Contribution ID : **16** Type : **not specified**

QNAME minimisation in Unbound

Thursday, 31 March 2016 16:30 (30)

Data stored in the DNS is publicly visible. DNS transactions, on the other hand, contain privacy sensitive information. The Snowden revelations about pervasive monitoring are seen as a wake up call for the internet community to increase the focus on privacy protection. One of the privacy threat mitigation methods mentioned in RFC6973, is the principle of data minimisation[0]. The RFC states that: "Reducing the amount of data exchanged reduces the amount of data that can be misused or leaked.".

One of the new features in Unbound 1.5.7 is the support of QNAME minimisation[1]. QNAME minimisation is a technique to improve DNS privacy by limiting the amount of privacy sensitive data exposed to authoritative nameservers. This is done by limiting the number of labels in the QNAME sent to nameservers and by setting the QTYPE to NS in order to hide the original QTYPE where possible.

Although the proposed minimisation of the QNAME and using the NS QTYPE are not strictly forbidden in the original DNS RFC, not all nameservers handle these queries the way they should. Common wrong responses are NXDOMAIN on empty-non-terminals and refusing queries with QTYPE=NS. Resolving when using QNAME minimisation will fail on these broken nameservers. We suspect that operators will not adopt QNAME minimisation when it is implemented according to the specification. Unbound is shipped with an implementation that will resolve queries "as usual" when broken nameservers are detected.

QNAME minimisation can increase the number of queries sent to nameservers. This is most notable when resolving in the ip6.arpa name space. To limit the number of queries for reverse IPv6 lookups, unbound increments the minimised QNAME with 8 labels on each iteration when the original QNAME is a subdomain of ip6.arpa.

An uncovered topic in the specification is QNAME minimisation and forwarders. Because of the "best effort" approach, there is no privacy enhancement when minimising queries to forwarders. Unbound does not minimise queries sent to forwarders.

The most important reason to enable QNAME minimisation is the improved privacy. There are, however, some other benefits. One of them is that querying all intermediate domain names will result in a more precise negative cache. This improves both performance and privacy. Although using a completely different technique, QNAME minimisation can lead to the same result as described in draft-wkumari-dnsop-cheese-shop-00[2]. Namely reducing the amount of traffic to the root servers.

[0] - https://tools.ietf.org/html/rfc6973#section-6.1
[1] - https://tools.ietf.org/html/draft-ietf-dnsop-qname-minimisation-09.
[2] - https://tools.ietf.org/html/draft-wkumari-dnsop-cheese-shop-00

Summary

Primary author(s) : DOLMANS, Ralph (NLnet Labs)

Presenter(s) : DOLMANS, Ralph (NLnet Labs)

Session Classification : Public Workshop: Privacy

Track Classification : Public Workshop