DNSSEC @ root level

Roy Arens Ondrej Filip Eberhard W Lisse

October 31, 2007

Abstract

On 2007-06-12 RIPE NCC on behalf of its DNS Working group sent a letter to ICANN with a request to sign the DNS root zone. This material was discussed among others in the ccNSO community and the ccNSO council asked the Technical Working group of the ccNSO for consultation on this issue. The purpose of this document is to explain the basic concepts in this area and form the basis of a discussion in the Technical Working group and the TechDay in Los Angeles.

1 DNSSEC

The Domain Name System Security Extensions (DNSSEC) have gone through several iterations since they were introduced in January 1997 (RFC 2065). The current DNSSEC (RFC 4033/4034/4035) specification is stable, and has been successfully deployed by various registries.

The DNS is one of the oldest standards, and is a key element to todays' Internet infrastructure. The DNS is an hierarchical structure, with the root and the top level domains as its most visible part. Though stability and availability of the DNS infrastructure is important, it lacks any means to certify the authenticity of data. DNS resolvers have no means to cryptographically verify the validity of received data.

In short, this means that any traffic can be diverted by means of spoofing DNS data. DNSSEC fixes this problem and adds strong security mechanism to assure data integrity and authenticity. This service is provided to security aware resolvers through the use of digital signatures. It acts as an additional layer, and makes sure that deployment of DNSSEC on the server side does not require deployment on the resolver side. In that sense, the DNSSEC is backwards compatible with the deployed base.

The principle behind the verification hierarchy of DNS data is analogous to that of resolving DNS data. A typical security aware resolver would have a trust anchor configured, analogous to having root-hints configured. This trust anchor enables verification of data associated with the trust anchor. The hierarchy of the signing keys follows the structure of the whole DNS system. Just like a resolver is capable of resolving from the root, through several layers to the desired

end point, a security aware resolver is subsequently able to verify data from the root, through several layers, to the end point, provided that all the data has been signed. Each zone would then typically have its own DNSKEY or trust anchor, signed by the parents' DNSKEY.

In the absence of a signed root zone, and thus a single entry point into the secured system, ccTLDs resort to making their trust-anchor available themselves. Though configuration of these trust-anchors is trivial, care must be taken keeping these trust anchors up to date. Since there has been successful deployment on the TLD level, there are now a plethora of trust anchors available for several zones, that all require tracking through several means of publication. It is clear that tracking many of these islands of security does not scale.

DNSSEC is fully compatible with traditional DNS. The signing of zones causes no problems to non-DNSSEC aware users. It should be noted, that the sole purpose for deploying DNSSEC is to guarantee the **validity** of resource records.

DNSSEC brings one potential problem for some registries in that the complete content of the zone is made available. This is known as the ***zonewalk*** problem. Additional work on DNSSEC is in progress to address that issue, but that has no impact on current deployments.

2 DNSSEC and the root

There are a few islands of security in today's Internet. Some TLD registries (for example .SE, .BG, .PR) started to sign theirs zones and deploy DNSSEC. It is highly likely that other TLD operators will follow them. As stated, the problem is that manually configuring and tracking a plethora of trust anchors does not scale. Using a similar analogy as before, it would be like every resolver operator to manually track all the name servers of every Top Level Domain in absence of a common root.

Therefore, a high demand for a single repository of keys exists. There are a two ways to create such single repository:

1. Sign the root zone, and publish signed pointers to trust anchors of the DNSSEC enabled TLDs.
2. Create an external repository outside the normal DNS hierarchy maintained by a trusted authority. Technology like a DNS Lookaside Validation (DLV) could be used for this purpose.

Signing the root zone seems to be a high political issue so at first sight the second solution looks easier. But in more detailed view there is no real advantage in that. From a security perspective, it is irrelevant whether the DNS resolver uses **pure** DNSSEC or DNSSEC **with** the DLV mechanism. However, the DLV mechanism is not a standard. There is an implementation by a vendor, but it is essential that DLV is standardized before other vendors implement this to avoid an incompatibility nightmare. Politically it is the same problem to find a trusted authority that will maintain the trusted repository (and sign it somehow anyway) as to find a trusted authority for signing the root zone.

From technical point of view, signing the root zone is not a problem. IANA have already declared to be technically ready for such step. Also, the ***zonewalk*** issue is not a problem for the root zone. The root zone is published in various formats, and its contents are well known. Operators without a mandate for DNSSEC do not need to change their domain maintenance. The same applies for end users (stub of recursive resolver operators).

3 IANA

Signing the root zone implies changing the technical processes that IANA has in place. The zone can be signed by IANA itself or by some other trusted organization. Such organization needs to be able to safely collect the public keys from TLD operators and to be able to publish them. The entity responsible for signing the root need to be able to manage trust anchors swiftly and securely. DNSSEC Keys have limited lifetimes and will be rolled frequently, and in case of a key compromise at the TLD level there is a need to amend the trust anchors for this TLD fast. This entity should be closely bound to publication of the root zone data, since cryptographic signatures are fairly volatile. This entity needs to be able to respond in a timely manner on a 24x7 basis to TLD Registries in case an emergency key rollover is needed.

4 Threats of Signing the root Zone

The DNSSEC protocol itself can bring a lot of new potential security problems as it will be needed to establish new procedures. The strength of entire security model is dependent on proper key management. Maintaining a signed zone introduces additional complexity, and risk of a human failure (or attack) is higher. Processes to swiftly and securely manage a signed zone and procedures to maintain trust relations with TLD registries need to be well established before actual deployment of either a signed root zone or a DLV trust anchor repository.

5 Recommendation

The ccNSO Working Group recommends that ccNSO Council requests ICANN/IANA to work towards having the Root zone signed (as soon as possible).