QNAME minimisation

Ralph Dolmans
ralph@nlnetlabs.nl (NLnet Labs)
Introduction

• About NLnet Labs
  - A not for profit, public benefit foundation
  - “develop Open Source software and open standards for the benefit of the Internet”
  - NSD, OpenDNSSEC, getdns, Ldns, Net::DNS

• Unbound
  - Validating, caching resolver
“Pervasive Monitoring Is an Attack”

• RFC7258
  - Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.
Privacy in DNS

• DNS data is public
• Transactions should not be public
  – MX nlnetlabs.nl.
  – `H(ralph)`._openpgpkey.nlnetlabs.nl
Privacy Threat Mitigations

• Privacy Considerations for Internet Protocols, RFC6973
  - 6.1 Data Minimization
    • “Reducing the amount of data exchanged reduces the amount of data that can be misused or leaked.”
  
  - 6.3 Security
    • “Confidentiality: Keeping data secret from unintended listeners.”
Resolving

stub → resolver
  ^  ^  ^
A nlnetlabs.nl | A nlnetlabs.nl | A nlnetlabs.nl

resolver → nl.
  ^  ^
A nlnetlabs.nl | A nlnetlabs.nl

nl. → nlnetlabs.nl.
QNAME minimisation

• DNS Query Name Minimisation to Improve Privacy, RFC7816:
  – “The request is done with:
    • the QTYPE NS,
    • the QNAME which is the original QNAME, stripped to just one label more than the zone for which the server is authoritative.”
Resolving with QNAME minimisation

stub -> A nlnetlabs.nl

resolver

NS nl

A nlnetlabs.nl

nl.net

NS nlnetlabs.nl

A nlnetlabs.nl

nlnetlabs.nl.
QNAME minimisation in Unbound

• Version 1.5.7
• Default off
• Enable in config:

server:
  qname-minimisation: yes
Resolve AAAA nlnetlabs.nl

./unbound -dd 2>&1 | grep send

info: sending query: nl. NS IN
debug: sending to target: <.> 2001:500:2d::d#53
info: sending query: nlnetlabs.nl. NS IN
debug: sending to target: <nl.> 194.171.17.10#53
info: sending query: nlnetlabs.nl. AAAA IN
debug: sending to target: <nlnetlabs.nl.> 2a04:b900::8:0:0:60#53
State diagram

- qname-minimisation: yes
- qname-minimisation: no

*INIT_MINIMISE_STATE*

- dp change (referral or cname)
- timeout

*SKIP_MINIMISE_STATE*

*MINIMISE_STATE*

- RCODE not NOERROR or last label
- next iteration

*DONOT_MINIMISE_STATE*

- Done resolving
When to stop?

• Continue iterating until all labels from original QNAME are in minimised QNAME?
  – DoS

• Until the nameserver indicates requested domain doesn't exist (NXDOMAIN) or on error?
wildcard.whitehouse.gov.edgekey.net

info: sending query: edgekey.net. NS IN
debug: sending to target: <net.> 192.5.6.30#53
info: sending query: gov.edgekey.net. NS IN
debug: sending to target: <edgekey.net.> 95.100.168.65#53

NXDOMAIN
Other wrong RCODEs

$ dig ns www.limburg.nl | grep status
;; ->>>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 14956

-Also: REFUSED on QTYPE=NS
When to stop resolving?

• We can't ignore the RCODE and continue resolving
• We can't trust the RCODE and stop resolving
• Stop minimisation when RCODE is not NOERROR
  - DONOT_MINIMISE_STATE: send full QNAME and original QTYPE
• Not conform RFC
Impact fall-back

- Stop on NXDOMAIN decreases privacy
  - Queries become visible
    - www.nlnetlabs.nl – visible at root
    - www.nlnetlabss.nl – visible at .nl
  - Active attacks possible but detectable
Number of queries

stub
A www.nlnetlabs.nl

resolver

ns.nl

ns.nl

ns www.nlnetlabs.nl

A www.nlnetlabs.nl

www.nlnetlabs.nl.

nl.

.
Number of queries - 2

• Without QNAME minimisation
  - Number of zones

• With QNAME minimisation
  - Total number of labels
    • original QNAME, delegations, CNAME, ...
    - + number of resolved delegations
  - +1 (original QTYPE query)
    • Except when QTYPE is DS or QTYPE is NS and QNAME not zone apex
Number of queries - 3

- AAAA www.ietf.org
  - 3 labels, 3 zones
  - NS:
    - ns1.ams1.afilias-nst.info.
      - 4 labels, 3 zones
      - +1 query for QTYPE=AAAA
  - CNAME:
      - 6 labels, 3 zones
      - +1 query for QTYPE=AAAA

9 vs 15 queries
Reverse IPv6

• nlnetlabs.nl reverse IPv6:
  0.1.0.0.0.0.0.0.0.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.b.4.0.a.2.ip6.arpa.
  - 4 zones
  - 34 labels

• Unbound 1.5.7 “solution”: increase IPv6 address by 8 labels every iteration. Start with ip6.arpa.
Other large zones

• DNSBL, Wildcards(!!)

• Next release:
  - Limit QNAME minimisation iterations to 10
  - Always append one label for the first 4 queries
  - Example, QNAME with 18 labels, appended labels per iteration:
    • 1,1,1,1,2,2,2,2,3,3
Forwarding

- Forwarder will eventually receive full QNAME and QTYPE
  - Except when NXDOMAIN on intermediate query
  - Not with current fall-back

- Forwarder has to do it anyway
  - Minimising minimised queries

- No QNAME minimisation when forwarding query
Benefits

• Cache intermediate domain names
  – More specific NXDOMAIN cache
    • draft-vixie-dnsext-resimprove
    • draft-ietf-dnsop-nxdomain-cut
  – Improves privacy and performance
    • No need to perform lookup
    • No need to expose data

server:
  qname-minimisation: yes
  harden-below-nxdomain: yes

https://www.nlnetlabs.nl/  OARC 24 (Buenos Aires) - March 2016
Benefits cont.

• Example queries:
  - Q1: b.nonexistent.
  - Q2: a.b.nonexistent.
  - Q3: c.nonexistent.

• With QNAME minimisation: Q3 NXDOMAIN from cache
$ drill txt qnamemintest.internet.nl

"HOORAY - QNAME minimisation is enabled on your resolver :)!"

"NO - QNAME minimisation is NOT enabled on your resolver :(."

Test
More to be done

• Only minimising data received by authoritative nameservers
• Not on resolvers!
• Not hiding data on the wire!
  – DPRIVE (stub to resolver)

• No full QNAME fall-back for NXDOMAIN in signed zones?
Questions?