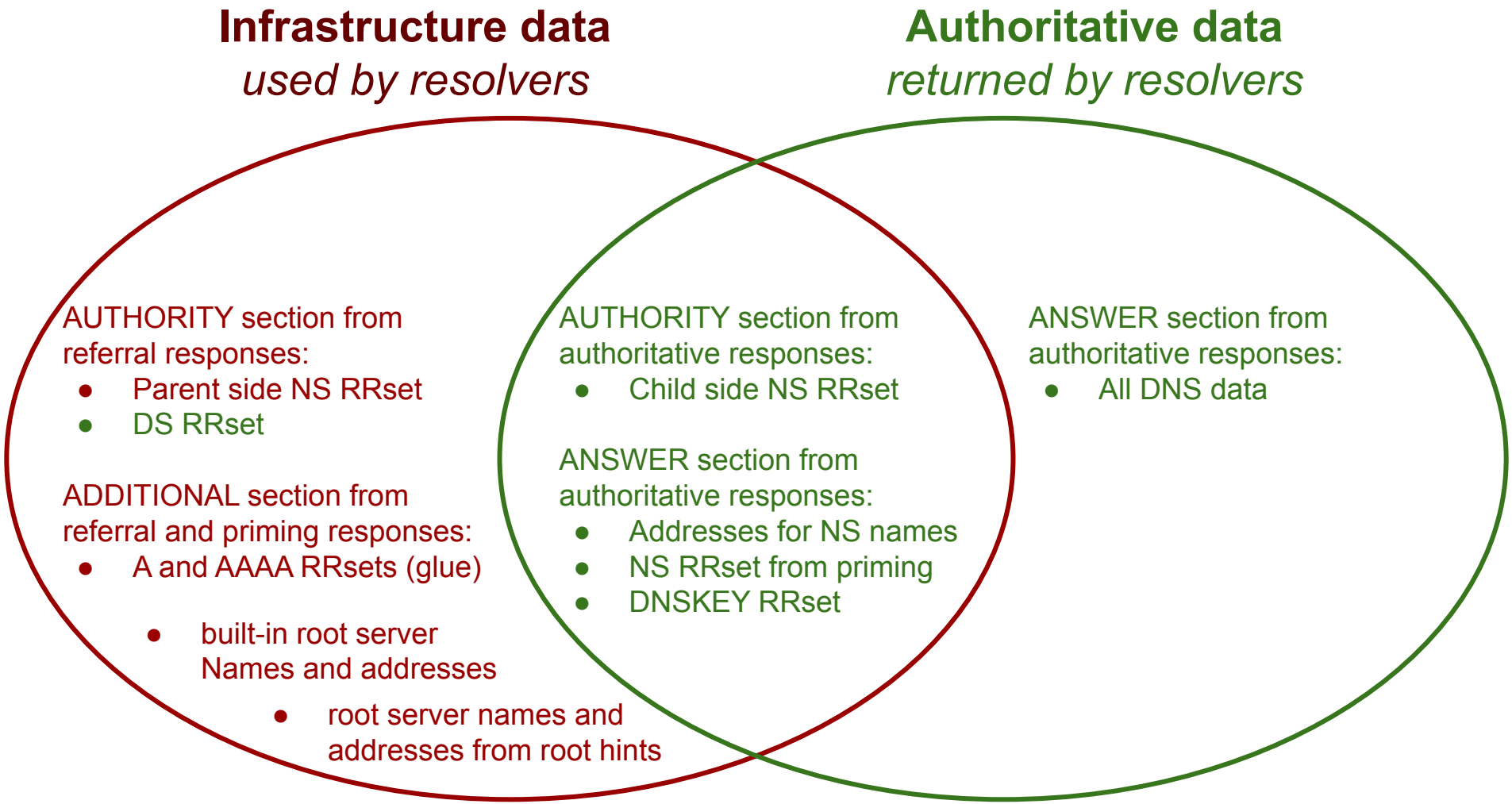
Delegation Revalidation

draft-ietf-dnsop-ns-revalidation

Shumon Huque
Paul A. Vixie
Willem Toorop

Motivation

- Increase trustworthiness of ***infrastructure RRsets***


Infrastructure data
used by resolvers
Authoritative data
returned by resolvers
AUTHORITY section from referral responses:
Parent side NS RRset
DS RRset
ADDITIONAL section from referral and priming responses:
A and AAAA RRsets (glue)
built-in root server Names and addresses
root server names and addresses from root hints
AUTHORITY section from authoritative responses:
Child side NS RRset
ANSWER section from authoritative responses:
Addresses for NS names
NS RRset from priming
DNSKEY RRset
ANSWER section from authoritative responses:
All DNS data

Motivation

- Increase trustworthiness of ***infrastructure RRsets***
- [RFC 2181 5.4.1. Ranking data]

AAA	-	Data from a primary zone file, other than glue
AA	-	Data from a zone transfer, other than glue
A	-	Authoritative data in the answer section
A-	-	The authority section of an authoritative answer
BBB	-	Glue from a zone file or zone transfer
BB	-	The answer section of a non-authoritative answer, and
	-	Non-authoritative data from the answer section
B	-	Additional information from an authoritative answer,
	-	The authority section of a non-authoritative answer,
	-	Additional information from non-authoritative answers.

Name server addresses
Revalidated NS RRset
NS RRset from referral
Glue from referral

Motivation

- Increase trustworthiness of infrastructure RRsets
  - Reduce risk of cache poisoning
  - Reduce risk of query redirection (Improve privacy)
  - **DNSSEC grade protection of infrastructure RRsets**!

The reduced risk of redirected query traffic with signed root name server data

“ Revalidation is the **only** mitigation that also works against **on-path** attackers!

Motivation

- Increase trustworthiness of i
  - Reduce risk of cache p
  - Reduce risk of query re
  - **DNSSEC grade pr** **sets**!

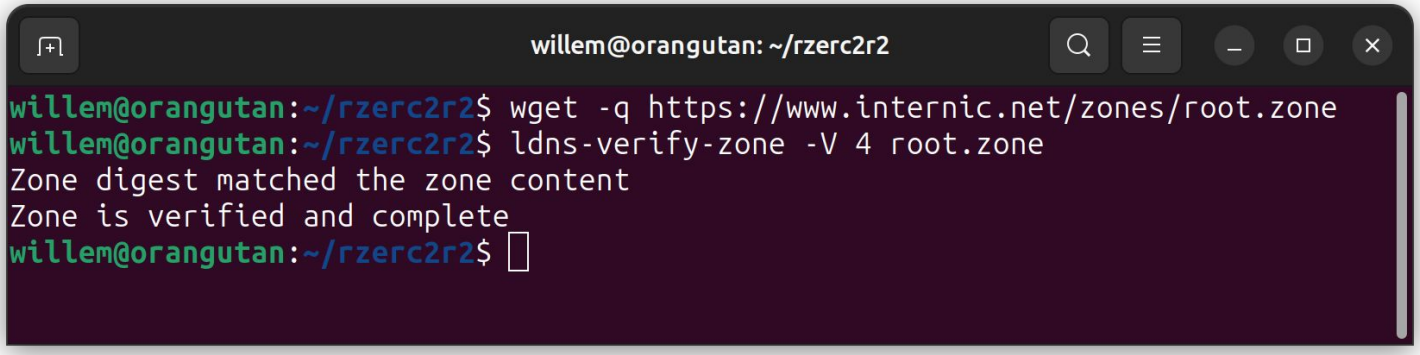
Don't be a DNSSEC snob and also help the unsigned!

The reduced risk of redirected query traffic with signed root name server data

" Revalidation is the **only** mitigation that also works against **on-path** attackers!

New since version -07

- Send DNS Error report when NS RRset mismatch is detected
- Mention that ZONEMD + local root give comparable protection



- Acknowledge parent only resolvers (*draft-fujiwara-dnsop-resolver-update*)
  - Not vulnerable to many cache poisoning attacks
  - But also no DNSSEC grade protection against query redirection

New since version -07

- Mention possibility for implementations wishing to consider to limited revalidation to the parts of the domain name space where it counts the most.
- Added an Implementation status section
  - The Unbound resolver since version 1.1 (August 29, 2008)
  - Redhat Enterprise Linux has been running revalidating Unbound for years without problems
  - The Knot Resolver software revalidates the priming response since version 1.5.1 (released December 12, 2017)

Mission accomplished

- We’re done
- Questions?
- Comments?