Recommendations for Adding Zone Data Protections to the Root Zone

Recent years have seen an increase in recognition of the root zone as a critical resource. As distribution of the root zone grows, both internal to the root server system (RSS), as well as external to it, questions arise regarding how to verify that the content of the root zone in someone's possession matches the content as originally published.

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, AXFR is used to transfer the root zone from the root zone maintainer (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.

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

The RZERC has discussed the idea of data protection for the root zone in general, and ZONEMD in particular. RZERC supports deploying ZONEMD in the root zone, subject to the following recommendations:

1) The root zone maintainer and root server operators should verify and confirm that the addition of a ZONEMD resource record will in no way negatively impact the distribution of root zone data within the RSS.

2) The IETF should carefully consider the ZONEMD draft document, draft-ietf-dnsop-dns-zone-digest, and follow established procedures for finalizing it as an RFC. Publication as an RFC is a prerequisite for adding a ZONEMD record to the root zone.

3) The DNS and Internet community should be made aware of plans to use ZONEMD in the root zone, and be given an opportunity to offer feedback. This may include technical presentations at meetings such as ICANN, DNS-OARC, NANOG, RIPE, etc.

4) Developers of name server software are encouraged to implement ZONEMD and consider enabling it by default for the root zone, hyperlocal root, and RFC 7706 deployments.
