Network Security III

Question 1 ***NSEC***

In class, you learned about DNSSEC, which uses certificate-style authentication for DNS results.

(a) In the case of a negative result (the name requested doesn't exist), what is the result returned by the nameserver to avoid dynamically signing a statement such as "`aaa.google.com` does not exist"?

(b) One drawback with this approach is that an attacker can now enumerate all the record names in a zone. Why might this be a security concern?

(c) Louis proposes to modify NSEC as follows. First, the site operator will take a hash of each domain that does exist. Then, the site operator proceeds as in NSEC: they sort the hashes and sign each adjacent pair. How can this be used to provide authenticated denial? How does this help mitigate enumeration attacks?

Question 2 ***TLS / DNSSEC***

(a) Oski wants to securely communicate with CalBears.com using TLS. Which of the following entities must Oski trust in order to communicate with confidentiality, integrity, and authenticity?

1. Oski's computer
2. CalBears.com's CA
3. All of the CAs that come configured into Oski's browser
4. All of the CAs that come configured into CalBears.com's software
5. The operators of CalBears.com
6. Cryptographic algorithms
7. Computers on Oski's local network
8. The entire network between Oski and CalBears.com
9. The operators of CalBears.com's authoritative DNS servers
10. The operators of `.com`'s Authoritative DNS servers
11. The operators of the Authoritative DNS root servers

(b) Suppose we didn't want to trust any of the existing CAs, but DNSSEC was widely deployed and we were willing to trust DNSSEC and the operators of the root zone and of `.com`. How could TLS be modified, to avoid the need to trust any of the existing CAs, under these conditions?

(c) Assume end-to-end DNSSEC deployment as well as full deployment of your change. Oski wants to securely communicate with CalBears.com using TLS. What changes are there to the list in part A (i.e., what must Oski trust in order to communicate with confidentiality, integrity, and authenticity)?

(d) Is this change good or bad? List at least one positive and one negative effect that would result from this change.