Parker Eischen
December 13, 2018

Homework 15

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)*

    a. Request the RRset for 'com' which in turn, will also return the corresponding RRSIG
    b. Request the DNSKEY records for 'com' which contain the public ZSK and public KSK, this will return the RRSIG for the DNSKEY RRset
    c. Verify the RRsig with the public ZSK
    d. Verify the RRSIG of the DNSKey RRset with the public KSK
    e. If verified, everything proceeds as normal
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*

    What DNS would do

    a. Request the RRset for 'baa.darpa.mil'
    b. Try to find a RRset for zone darpa.mil
    c. The RR searches through the .mil domain server
    d. RR finds .darpa. In the domain server and searches for baa
    e. RR finds baa and sends the RR query to the domains name server thus confirming the DNSKEY and RSIG to provide the IP address of baa.darpa.mil

    How to authenticate in console

    f. Type dig +dnssec baa.darpa.mil
    g. In the Answer section there is an answer as follows 'baa.darpa.mil. 85788 IN A 192.5.18.135'
    h. 192.5.18.135 is the IP of the web server
    i. In the command line, use 'dig -x 192.5.18.135 +short'
    j. This command is used to reverse lookup an IP address to its domain main
    k. The command returned 'baa.darpa.mil' confirming it is authenticated
3. *Use the dig command to obtain all the DNSKEYs you need to authenticate the darpa.mil DNSKEY*

    a. **DNSKEY 1** 257 3 8 AwEAAbIwRPXs66IueHkuvY4SHdiMUQQP8nZ6FM5djokqxH58sqdowtz6

Y+0vktOvAqlNkAbW0F75Qb8MoOrg1Ehn+5S/IKypOuXzY1LSi2le4I7h
qjWCAIot+rlRp6oSruuEGN35qQRZdfyggaquo+XxLG2Ex1vNZagd1N15
XNFbUmu5On1ekRFl+VPAp0/bHUHFjQykwcZbwkEdxcaGq+0NhpXBYvs
F
itTWI3BsgGCwKG7FSyY91ICCBFKjio3XS8z6KuQ64w3Y9cCvwn3FyC1y
o/uhqGDkocKwaPz+GFtpoUpGEG75IaAIwE6jrDFfwQchF8XAzHkBihO5
/mkXwATVLtX0=

b. DNSKEY 2 256 3 8
AwEAAdmxfVrLS1w/JuPN3XHs51o13XEXJ+51X3RTGMRqACP3iHsoha
Ka
Eo/GH4mBUTMrMVbmU/4s14XHXFXlKW5QPbd0Bi+ZBtxSJ8srMCCEs6
eT E8tTmxoHjKo1tCU12Lr0gICrvBmd84e/GE7beZGJkk9I/BL/4yp0igNd
87CVWRLof5xICgY2MFyYvqxnE/u5zJfCBpC1QWpxBmDMnvo5HqBScqa
3 thON71NfFpLoCOHUqoeoIyrFU/NAejMhzLy1fiFVMThNdZfpuWig5PGM
ZLGFfu1OlVbjevvUQ6Gd4yasMjBq/fuUC59BHItTJQSLobbtpOdoaPOg
sihKDYnFjX0=

c. **DNSKEY 3** 256 3 8
AwEAAcy5V6La+cumuK8cw0Z+tprYrbzAI185/98K4Xb8paZPMX/ffBJr
jnd+k9Qf0qh7pi7Q68YizcUQP5OofOoIspfUqf5gaTSJZAcMcOwVeRkO
oIhXGodK3bz+0qx0ETu2I4M8RqbrgEttfeI0IpDZGPJcq2pCDXA3C1wN
ASpLXwN0X/gYAcLEUIFu2xn7WMEF9oANA5xFDYdrWFnAEOaS707u1y
aC
FIQfVwzSp3LzuLGj7HVtuVr3WoKRoo9gp9MWOHy/dxK/n3O0+F/rbmum
qrso9kiD+qbHKXUnh3s+zNfWX4JkC3IbyFkhQueyxYZwHBhtUkg745DC
SDetmvGqrqM=

4. *From a terminal (unix, mac, windows, whatever), type the command "dig +dnssec www.dapra.mil". Can you authenticate the IP address of www.darpa.mil Explain why or why not.*
    a. No we cannot. Using the provided command above, we find an IP address in the Answer Section of 184.29.145.176
    b. Now using dig to reverse lookup by inputting the command 'dig -x 184.29.145.176 +short' the result is 'a184-29-145-176.deploy.static.akamaitechnologies.com.'
    c. This is not the same web domain as www.darpa.mil, meaning this address cannot be authenticated. Unlike baa.darpa.mil and its address
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."?

a. If the host doesn't exist, it will return a NSEC(next secure record). If server.example.com doesn’t exist, the NSEC would be www. Or some record that exists earlier alphabetically between server-www. Without DNSSEC it would return an empty answer.