Introducing Root Zone Data Protections

Summary

Verisign, in its role as the Root Zone Maintainer (RZM), requests that RZERC develop and publish a document that explores the idea of introducing protections to root zone data. Such protections should allow a recipient of the zone data to verify that it has not been modified since its publication by the RZM.

Verisign believes that a method for verification of root zone data may be useful in the following ways:

- in the distribution of the root zone from the RZM to the root server operators (RSOs).
- to demonstrate that RSOs are not serving modified zone data, including the removal of, or addition of, TLDs to the root zone.
- when root zone data is served locally, as described in RFC 7706 or in ICANN's "hyperlocal root" initiative.

Detailed Scope of Work

Traditionally in the DNS, zone data is transferred between name servers using the "DNS Zone Transfer Protocol," also known colloquially as AXFR. This is the standard technique for delivering zone data from primary servers to secondary servers. In the root server system (RSS), AXFR is used to transfer the root zone from the RZM to the root server operators (RSOs).

The AXFR protocol alone provides relatively little to ensure data integrity. For this reason, the root server system uses "Secret Key Transaction Authentication," or TSIG, for zone transfers from the RZM. A TSIG key is simply a pre-shared secret. Its use in a zone transfer provides authentication, as well as data integrity checks. However, the protections afforded by TSIG are ephemeral, lasting only as long as the connection over which the data is transferred. Once the zone data is stored in memory or saved to a file on disk, the data is no longer protected by TSIG.

Since the root zone is signed with DNSSEC, one might expect that those signatures already provide sufficient data integrity. However, in DNSSEC none of the delegation NS records, nor their corresponding A and AAAA glue records, are signed. Furthermore, DNSSEC has been primarily designed to protect consumers of DNS responses (i.e., recursive and stub name servers, not entire zones as consumed by authoritative name servers.

Based on current activity within both ICANN (hyperlocal root) and the IETF (RFC 7706), we can expect the root zone to spread beyond its traditional deployment boundaries. There is likely to be growth both in the number of systems and devices serving root zone data, as well as the number of entities providing root zone transfer or download services. A reliable technique for verifying root zone content becomes important in this new model.

A proposal for such a technique, titled Message Digests for DNS Zones, is currently making its way through the IETF's RFC process.[1] This proposal embeds a cryptographic digest of zone data into the zone itself, with a new ZONEMD RR type. Deploying this for the root zone would necessarily require adding a ZONEMD record to the root zone.

We propose that RZERC discuss and investigate the general problem of securely protecting widely distributed root zone data, as well as the specific ZONEMD proposal.

[1] https://datatracker.ietf.org/doc/draft-ietf-dnsop-dns-zone-digest/