

# Zone File Enumeration in DNSSEC

## Contents

1.	Issue .....	1
2.	Possible Solutions.....	1
2.1	Adopt DNSSEC but do nothing else .....	1
2.2	Not adopt DNSSEC.....	1
2.3	Change DNSSEC.....	2
2.4	Allow access to zone files .....	2
3.	Request for comment.....	2

## 1. Issue

The IETF is currently close to agreeing a set of new security extensions for DNS called DNSSEC. These extensions enable the use of secure signatures in responses from nameservers thereby giving people a greater degree of trust that the answer they have received is from the nameserver they were expecting it from.

DNSSEC includes a mechanism for proving that a domain name does not exist within a zone file called the NSEC record (previously the NXT record). Each domain name has an NSEC record associated with it that holds the name of the next domain name in the zone file in alphabetical order.

So if you asked for the domain bb.co.uk the nameserver might respond (if it could talk) – “I’m sorry but bb.co.uk does not exist and just to prove it let me tell you that the name before that does exist is aa.co.uk and the next one after that is cc.co.uk. So as you can see there is nothing in between, which is where bb.co.uk would be if it did exist.”

The problem is that someone can carry out a data mining attack that enumerates any DNSSEC secured zone file by iteratively querying for the NSEC record of each domain name. We do not currently provide anyone with a full copy of the zone file as this is our intellectual property. The old PRSS system does allow people to derive the zone file but this is being replaced with a new system that will not provide enough information to do this.

Stopping people from doing this enumeration is only really possible if they do it all from one computer and in quick succession. If someone wants to find a way around our detection mechanisms then they will always be able, for example by spreading queries across multiple computers and doing them slowly.

Currently we only intercept requests to the nameservers in serious cases, not as a matter of course, as doing so introduces latency that affects the response the end user gets from our nameservers. To stop this enumeration from happening even for the trivial case above would require such constant interception.

## 2. Possible Solutions

### 2.1 Adopt DNSSEC but do nothing else

This is currently the default option as the adoption of DNSSEC has been agreed as strategy. However it would lead to inevitable data mining and a need for us to respond to protect our intellectual property.

### 2.2 Not adopt DNSSEC

Whilst DNSSEC has taken a long time to develop it is seen as very important and is likely to gain widespread adoption when finalised. Not adopting would leave us out on a limb.

## **2.3 Change DNSSEC**

We have maintained a watching brief on these issues for a long time but missed the opportunity to intervene at an early enough stage in the development of this protocol. It is unlikely that we would have succeeded if we had tried.

The possibility remains that enough TLDs begin to recognise this issue and together force a change but there are currently no signs of this happening. Some of the gTLDs already allow access to their zone files through a specific programme.

## **2.4 Allow access to zone files**

This would mitigate though not eliminate the problem if access were sufficiently straightforward. There are a variety of possible mechanisms for providing this facility, from the more favourable of a special contract through to the less favourable of allowing open zone file transfers.

## **3. Request for comment**

The CoM asks the PAB for views on the policy implications of this subject, especially on the possible solutions described above or other solutions so far not mentioned. In particular the CoM asks whether the PAB feels that the current policy of no access to zone files should be reviewed or alternative remedies to this problem sought.