1 Introduction

A DNSSEC Check Proxy is a software program that can read a signed zone and performs some checks. Based on the outcome of these checks, one can decide whether to serve the zone or not.

The reason to develop such a tool is to minimize the number of DNSSEC problems. Recently, some organizations that have deployed DNSSEC encountered issues, which caused them to serve badly signed zones. The DNSSEC Check Proxy must prevent badly signed zones to reach the public, secondary name servers.

2 Requirements Version 1

- Configuration Options:
  1. It MUST be possible to specify the zone or zones for which the tool is to perform checks.
  2. It MUST be possible to specify a set of trust anchors for each zone.
  3. It SHOULD be possible to set an allowed safety margin for the RRSIG expiration times.
  4. It SHOULD be possible to set a required offset for the RRSIG inception times.
  5. It SHOULD be possible to set a minimum level on the RRSIG lifetime (expiration - inception).
  6. It SHOULD be possible to extend the configuration options.
• Zone Access:

1. It MUST be possible to read a zone from a zone transfer (AXFR).
2. The tool SHOULD read a zone from a zone transfer after being notified (DNS NOTIFY) of its change.
3. It MAY be possible to use an ACL to determine where the transfer should come from.

• Zone Serving:

1. The tool MUST be able to serve a zone through the means of a zone transfer (AXFR).
2. After a zone is found to be well, the tool SHOULD announce the availability by means of DNS NOTIFY.
3. It MAY be possible to use an ACL to determine where the transfer should go to.

• Zone Checking:

1. The following records MUST be checked at the zone apex : DNSKEY, SOA and NS.
2. Authoritative records below the zone apex SHOULD be checked.
3. It MUST be possible to check a random sample set of authoritative records.
4. The check on a RRset includes the following:
   - If a trust-anchor is known for the zone, the RRset must be validated with that trust-anchor.
   - An option MUST be available that specifies whether the network may be accessed by validating with a trust-anchor.
   - The signature MUST be verified using one of the DNSKEYs at the zone apex.
   - The RRSIG expiration MUST be checked to ensure it is in the future.
   - The RRSIG expiration SHOULD be checked to ensure it is higher than the current time minus a safety margin.
   - The RRSIG inception MUST be checked to ensure that the it is in the past.
   - The RRSIG inception SHOULD be checked to ensure that the it is lower than the current time minus an offset.
   - The RRSIG lifetime SHOULD be checked to ensure it is higher than a minimum level.
5. It MUST check if the Denial of Existence Chain (NSEC or NSEC3) is complete.
6. It MUST be possible to extend the procedure with third-party checks.
   – Checks might only be interested in modification of certain zones or even just certain parts of a zone. For example a check that tests if a name has no other RR than a CNAME (RRSIGs disregarded) might only be fired when a change involves a CNAME. There SHOULD be a framework that allow the configuration of what checks are fired under what circumstances.
   – Checks SHOULD be able to query the zone to be served using the DNS protocol.
   – Inter check dependencies and parallelization of checks SHOULD be taken into account.

3 Requirements Version 2

• General Requirements:

   1. All the requirements for version 1 MUST also be provided in version 2.
   2. Changes to a zone in version 1 are handled per whole zone. This means that version 1 is quiet serviceable for situations in which there are many small zones (like with ISPs), but less suitable for handling a few big zones (Like with Top Level Domain registries or Regional Internet Registries authoritative for sections in-addr.arpa. and/or ip6.arpa). In version 2 of DNSSEC Check Proxy the granularity of handling changes will be more refined to extend the usefulness to big zones.

• Zone Access:

   1. In addition to AXFR, the tool MUST be able to read a zone from an incremental zone transfer (IXFR).
   2. It MAY be possible to read a zone through Dynamic Update.
   3. It MAY be possible to read a zone from disk (for example from a zonefile).

• Zone Serving:

   1. In addition to AXFR, the tool MUST be able to serve a zone through the means of an incremental zone transfer (IXFR).
   2. It MAY be able to serve the zone as a Dynamic Update.

• Zone Checking:

   1. The interface towards checks MUST be extended in the therefor in version 1 designed canonical way to handle parts of a zone to be passed in.
4 Approach

For version 1, the design is to fork of NSD3 and facilitate a hook in between zone reception (via AXFR) and serving. NSD3 already has the functionality to transfer and serve a zone, with ACL if necessary. The hook will be used to call a program or a script with arguments and environment variables that provide information on, the calling NSD3 instance, which zone should be assessed, and what has changed. The program will operate a framework which schedules what checks to run in what order. NSD3 should already serve the zone to be assessed to and only to those checks.

The ldns-verify-zone tool has basic functionality to do checks on a signed zone. It will be extended with the functionality described in item’s 1 .. 4 of the requirements and used as a check in the framework.

The ldns-verify-zone tool will be adjusted so that it will have:

- Support for trust-anchors.
- More command line parameters for more elaborate inception and expiration time checking.

Currently ldns-verify-zone reads a zone in memory completely before assessing the records within. This is adequately for many small zones, but is not ideal for big zones. Also, zones could already be sorted when received via AXFR\(^1\), which could be exploited by ldns-verify-zone using a sliding window technique. A zone will then be assessed name by name while reading which is expected to have good impact on the performance.

When a verified AXFR is received, NSD3 might notify another “public” nameserver that may then choose to load the zone from DNSSEC Check Proxy via AXFR, or from the original master. Although in the latter case one has to be careful that AXFRs can also be performed when no notifies have been received.

In version 2, ldns-verify-zone needs to be adjusted so that it can have:

- Incremental zone checking.

For version 2, NSD3 is not suitable to use anymore, since the name server does not support IXFR out. The framework should then be integrated with the OpenDNSSEC adapters. The OpenDNSSEC adapters are currently under development. They have a small, straight forwarded API, to make it possible to access and serve a zone in any kind of format, including IXFR.

The check scheduling framework with the improved version of ldns-verify-zone should be combined with the OpenDNSSEC adapters to become the stand-alone DNSSEC Check Proxy tool.

---

\(^1\)NSD3 transfers its zones sorted