Name: Jai Anish Mehta SBU id: 114834757 Course: CSE 534 (FCN)

ASSIGNMENT 1/ HOMEWORK 1

PART B

For an example of this explanation, let's take the domain name to be resolved as **"www.googe.com."** .

[1] I send an iterative UDP query to the root server for www.google.com. With the wantdnssec and record type "A" parameter enabled to get the next address.
The other query I send is the one for com. to the root with the record type as DNSKEY.

[2] The response I get from the root server includes the authoritative name servers for the "com." zone, the DNSKEY records for the root zone along with the RRset, KSK, ZSK and RRsig of the root zone.
Additionally this response has the delegation signer records for the child zone i.e. the com. Zone. These DS records contain the hash, digest and fingerprint of the com. Zone and the RRsig of the DS record, which was signed by the root zone.

[3] If I don't get any of the requested information for validation and verification of the respective zones on sending the UDP query, I conclude that DNSSEC is not supported for that website.

[4] From the information I got in the response I verify the following:
DNSKEY RRset of the root zone is verified by decrypting its RRsig using its KSK.
DS record of root zone for com. is verified by decrypting its RRsig using the roots ZSK.
We already have the trusted copy of the root's KSK obtained directly from official website which needs to be matched with the one we got in response.

[5] If the above verification fails, I conclude that DNSSEC is configured but could not verified.

[6] Now I send an iterative UDP query for www.google.com to the com. server with the record type A.
The other query I send is the one for the google.com. with the record type as DNSKEY.

[7] The response I get from the com. server includes the authoritative name servers for the "google.com." zone, the DNSKEY records for the com. zone along with the RRset, KSK, ZSK and RRsig of the com. zone.
Additionally this response has the delegation signer records for the child zone i.e. the google.com. Zone. These DS records contain the hash, digest and fingerprint of the google.com. Zone and the RRsig of the DS record, which was signed by the com. zone.

[8] From the information I got in the response I verify the following:
DNSKEY RRset of the com. zone is verified by decrypting its RRsig using its KSK.
DS record of com. zone for the google.com. is verified by decrypting its RRsig using the com. zone's ZSK.
The com. zone is verified by comparing the digest of the com. zone's KSK with the previously obtained DS record from the root zone for the com. zone.

[9] If the above verification fails, I conclude that DNSSEC is configured but could not verified.

[10] Now I send an iterative UDP query for www.google.com to the google.com. server with the record type A.
The other query I send is the one for the www.google.com. with the record type as DNSKEY.

[11]The response I get from the google.com. server includes the authoritative name servers for the “www.google.com.“ zone, the DNSKEY records for the google.com. zone along with the RRset, KSK, ZSK and RRsig of the com. zone.
Additionally this response has the delegation signer records for the child zone i.e. the www.google.com. Zone. These DS records contain the hash, digest and fingerprint of the www.google.com. Zone and the RRsig of the DS record, which was signed by the google.com. zone.

[12]From the information I got in the response I verify the following:
DNSKEY RRset of the google.com. zone is verified by decrypting its RRsig using its KSK.
DS record of google.com. zone for the www.google.com. is verified by decrypting its RRsig using the com. zone’s ZSK.
The google.com. zone is verified by comparing the digest of the com. zone’s KSK with the previously obtained DS record from the com. zone for the google.com. zone.

[13]If the above verification is successful I conclude that validation and verification of DNSSEC is successful , otherwise if final verification fails, I conclude that DNSSEC is configured but could not verified.