Part B - DNSSEC Implementation Details

Allen Kim

For my implementation of DNSSEC, I check in a top-down approach from the root to make sure everything is valid on the way. There are three main possibilities: either the server I am querying does not support DNSSEC, the server implements DNSSEC correctly, or the signature given by the server fails to be validated.

We first assume that the root key is trustworthy when we query for it on the root server. This is the start of the chain of trust that the program verifies as it goes down the chain.

We first request the DNSKEY record for every zone we visit. The DNSKEY record provides us with a zone signing key (ZSK) and a key signing key (KSK). The KSK validates the ZSK, and the ZSK validates the signature we find in the actual query. Since we generally do not have our query answered by the top servers, they return a delegation of signing (DS) record that validates the DNSKEY of the domain of the child servers specified in its NS record. The DS record also comes with a corresponding RRSIG record that we verify with the ZSK to validate the DS itself. The verification follows from the DNSSEC module in the dnspython library. If the verification of these signatures fail, the program raises an error.

The DS record is then used to validate the DNSKEY record of the child domain. We do this by hashing the DNSKEY in a particular format as specified by the RFC, and then confirming that it matches the DS record of the parent. The hashes are constructed by turning the records into hexadecimal digits and then concatenating them with the domain name, which is done by a function I wrote into the program (probably there was a function I missed in the library). If the hashes do not match, the program raises an error that the validation failed. Otherwise, if they match, we know that the DNSKEY is legitimate, and we continue.

Finally, if we reach the answer, we will also get a RRSIG record that acts as its signature. By this point, the DNSKEY will have been verified by the parent's DS record, and thus, we can use the ZSK to verify that the RRSIG is a correct signature. If it is valid, we know we can trust the answer. If the program gets to this point, it returns the result as it normally would.