DNSSEC Resolution Implementation Details

Author - Koushik Kumar Reddy Modugu

We start the series of queries from Root Servers up until the IP Address for the domain is observed in the Answer section of the query output or the labels (‘A’, ‘B’, ‘C’, ‘.’ for A.B.C) in the DomainName are extinguished, at which stage we end the program as no records are found.

DS (Delegation Signer) records in a zone implies that the children zones are DNSSEC enabled and establish the The Chain of Trust. Thus, while traversing the path from Root Server to the appropriate authoritative Domain, if a zone doesn’t have a DS record, we end the program returning ‘DNSSEC not Supported’ status.
In order to validate the DS records in a zone (server), Signed DS records are maintained in the zone (server) as RRSIG (DS) records. DS records are validated in every zone against signed DS records using ZSK of the zone. If validation fails, ‘DNSSEC Verification Failed’ status is returned.

At every zone, 2 queries are made -

1. UDP query to the current query server to retrieve the records of type A for the target Domain. Query output has 3 main sections - answer, authority and the additional sections capturing corresponding resource records.
    a. If the target domain’s IP address is available at the current server, it’ll be captured in the answer section of the query output. We then validate this IP address RRSet(A type) records against RRSIG (A) records. If validation succeeds we return the IP address else, return a ‘Validation failed’ Status.
    b. If the target domain’s IP address is not available at the current server, we consider the Name Servers in the authority section, for further querying. The IP addresses for these Name Servers are usually available in Additional Section. If not, we need to resolve the Name Servers and use their IP for further querying.
2. UDP query to the current server to retrieve the DNS Keys (ZSK and KSK) keys.
    a. If the DNS Keys aren’t present, either the input Domain is invalid (most likely) in which case all the (answer, authority and additional) sections will be empty or there’s an issue with server configuration. In which case, we return ‘Records Not found’.

b. If the DNS Keys are present, we validate the RRSet (DNS Key) against RRSIG (DNS Key).
c. We validate the KSK key of the current zone using the parent zone DS record. For this, digest of DS record is compared against the digest of the DS record generated utilizing KSK key with algorithm set to the digest type of the Parent DS record.

Finally, at any stage, if the verification fails, we stop and return the status. On the other hand, if we don't find the target domain's IP address, through a name server at a given zone, we move on to the next name server indexed in the zone, to find the target domain's IP address.