DNS privacy using Unbound

Ralph Dolmans

ralph@nlnetlabs.nl

Nordic Domain Days 2018

Unbound

NSD

unbound

Methods to improve DNS privacy

- Limit the number of DNS queries
- Minimise the data disclosed in DNS transactions
- Encrypt DNS transactions

RFC7706 – root zone in resolver

- In RFC: Unbound with stub + NSD
- Unbound implementation: auth-zone

```
auth-zone:
        name: "."
        fallback-enabled: yes
        for-downstream: no
        master: b.root-servers.net
        master: c.root-servers.net
        master: e.root-servers.net
        master: f.root-servers.net
        master: g.root-servers.net
        master: k.root-servers.net
```

Auth-zone – local TLD

- Not limited to the root zone

```
auth-zone:
        name: "se"
        fallback-enabled: yes
        for-downstream: no
        master: zonedata.iis.se
        zonefile: “se.zone”
```

RFC8198 - Aggressive NSEC

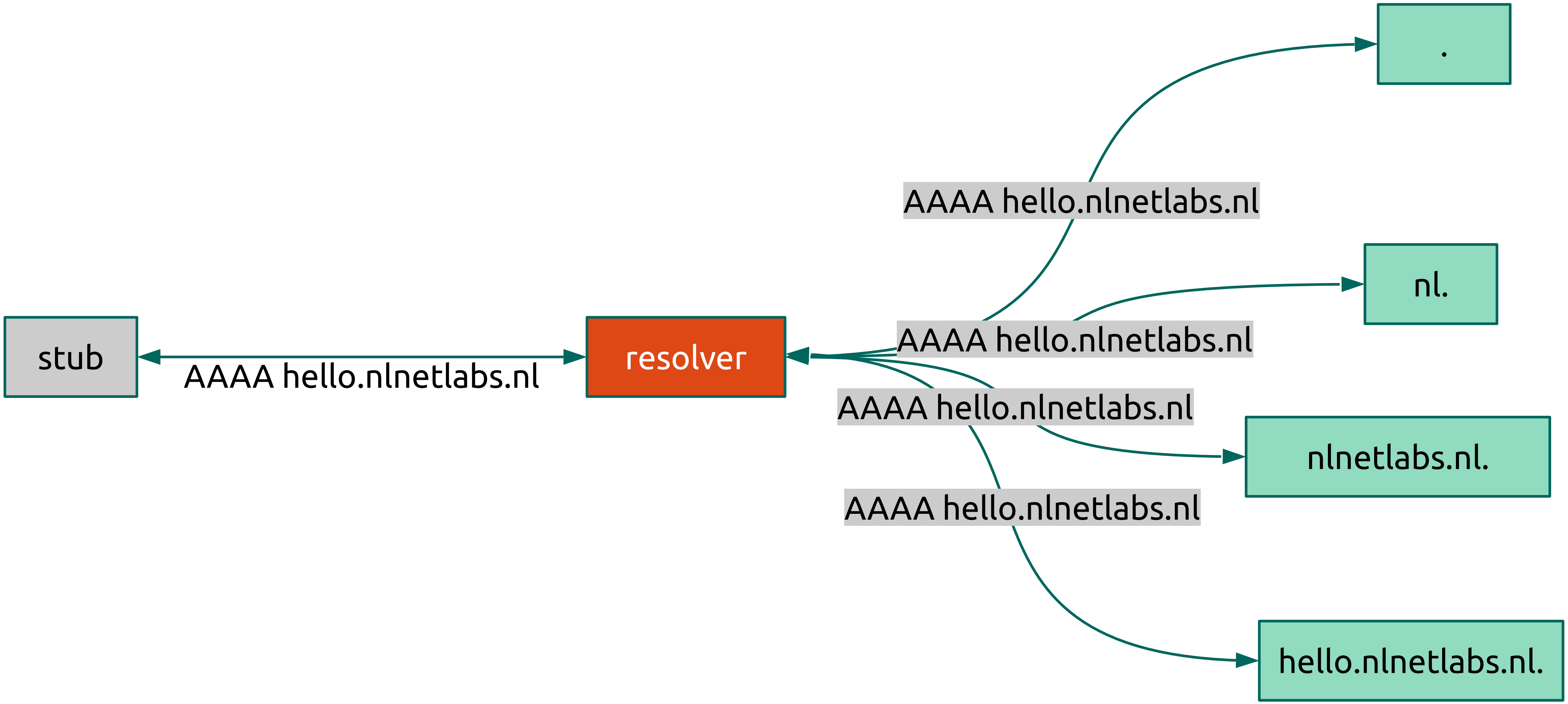
- Use cached NSEC records to synthesise answers
  - Negative answers (NODATA and NXDOMAIN)
  - Wildcard answers
- Also for NSEC3 in the future
  - With an exception for NSEC3 opt-out

```
aggressive-nsec: yes
```

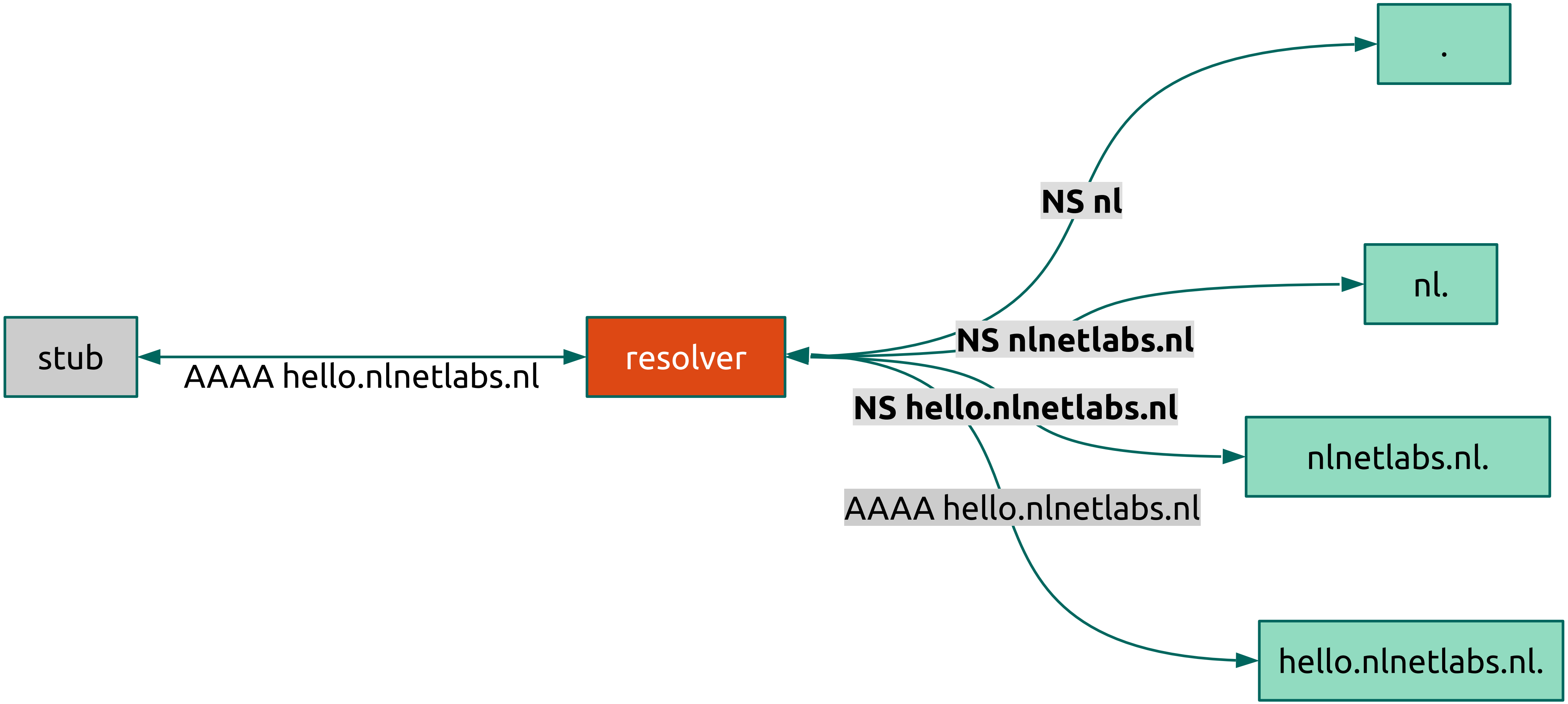
Minimise disclosed data

- RFC7816 - **QNAME minimisation**
- Do not show more of the QNAME than necessary
- Do not show the QTYPE if not necessary

Without QNAME minimisation



With QNAME minimisation

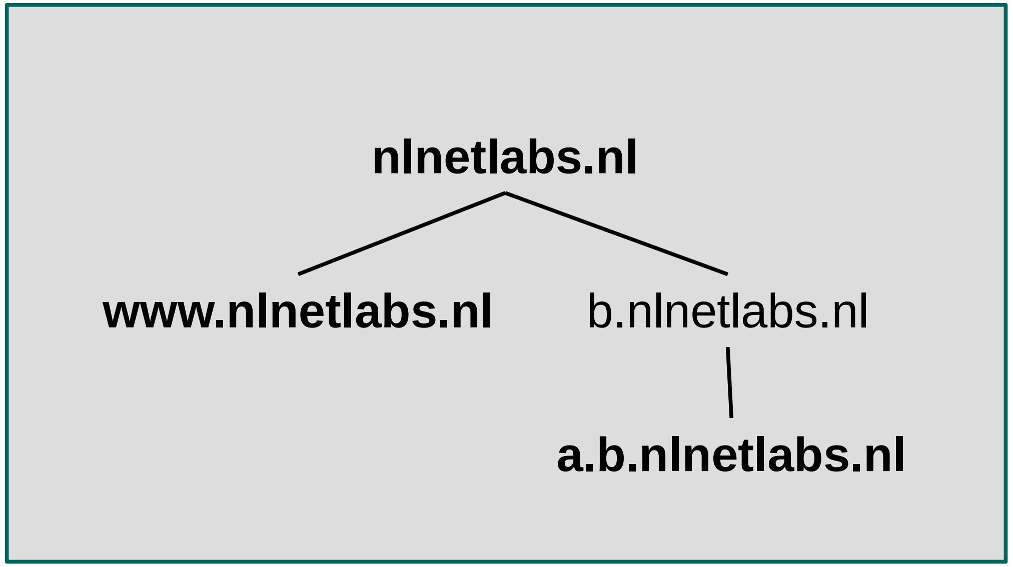


QNAME minimisation issues

- Lot of queries for some domains, e.g. 0.1.0.0.0.0.0.0.0.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.9.b.4.0.a.2.ip6.arpa.
- Queries for NS QTYPE not always (correctly) answered
- Unclear when to stop resolving
    - RFC8020- NXDOMAIN: There Really Is Nothing Underneath

Empty-non-terminals

- Existing name without records
- Example zone with records for **nlnetlabs.nl**, **www.nlnetlabs.nl** and **a.b.nlnetlabs.nl**
- b.nlnetlabs.nl is an empty-non-terminal



QNAME minimisation in Unbound

- Do QNAME minimisation with QTYPE=A
- Limit number of queries
  - Limit QNAME minimisation iterations to 10
  - Always append one label for the first 4 queries
- Continue without minimisation when RCODE != NOERROR
  - Exception for DNSSEC signed domains

Encrypt DNS transactions

TLS to client

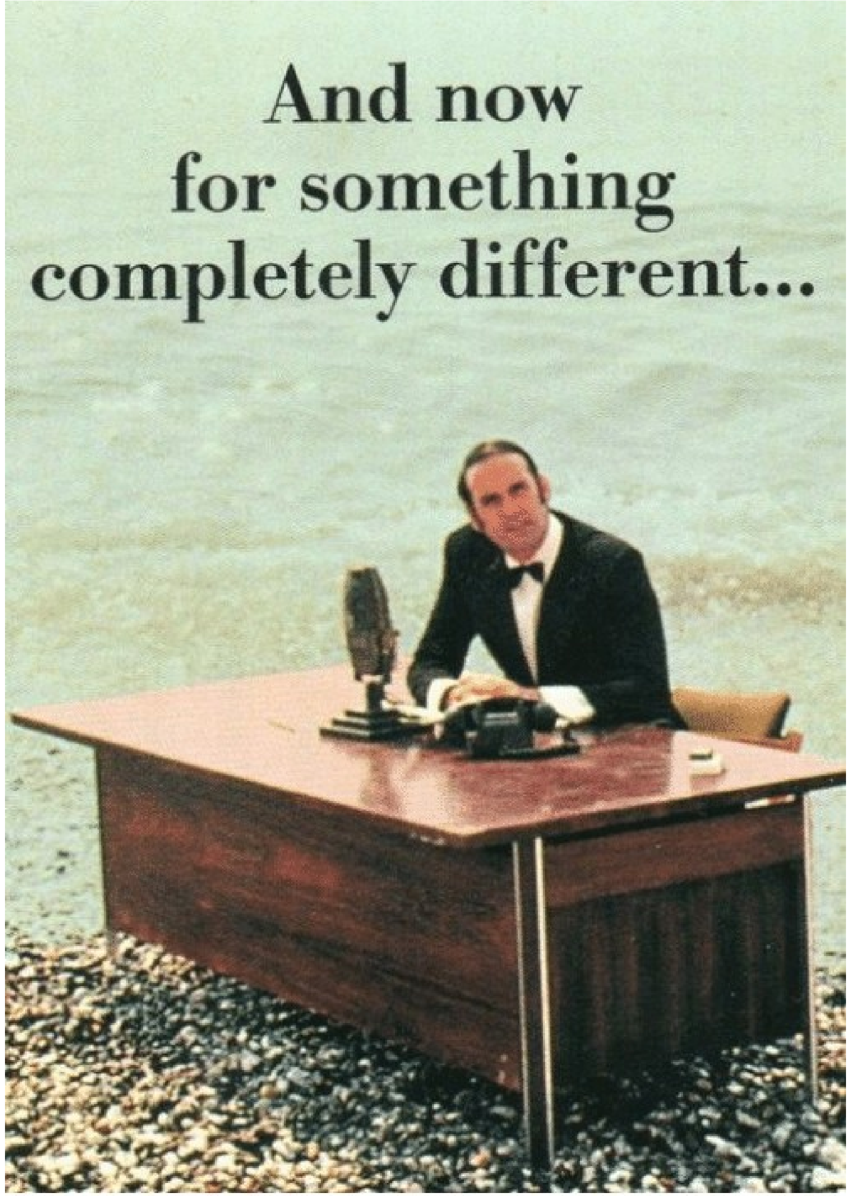
```
server:
        interface: 0.0.0.0@853
        interface: ::0@853
        tls-service-key: "privatekeyfile.key"
        tls-service-pem: "publiccertfile.pem"

        do-udp: no
        udp-upstream-without-downstream: yes
```

TLS to forwarder

```
server:
        tls-cert-bundle: “/etc/ssl/certs/ca-certificates.crt”

forward-zone:
        name: “.”
        forward-tls-upstream: yes
        forward-addr: 9.9.9.9@853#dns.quad9.net
        forward-addr: 1.1.1.1@853#cloudflare-dns.com
```


And now
for something
completely different...

DNS flag day – February 1st 2019

- Query timeout will no longer be a reason to re-query without EDNS
- Test your domain: https://dnsflagday.net

Questions?

Ralph Dolmans

ralph@nlnetlabs.nl