DNS and DNSSEC

Question 1 ***True/false***

Q1.1 Suppose we increase the entropy of the DNS ID field to 128 bits. It is infeasible for an on-path adversary to spoof a DNS answer.

○ True ○ False

Q1.2 True or False: A DNS lookup for `en.wikipedia.org` will always force the recursive resolver to send at least 3 DNS queries.

○ True ○ False

Q1.3 Suppose we increase the entropy of the DNS ID field to 128 bits. It is infeasible for an on-path adversary to spoof a DNS answer.

○ True ○ False

Q1.4 True or False: There is nothing a man-in-the-middle attacker (MITM) can do to interfere with a DNSSEC query.

○ True ○ False

Q1.5 True or False: Destination port randomization could be implemented to increase the security of DNS without breaking the DNS protocol shown in lecture.

○ True ○ False

Q1.6 True or False: In DNSSEC, if the root key is compromised, then no DNS records can be trusted.

○ True ○ False

Question 2

Alice is using a DNS resolver to perform a DNS lookup for `www.google.com`. A single, valid nameserver is authoritative for each of the following zones:

Zone	*Nameserver*
`.`	`a.root-servers.net`
`.com`	`a.gtld-servers.net`
`google.com`	`ns1.google.com`

Assume no other legitimate clients will query the resolver (but the adversary can query it if they wish), the resolver's cache is initially empty, and the resolver uses iterative querying.

Assume that in DNSSEC, no one will accept a record unless it has a valid signature.

The attacker is on-path between the resolver and `ns1.google.com`, but off-path to the other name servers. The attacker also knows when Alice makes a request. **Assume DNS uses a static source port known to the attacker**.

For each part, select all of the records that the attacker can poison.

Q2.1 Standard DNS is used.

☐ (A) Alice's cached A record for `www.google.com`

☐ (B) Resolver's cached NS record for `.com`

☐ (C) Resolver's cached NS record for `google.com`

☐ (D) Resolver's cached NS record for `.`

☐ (E) ——

☐ (F) ——

Q2.2 Standard DNS is used. Also, the resolver has a hardcoded NS record that maps the `google.com` zone to `ns1.google.com`, and a hardcoded A record with the IP address of `ns1.google.com`.

☐ (G) Alice's cached A record for `www.google.com`

☐ (H) Resolver's cached NS record for `.com`

☐ (I) Resolver's cached NS record for `google.com`

☐ (J) ——

☐ (K) ——

☐ (L) ——

Q2.3 The resolver and nameservers use DNSSEC, and Alice uses standard DNS.

☐ (A) Alice's cached A record for `www.google.com`

☐ (B) Resolver's cached NS record for `.com`

☐ (C) Resolver's cached NS record for `google.com`

☐ (D) —

☐ (E) —

☐ (F) —

Q2.4 The resolver and nameservers use DNSSEC, and Alice uses standard DNS. The adversary compromises `a.gtld-servers.net`.

☐ (G) Alice's cached A record for `www.google.com`

☐ (H) Resolver's cached NS record for `.com`

☐ (I) Resolver's cached NS record for `google.com`

☐ (J) —

☐ (K) —

☐ (L) —

Q2.5 The resolver and nameservers use DNSSEC, and Alice uses standard DNS. The adversary compromises `ns1.google.com`.

☐ (A) Alice's cached A record for `www.google.com`

☐ (B) Resolver's cached NS record for `.com`

☐ (C) Resolver's cached NS record for `google.com`

☐ (D) —

☐ (E) —

☐ (F) —

Q2.6 All parties use standard DNS, but the resolver and Alice encrypt their DNS messages with TLS.

☐ (G) Alice's cached A record for `www.google.com`

☐ (H) Resolver's cached NS record for `.com`

☐ (I) Resolver's cached NS record for `google.com`

☐ (J) —

☐ (K) —

☐ (L) —

Q2.7 All parties use standard DNS, but Alice, the resolver, and `ns1.google.com` encrypt their DNS messages with TLS.

☐ (A) Alice's cached A record for `www.google.com`

☐ (B) Resolver's cached NS record for `.com`

☐ (C) Resolver's cached NS record for `google.com`

☐ (D) —

☐ (E) —

☐ (F) —

Q2.8 All parties use standard DNS, but everyone encrypts their DNS messages with TLS.

☐ (G) Alice's cached A record for `www.google.com`

☐ (H) Resolver's cached NS record for `.com`

☐ (I) Resolver's cached NS record for `google.com`

☐ (J) —

☐ (K) —

☐ (L) —

Q2.9 Alice and the resolver use standard DNS, but encrypt their DNS messages with TLS. The resolver and nameservers use DNSSEC.

☐ (A) Alice's cached A record for `www.google.com`

☐ (B) Alice's cached NS record for `google.com`

☐ (C) Resolver's cached NS record for `.com`

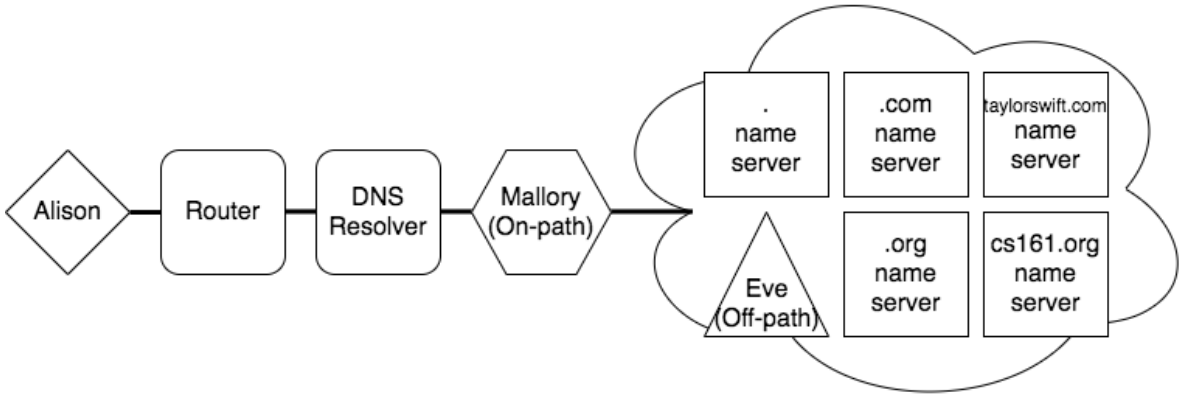
☐ (D) Resolver's cached NS record for `google.com`

☐ (E) —

☐ (F) —

Question 3 ***I Knew UDP Was Trouble***

In the following diagram, Alison is connected to the network through her local router, which is connected to the local DNS resolver, which in turn uses iterative queries to resolve domains. Ports and the random UDP ID numbers are 16 bits, and DNS queries use 53 as both the source and destination ports. Mallory is an on-path attacker, while Eve is an off-path attacker. `cs161.org`, `.org`, `.com`, and the root domain support DNSSEC, but `taylorswift.com` does not. DNS caches always start empty. Each subpart is independent.



Q3.1 Which of the following entities, if malicious, could poison Alison's DNS resolver's cache for `taylorswift.com`?

- ☐ (A) Mallory
- ☐ (B) Name server for `.`
- ☐ (C) Name server for `.com`
- ☐ (D) Name server for `.org`
- ☐ (E) Name server for `taylorswift.com`
- ☐ (F) None of the above

Q3.2 Which of the following entities, if malicious, could poison Alison's DNS resolver's cache for `cs161.org`?

- ☐ (G) Mallory
- ☐ (H) Name server for `.`
- ☐ (I) Name server for `.com`
- ☐ (J) Name server for `.org`
- ☐ (K) Name server for `taylorswift.com`
- ☐ (L) None of the above

Q3.3 Which of the following actions would be effective in preventing Mallory from having a non-negligible probability of being able to poison the cache for `taylorswift.com`?

☐ (A) Using TLS for all DNS queries

☐ (B) Using DNSSEC for `taylorswift.com`

☐ (C) Using TCP instead of UDP for the DNS query

☐ (D) Source port randomization

☐ (E) None of the above

☐ (F) ——

Q3.4 Which of the following actions would be effective in preventing Eve from having a non-negligible probability of being able to poison the cache for `taylorswift.com`?

☐ (G) Using TLS for all DNS queries

☐ (H) Using DNSSEC for `taylorswift.com`

☐ (I) Using TCP instead of UDP for the DNS query

☐ (J) Source port randomization

☐ (K) None of the above

☐ (L) ——

Q3.5 Which of the following actions would be effective in preventing a malicious `.com` name server from having a non-negligible probability of being able to poison the cache for `taylorswift.com`?

☐ (A) Using TLS for all DNS queries

☐ (B) Using DNSSEC for `taylorswift.com`

☐ (C) Using TCP instead of UDP for the DNS query

☐ (D) Source port randomization

☐ (E) None of the above

☐ (F) ——