Network Working Group
Internet-Draft
Intended status: Informational
Expires: November 20, 2014

S. Bortzmeyer
AFNIC

May 19, 2014

DNS query name minimisation to improve privacy
draft-bortzmeyer-dns-qname-minimisation-02

Abstract

This document describes one of the techniques that could be used to improve DNS privacy (see [I-D.bortzmeyer-dnsop-dns-privacy]), a technique called "qname minimisation".

Discussions of the document should currently take place on the dns-privacy mailing list [dns-privacy].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on November 20, 2014.

Copyright Notice

Table of Contents

1. Introduction and background

The problem statement is exposed in [I-D.bortzmeyer-dnsop-dns-privacy]. The terminology ("qname", "resolver", etc) is also defined in this companion document. This specific solution is not intended to completely solve the problem, far from it. It is better to see it as one tool among a toolbox.

It follows the principle explained in section 6.1 of [RFC6973]: the less data you send out, the less privacy problems you'll get.

2. Qname minimisation

The idea is to minimise the amount of data sent from the DNS resolver. When a resolver receives the query "What is the AAAA record for www.example.com?", it sends to the root (assuming a cold resolver, whose cache is empty) the very same question. Sending "What are the NS records for .com?" would be sufficient (since it will be the answer from the root anyway). To do so would be compatible with the current DNS system and therefore could be easily deployable, since it is an unilateral change to the resolvers.

If "minimisation" is too long, you can write it "m12n".

To do such minimisation, the resolver needs to know the zone cut [RFC2181]. There is not a zone cut at every label boundary. If we take the name www.foo.bar.example, it is possible that there is a zone cut between "foo" and "bar" but not between "bar" and "example". So, assuming the resolver already knows the name servers of .example, when it receives the query "What is the AAAA record of www.foo.bar.example", it does not always know if the request should be sent to the name servers of bar.example or to those of example. [RFC2181] suggests a method to find the zone cut (section 6), so resolvers may try it.

Note that DNSSEC-validating resolvers already have access to this information, since they have to find the zone cut (the DNSKEY record set is just below, the DS record set just above).

It can be noted that minimising the amount of data sent also partially addresses the case of a wire sniffer, not just the case of privacy invasion by the servers.

One should note that the behaviour suggested here (minimising the amount of data sent in qnames) is NOT forbidden by the [RFC1034] (section 5.3.3) or [RFC1035] (section 7.2). Sending the full qname to the authoritative name server is a tradition, not a protocol requirment.

3. Operational considerations

The administrators of the forwarders, and of the authoritative name servers, will get less data, which will reduce the utility of the statistics they can produce (such as the percentage of the various qtypes). On the other hand, it will decrease their legal responsability, in many cases.

Some broken name servers do not react properly to qtype=NS requests. As an example, look at www.ratp.fr (not ratp.fr), which is delegated to two name servers that reply properly to "A www.ratp.fr" queries but send REFUSED to queries "NS www.ratp.fr". This behaviour is a gross protocol violation and there is no need to stop improving the DNS because of such brokenness. However, qname minimisation may still work with such domains since they are only leaf domains (no need to send them NS requests).

Another way to deal with such broken name servers would be to try with A requests (A being choosen because it is the most common and hence the least revealing qtype). Instead of querying name servers with a query "NS example.com", we could use "A _.example.com" and see if we get a referral.

4. Other advantages

The main goal of qname minimisation is to improve privacy, by sending less data. However, it may have other advantages. For instance, if a root name server receives a query from some resolver for A.CORP followed by B.CORP followed by C.CORP, the result will be three NXDOMAINs, since .CORP does not exist in the root zone. Under query minimization, the root name servers would hear only one question (for .CORP itself) to which they could answer NXDOMAIN, thus opening up a negative caching opportunity in which the full resolver could know a priori that neither B.CORP or C.CORP could exist. Thus in this common case the total number of upstream queries under query minimisation would be counter-intuitively less than the number of queries under the traditional iteration (as described in the DNS standard).

5. Security considerations

Under study. TODO: better handling of phantom domains?

6. Acknowledgments

Thanks to Olaf Kolkman, Mark Andrews and Francis Dupont for the interesting discussions on this qname minimisation. Thanks to Mohsen Souissi for proofreading. Thanks to Tony Finch for the zone cut algorithm in Appendix A. Thanks to Paul Vixie for pointing out that there are practical advantages (besides privacy) to qname m12n. Thanks to Phillip Hallam-Baker for the fallback on A queries, to deal with broken servers.

7. References

7.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, July 2013.

[I-D.bortzmeyer-dnsop-dns-privacy]
Bortzmeyer, S., "DNS privacy problem statement", draft-bortzmeyer-dnsop-dns-privacy-01 (work in progress), December 2013.

7.2. Informative References

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.

[dns-privacy]
IETF, , "The dns-privacy mailing list", March 2014.

Appendix A. An algorithm to find the zone cut

Although a validating resolver already has the logic to find the zone cut, other resolvers may be interested by this algorithm to follow in order to locate this cut:

(0) If the query can be answered from the cache, do so, otherwise iterate as follows:

(1) Find closest enclosing NS RRset in your cache. The owner of this NS RRset will be a suffix of the QNAME - the longest suffix of any NS RRset in the cache. Call this PARENT.

(2) Initialize CHILD to the same as PARENT.

(3) If CHILD is the same as the QNAME, resolve the original query using PARENT's name servers, and finish.

(4) Otherwise, add a label from the QNAME to the start of CHILD.

(5) If you have a negative cache entry for the NS RRset at CHILD, go back to step 3.

(6) Query for CHILD IN NS using PARENT's name servers. The response can be:

(6a) A referral. Cache the NS RRset from the authority section and go back to step 1.

(6b) An authoritative answer. Cache the NS RRset from the answer section and go back to step 1.

(6c) An NXDOMAIN answer. Return an NXDOMAIN answer in response to the original query and stop.

(6d) A NOERROR/NODATA answer. Cache this negative answer and go back to step 3.

Author's Address

Stephane Bortzmeyer
AFNIC
1, rue Stephenson
Montigny-le-Bretonneux 78180
France

Phone: +33 1 39 30 83 46
Email: bortzmeyer+ietf@nic.fr
URI: http://www.afnic.fr/