CONNOTECH Experts-conseils inc.

A Short Note about

DNSSEC Impact on Root Server Answer Sizes

Thierry Moreau

Document Number C003924

2006/08/08

Table of Contents

Document Revision History

C-Number	Date	Explanation
C003924	2006/08/08	Initial release, adapted from document C003725 section 2.3.2.5
C003924		Current version

1. Introduction

The present document reports simple measurements of DNS response sizes for representative queries answered by DNS root servers, with emphasis on impact of the DNSSEC support at the root. From the mix of DNS queries reported in reference [2], we attempted to measure response sizes for the most prevalent DNS queries received by root servers. In addition, we anticipated the additional DNS queries implied by two DNS root key rollover schemes. This document reports measurements which should be verifiable independently, and does not attempt to predict a single performance factor implied by DNSSEC adoption at the root.

A comprehensive study of DNSSEC bandwidth impact is beyond the scope of the present document. We therefore present some observations on DNS response sizes on representative queries, with or without DNSSEC, from DNS root servers.

There are two kinds of queries of interest in this study:

- o normal DNS data queries, and
- o DNSSEC overhead queries, for key management support.

2. Normal DNS Data Queries

For normal DNS data queries we present some observations on DNS response sizes from a secure DNS root for a typical query for 'A' resource records for three types of domain names, namely

A) a sub-domain of a security-oblivious TLD,
B) a sub-domain of a security-aware TLD, and
C) a sub-domain of a non-existent TLD.

When turning on DNSSEC, the response sizes are influenced by the number of DNSSEC digital signatures, i.e. RRSIG RRs, for RRsets present in a response. The minimal response sizes occur when a single RRSIG RR is affixed to any RRset that deserves a DNSSEC digital signature. During a public key rollover operation, it is possible that two RRSIG RRs are needed for the same DNSKEY signature algorithm. We thus report response sizes for normal DNS queries with one or two RRSIG RRs affixed to any signed RRset.

Type of domain name	Security oblivious response size (ad hoc measurements)	Security awareness overhead, according to number of RRSIG RRs	
		1 RRSIG RR per signed RRset	2 RRSIG RRs per signed RRset
A	280 bytes	+200 bytes: 1 DS or NSEC RR 1 RRSIG RR	+365 bytes: 1 DS or NSEC RR 2 RRSIG RRs
B	403 bytes		
C	105 bytes	+541 bytes: 2 NSEC RRs 3 RRSIG RRs	+1011 bytes: 2 NSEC RRs 6 RRSIG RRs

In actual secure DNS operations, if the deployed key management scheme includes a KSK/ZSK separation, there would be transient conditions, i.e. a ZSK rollover, where the figures on the right column in the above table would apply (reference [4]).

The bandwidth required for normal DNS data queries is proportional to the query rate, and the proportion of DNSSEC-aware queries. So, the foremost factor to monitor for the DNSSEC impact on normal DNS data queries is the number of DNSSEC signatures affixed to a response RRset. In this respect, the selection of a key management scheme has no significant direct impact, i.e. as long as a scheme does not extend the periods during which two signatures are needed for each signed RRset (e.g. it avoids KSK/ZSK separation or it limits the periods in which two RRSIG RRs are affixed to a signed RRset).

3. DNSSEC Overhead Queries

For DNSSEC response sizes measurements, we use four hypotheses on the DNS zone key management. They come from the selection of trust anchor rollover procedure, and the decision to use or omit a zone signing key (i.e. KSK/ZSK separation):

Key management hypothesis	Selection of trust anchor rollover procedure	ZSK (zone signing key) use or omission
1	Timers-based trust anchor rollover (reference [1])	ZSK omitted
2		ZSK used
3	TAKREM trust anchor rollover (references [5] and [6])	ZSK omitted
4		ZSK used

DNSSEC overhead queries provide a DNS resolver with

1) the current set of zone keys (i.e. the DNSKEY RRset for a domain name) and
2) data relevant to the trust anchor key rollover operations.

For timers-based trust anchor rollover (reference [1]), the latter is embedded in the DNSKEY RRset, while the TAKREM trust anchor rollover uses the SDDA RRset for this purpose. A well run DNS resolver uses a cache to avoid repeated queries for the same data, primarily based on the TTL (Time To Live) field in RRsets in DNS responses. This applies to a zone key (DNSKEY RR) when it is encountered in a DNSSEC signature validation (i.e. RRSIG RR processing), *except when this zone key is a current trust anchor*. This exception is important for TAKREM bandwidth efficiency: because the TAKREM for DNSSEC rollover mechanism establishes an explicit cryptoperiod for a trust anchor (in SDDA RR fields), it avoids queries for the DNSKEY RRset when the trust anchor itself is used as a zone signing key (ZSK). The DNSSEC protocol allows the direct use of a trust anchor to sign a complete DNS zone file. This practice might be questioned only on the ground of key management dogma about cryptographic key separation.

In the case of the DNS root, as soon as the DNSSEC-awareness becomes noticeable in the fielded DNS resolvers, the operational advantage of limiting the DNSKEY RRset queries could be significant.

The query frequencies for DNSSEC overhead queries is best modeled on a per DNS resolver basis. In this perspective, there are three triggers for a DNSSEC overhead query:

1) The DNS resolver encounters an RRSIG RR using a key (identified by the key tag field) which is not a trust anchor and for which the DNSKEY RR is either unknown or has an expired TTL. The triggered query is for the DNSKEY RRset for the zone, and its frequency depends on the TTL field (e.g. 5 days).
2) The DNS resolver supports the TAKREM rollover scheme and encounters a RRSIG RR using a key (identified by the key tag field) which is unknown to the resolver and for which the resolver has TAKREM configured data for this zone. This triggers two queries, respectively for the DNSKEY and SDDA RRsets, at a frequency dependent on the trust

anchor cryptoperiod established by the SDDA RR authenticating the new trust anchor (e.g. one year).

3) The DNS resolver supports the timers-based trust anchor rollover (reference [1]) which mandates a DNSSEC overhead query (i.e. DNSKEY RRset) at least every 15 days.

The TAKREM bandwidth efficiency comes from the avoidance of situation 1) above, leaving the infrequent rollover, i.e. situation 2) above. The aggregation of DNS traffic from these individual resolver actions for bandwidth estimation purposes requires a population count of DNS resolvers, and a distribution of level of activity per resolvers. Some statistics were presented in 2002 for a subset of the DNS root servers (reference [2]), but they are somehow dated and not comprehensive.

We now explain the DNSSEC overhead response contents and overall sizes. DNSSEC overhead responses are obviously absent from security-oblivious queries. Among overhead responses from the DNS root, there is a variant-independent message portion, which is the 13 NS RRs corresponding to the 13 DNS root servers, about 200 bytes. Otherwise, the DNSSEC overhead responses are detailed in the table below:

	Timers-based trust anchor rollover (reference [1])	TAKREM trust anchor rollover
Representative query period for rollover purposes	5 days	1 year
DNSSEC overhead response with ZSK omitted	Hypothesis 1 2 DNSKEY RR / 1 RRSIG RR 13 NS RR / 1 RRSIG RR Size: 847 bytes	Hypothesis 3 1 DNSKEY RR / 1 RRSIG RR 13 NS RR / 1 RRSIG RR Size: 702 bytes 1 SDDA RR / 1 RRSIG RR 13 NS RR / 1 RRSIG RR Size: 783 bytes
DNSSEC overhead response with ZSK used	Hypothesis 2 3 DNSKEY RR / 1 RRSIG RR 13 NS RR / 1 RRSIG RR Size: 992 bytes	Hypothesis 4 2 DNSKEY RR / 1 RRSIG RR 13 NS RR / 1 RRSIG RR Size: 847 bytes 1 SDDA RR / 1 RRSIG RR 13 NS RR / 1 RRSIG RR Size: 783 bytes

This table supports the view that the query period is the most significant factor for TAKREM bandwidth efficiency, i.e. hypothesis 3 with one-year query for DNSKEY RRset and SDDA RRset. Another usage scenario relies on hypothesis 4 with 5-days queries for DNSKEY RRset and one-year query for SDDA RRset.

Finally, here are some notes on the methodology for the above representative measurements:

a) Data collected with bind software version 9.3.2 [3] enhanced with SDDA RR support [7], [8], DNSSEC-aware authoritative nameserver on a local network queried with the dig utility.

b) As an assumed operational good practice, the DNSKEY RRset signature by a ZSK (with hypotheses 2 and 4) has been manually removed from the DNS root zone data after the zone file signature utility has been run.

c) Key sizes 1024 bits using the RSASHA1 algorithm. For each 512 bits increment in key sizes, add 32 bytes of security awareness overhead per RRSIG or DNSKEY RR.

d) The assumed periods for DNSSEC overhead queries (5 days, 15 days, and one year) may vary according to DNS operational practices.

4. Conclusion

As the fielded population of DNS resolvers is expected to become increasingly DNSSEC-aware, the DNS root key management scheme is going to have an impact on DNS response sizes returned by root servers. The general recommendation would be to use as few public signature keys as possible, i.e. preferably a single one. In order to provide confidence in the DNSSEC crypto at the root, perhaps a larger key size would be preferred to a larger number of keys.

Among the DNS root key management scheme issues, there is the selection of a trust anchor key rollover solution. The DNS response size data reported above shows a bandwidth efficiency gain in the TAKREM rollover mechanism ([5], [6]) over the timers-based rollover alternative ([1]).

5. References

[1] M. StJohns, "Automated Updates of DNSSEC Trust Anchors", internet draft draft-ietf-dnsext-trustupdate-timers-02.txt, January 10, 2006, archived at http://www.watersprings.org/pub/id/draft-ietf-dnsext-trustupdate-timers-02.txt

[2] CAIDA, the Cooperative Association for Internet Data Analysis, "Clients of DNS Root Servers", Data were collected on 2002-08-14 for 26 hours at 10 minute intervals, available at http://www.caida.org/%7Ekkeys/dns/2002-08-14/

[3] http://www.isc.org/index.pl?/sw/bind/, ISC (Internet Systems Consortium) BIND (Berkeley Internet Name Domain)

[4] O. Kolkman, R. Gieben, "DNSSEC Operational Practices", internet draft draft-ietf-dnsop-dnssec-operational-practices-08.txt, March 6, 2006, archived at http://www.watersprings.org/pub/id/draft-ietf-dnsop-dnssec-operational-practices-08.txt

[5] Thierry Moreau, "The SEP DNSKEY Direct Authenticator DNS Resource Record (SDDA-RR)", Internet Draft draft-moreau-dnsext-sdda-rr-02.txt, April, 2006, archived at http://www.watersprings.org/pub/id/draft-moreau-dnsext-sdda-rr-02.txt

[6] Thierry Moreau, "The Trust Anchor Key Renewal Method Applied to DNS Security (TAKREM-DNSSEC)", Internet draft, draft-moreau-dnsext-takrem-dns-02.txt, April, 2005, archived at http://www.watersprings.org/pub/id/draft-moreau-dnsext-takrem-dns-02.txt

[7] Thierry Moreau, "Server Management Tools for Trust Anchor Key Management Based on TAKREM", CONNOTECH Experts-conseils inc., Document Number C003595, 2006/02/02

[8] http://www.connotech.com/takrem_tools/trust-anchor-foundry_02.tar.gz