ERIKA BAILON
Homework 15

CSCI 3403
Daniel Massey

1. *From a terminal (unix, mac, windows, whatever), type the command "dig +dnssec com DNSKEY". Describe the steps you would take authenticate the DNSKEY of com (you may assume the root DNSKEY is known)*

    - First DNSKEY1 and DNSKEY2 will be returned signed by private DSNKEY which is the parent zone for *com*.
    - Since these signature were created with the private key, we now need the corresponding public key to verify((com DNSKEY1 DNSKEY2), signature RRSIG, public key 1).
    - Once we verified public key we ask the root. This one will return a hash and a a signature to verify the hash.
    - The root signs the signature, then verify((hash of com), signature RRSIG, public key 2 of root).
    - Then we try to ask root for the records of the keys - verify(root key1, key2, key 3, signature RRSIG, root key1). But we found that root key1 is configured into our browser in the trusted key file. This verifies that all the chain of trust up to the root are trusted since they are signed by root key1 which we trust.

2. *From a terminal (unix, mac, windows, whatever), type the command "dig +dnssec baa.darpa.mil". Describe the steps you would take authenticate the IP address of baa.darpa.mil*

    The steps are the same as question one. The only difference is to replace com with mil.

3. *Use the dig command to obtain all the DNSKEYs you need to authenticate the darpa.mil DNSKEY.*

    The commands we need to obtain all the DNSKEYs so we could authenticate were:

    - dig +dnssec darpa.mill DNSKEY
    - dig +dnssec mil DNSKEY
    - dig +dnssec . DNSKEY (to find the root)

4. *From a terminal (unix, mac, windows, whatever), type the command "dig +dnssec www.darpa.mil". Can you authenticate the IP address of www.darpa.mil Explain why or why not.*

    Yes we can because is an alias. Also, because it gives signatures, and it has the IP address from akamaiedge.net that is in DNS server for gov.

5. *Given the unsigned zone file below, suppose the DNS administrator decides to deploy DNSSEC and sign the zone using DNSSEC. If a resolver queries the signed zone for the A record (IP address) of "server.example.com, what record would be sent to securely prove that there is no host called "server.example.com."?*

    The records shown are:

    example.com

mail.example.com

mail2.example.com

mail3.example.com

ns.example.com

www.example.com

Would go between ns and www.

ns.example.com NSEC www.example.com

As you can see, server.example.com does not exist in that zone which is signed using DNSSEC, therefore, server.example.com does not exist.