CSCI 3403 **Brennon Lee**
Homework 15 **Fall 2018, CU-Boulder**

1. From the 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)

   To authenticate DNSKEY of com, begin by running the command above to return the 3 com keys and RRSIG made by com private key 1. Next we verify the RSA (i.e. verify([key1,key2,key3], RRSIG, com pub key 1)). Now we need to verify com pub key 1 which we can get from the root DNSKEY (which we already know!). So we take that response and use the hash that was signed by root private key 2. ‘Verify(”hash”, RRSIG, root pub key 2)‘ and then hash(com pub key 1) and see if that equals the hash. Lastly, we need to verify the root pub key2 now. So running ‘dig +dnssec . DNSKEY‘ gives us 3 keys and the RRSIG signed by root private key 1. Next we call ‘verify([key1, key2, key3], RRSIG, root pub key 1)‘. This will authenticate the DNS of com

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

   To authenticate the IP address of ‘baa.darpa.mil‘, you begin by asking for the record for that domain. There is no reason to believe the response is legit so you must verify it by taking the RRSIG and the ‘darpa.mil‘’s public key 2 to verify the signature that was signed by the parent’s private key. But we need to verify the public key 2 so we get that via ‘Dig +dnssec darpa.mil DNSKEY‘. The response contains three keys that we need to verify which can do something like ‘verify([key1, key2, key3], RRSIG, darpa.mil public key 1)‘. But now we need to verify darpa.mil.public key 1 so we ask ‘mil‘ for key 1 via ‘dig +dnssec darpa.mil DS‘. This returns a hash of the darpa.mil public key 1 which was signed with private mil key 2. So now we can take the hash and use our verify function (i.e. verify(hash, RRSIG, public mil key 2)) which tells us if the hash was correct. If public key 2 is known, you can verify the hash via ‘hash(darpa.mil pub key 1) === prev˙has‘ and if that’s true, the public key 1 is correct and everything has been authenticated.

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

running ‘dig +dnssec darpa.mil DNSKEY‘ gives the following 3 keys and 3 signatures:

key1 - DNSKEY 257 3 8 AwEAAbIwRPXs66IueHkuvY4SHdiMUQQP8nZ6FM5djokqx Y+0vktOvAqlNkAbW0F75Qb8MoOrg1Ehn+5S/IKypOuXzY1LSi2le4I7h qjWCAIot+rlRp6oSruuEGN35qQRZdfyggaquo+XxLG2Ex1vNZagd1N15 XNFbUmu5On1ekRFl+VPAp0/bHUHFjQykwcZbwkEdxcaGq+0NhpXBYvsF itTWI3BsgGCwKG7FSyY91ICCBFKjio3XS8z6KuQ64w3Y9cCvwn3FyC1y o/uhqGDkocKwaPz+GFtpoUpGEG75IaAIwE6jrDFfwQchF8XAzHkBihO5 /mkXwATVLt8=

key2 - DNSKEY 257 3 8 AwEAAbIwRPXs66IueHkuvY4SHdiMUQQP8nZ6FM5djokqx Y+0vktOvAqlNkAbW0F75Qb8MoOrg1Ehn+5S/IKypOuXzY1LSi2le4I7h qjWCAIot+rlRp6oSruuEGN35qQRZdfyggaquo+XxLG2Ex1vNZagd1N15 XNFbUmu5On1ekRFl+VPAp0/bHUHFjQykwcZbwkEdxcaGq+0NhpXBYvsF itTWI3BsgGCwKG7FSyY91ICCBFKjio3XS8z6KuQ64w3Y9cCvwn3FyC1y o/uhqGDkocKwaPz+GFtpoUpGEG75IaAIwE6jrDFfwQchF8XAzHkBihO5 /mkXwATVLt8=

key3 - DNSKEY 257 3 8 AwEAAbIwRPXs66IueHkuvY4SHdiMUQQP8nZ6FM5djokqx Y+0vktOvAqlNkAbW0F75Qb8MoOrg1Ehn+5S/IKypOuXzY1LSi2le4I7h qjWCAIot+rlRp6oSruuEGN35qQRZdfyggaquo+XxLG2Ex1vNZagd1N15 XNFbUmu5On1ekRFl+VPAp0/bHUHFjQykwcZbwkEdxcaGq+0NhpXBYvsF itTWI3BsgGCwKG7FSyY91ICCBFKjio3XS8z6KuQ64w3Y9cCvwn3FyC1y o/uhqGDkocKwaPz+GFtpoUpGEG75IaAIwE6jrDFfwQchF8XAzHkBihO5 /mkXwATVLt8=

RSSIG 1 - RRSIG DNSKEY 8 2 302400 20181218225351 20181211220726 55599 darpa.mil. uwp02bSnGco513FjqQoA87E8RqFhD5MAwmKoPtJQsrwl7lmiPwAw WaXCMN2dfWomZb6qJZAlJ22C9c255c3JwD6OY1a9PsMUsSoIWLLnL0kO 9eygBrPpqvE95v66IIdm++yWvYYU8Z0XPZa9JIE7a5Xvk7m34+RTCm5Z VkW9G0A+M8rwbOckBOHLG0RuurGSLa0C8/EECQkOTFWB2BwVyLURsVO/ 8PVuhj66jcFBH4OZfRu6y4RpmvwbK46o9WyK9cy9f9tnoggnZXTwcj3O BpPH1ODm bcZEPw==

RSSIG 2 - RRSIG DNSKEY 8 2 302400 20181218225351 20181211220726

4975 darpa.mil. mt0xo/JwYDmUqJZNIaZY+rQfdOh+lPl9zaaQerBVIqnCcNCi/shsoQ
81/Pe0pQp6s1JONH8KIvxBC7MwsDwSrnbVlgHknzgUSeBSxf5gXTIZSU vaKfVsbWP5Ngl3UFpDNwPbhS8XmjmZBgMJdlgaWJPkFUNdVZPchgdo+E
4laSqJxxRdyH7qvwK2rhISjVfjTNPs/3CclzGWRg3SgOS3sadKVQvVyv 9/IaJsGCzpeo48ug+jEmbiMCPdNanV2JPmizKWXm/0oXsfrgmmmjZteQ RkNkcQDXGbDNc/6UqsuGJ6qgdVD5iVcE3x8QUgXk67f6AdzG/Al+cpCe qLscnw==

RSSIG 3 - RRSIG DNSKEY 8 2 302400 20181218225351 20181211220726
36843 darpa.mil. Wz9LeUdGEePLLZxQ6beNySdjSmkR5Z/1zsza+F6zEv8MdhqFzRJL
vZu1Ib2VW7rcZen2j6Ki0daG1bFKmDokarI1Xep0CIoFntTG3gDCD89Z xuiEJvtKjl32v
eJR2c6RCzngIpPvex+zRqR22CtbfZ1ib27hGtF1IfEQElmfA2v2dVrEs ErLZOkSRrW5c7K9JHBzIRd6LbPhpqIxdQQ3OFfHOmcCD8aVR018VNog/ 1K9VOYZ0K
uHUovg==

Next we need mil's record which is found by: ‘dig +dnssec mil DNSKEY‘ and gives the following 5 authority responses

RRSIG SOA 8 0 86400 20181225210000 20181212200000 2134 . LeXTKc+2ovLnBH5cEN
AoKBJ5/DGEC6q1YsiFoatbEeuuoXyTb6BvrbFtS5yyzU010+CqX4/pMD glnav9ARem
g/HeqwkmMYwatq4k/6b+VE1oMZ5XR9SWi4WvSCNHrpuBTG5NILend2Mx
Zy0l4P2KKTgpNRsaXb7iCtEpqpG+iflfd/AdU+i3K38dDYh3i1Nf398P o0niRXiC8dN1
BDJNfQ==

NSEC do. NS DS RRSIG NSEC

RRRSIG NSEC 8 1 86400 20181225210000 20181212200000 2134 . FLfoN3VXJzpZGP6/H4lBb/h/cXyjAUMZTX5AuUgZbcGU6YO7qAXkYcrq rpvMqLO6M
M8MvTiajnwMj1M5UH2HZpPwYqiDmxVSUHt96E37tJKw83O0B8nu4tb/c
jjktetUSQULi09E0lHHiyEWDTujRPBXiLMcr9TARLYErMEbvNHgUsNck
cl8DUmVtwkYPOad948L3dihafAH3wSb1UZg/6p83DrlaSILpr69fEsAS nzJObNiBezAAl+/lscjcwnA/gKLRdmjPMAcOnkRH9hdxxq0aGxED/Ak1 P22/Ig==

NSEC aaa. NS SOA RRSIG NSEC DNSKEY

RRSIG NSEC 8 0 86400 20181225210000 20181212200000 2134 . pFQ5IN7eg326hrc1wR
6ieiO6TKG+5UX6TmxXBFXOsI6Dj/vlX3tFYsiZxW5QPMV9X8Ijtr6fuQ khEM+BrV

**uWgh2HS7H8FE+vMAGn0+2fzcShR1fn45q8GUo1da876wTpm1xZY3klhW
uRkSy7S0+Gwuk/hh2Py/JkSz2I82CS/VknOcgiPjmDLigUou7eXP7ISj fcjfuRv+K+FKPKWWzBTK3m7hQsJGHHSeGBV1R3zr7LPzaXHgGqG6O1yc
zX1++A==**

which gives us all the keys we need to authenticate by following the steps in the previous problem.

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.

   We are given two records of RRSIG signed by ‘darpa.mil‘ so yes we can authenticate the IP address since we use the process described above and start by using the public key of ‘darpa.mil‘ to verify the signature of RRSIG and then follow the steps to authenticating the public key.

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 response should be the signed message ”next name after ns.example.com is username.example.com” which proves there is not only a server.example.com but also that the next address after ns.example.com is username.example.com with nothing inbetween.