Q1 *DNS over TCP (SU20 Final Q6)* **(20 points)**

Standard DNS uses UDP to send all queries and responses. Consider a modified DNS that instead uses TCP for all queries and responses.

Q1.1 (3 points) Which of the following does DNS over TCP guarantee against a man-in-the-middle attacker? Select all that apply.

- ☐ Confidentiality
- ☐ Authenticity
- ☐ Integrity
- ● None of the above

Solution: TCP has no cryptographic guarantees, so a MITM attacker can read and modify any message.

Q1.2 (3 points) Compared to standard DNS, does DNS over TCP defend against more attacks, fewer attacks, or the same amount of attacks against an on-path attacker?

- ○ More attacks
- ○ Fewer attacks
- ● Same amount of attacks

Solution: An on-path attacker can see all relevant header fields in TCP and UDP, so they only need to win the race against the legitimate response in both standard DNS and DNS over TCP.

Q1.3 (5 points) What fields does an off-path attacker ***not know*** and need to ***guess*** correctly to spoof a response in DNS over TCP? Assume source port randomization is enabled. Select all that apply.

- ■ TCP sequence numbers
- ■ Recursive resolver port
- ☐ DNS NS records
- ☐ Name server port
- ☐ DNS A records
- ○ None of the above

Solution: To spoof a TCP packet, the off-path attacker needs to guess the TCP sequence numbers and the randomized resolver port (source port). The name server port (destination port) is public and well-known. The DNS records can be anything the attacker wants, so there is nothing to guess there.

Q1.4 (3 points) Is the Kaminsky attack possible on DNS over TCP? Assume source port randomization is disabled.

- ○ Yes, because the attacker only needs to guess the DNS Query ID
- ● Yes, but we consider it infeasible for modern attackers
- ○ No, because the attacker cannot force the victim to generate a lot of DNS over TCP requests
- ○ No, because TCP has integrity guarantees

Solution: The attacker would have to guess at least 32 bits of sequence numbers on top of the transaction ID, for a total of 48 bits per attempt.

Q1.5 (3 points) Recall the DoS amplification attack using standard DNS packets. An off-path attacker spoofs many DNS queries with the victim's IP, and the victim is overwhelmed with DNS responses.

Does this attack still work on DNS over TCP?

- ○ Yes, the attack causes the victim to consume more bandwidth than the standard DNS attack
- ○ Yes, the attack causes the victim to consume less bandwidth than the standard DNS attack
- ○ No, because the DNS responses no longer provide enough amplification
- ● No, because the attacker cannot force the server to send DNS responses to the victim

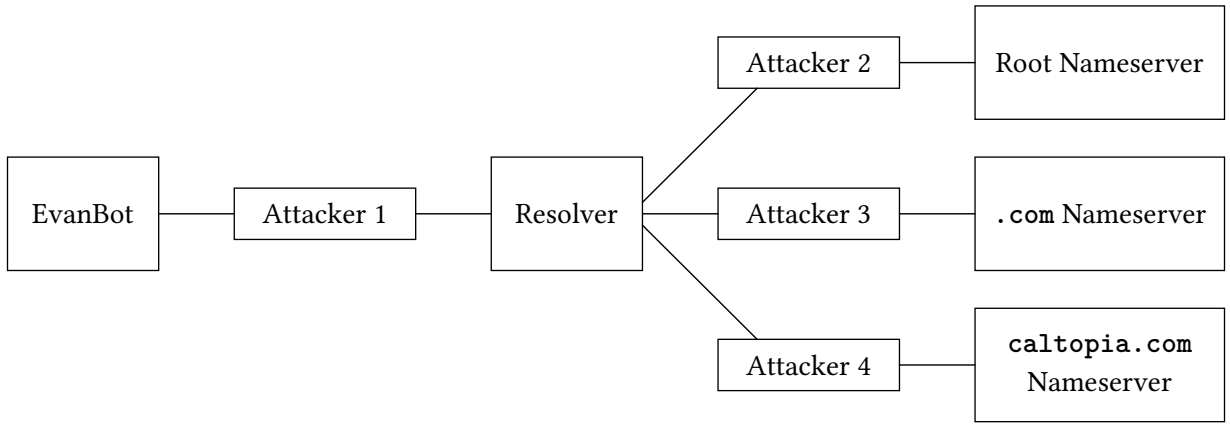
Solution: To force the victim to receive a DNS response, the attacker would need to initiate a TCP connection that looks like it's from the victim. However, an off-path attacker cannot do this, since they cannot see the SYN-ACK response sent to the victim.

Q1.6 (3 points) What type of off-path DoS attack from lecture is DNS over TCP vulnerable to, but standard DNS not vulnerable to? Answer in five words or fewer.

Solution: TCP SYN Flooding

Q2 *Caltopia DNS (SP21 Final Q8)* **(13 points)**

EvanBot is trying to determine the IP address of `caltopia.com` with DNS. However, some attackers on the network want to provide EvanBot with the wrong answer.



Assumptions:

- Each attacker is a man-in-the-middle (MITM) attacker between their two neighbors on the diagram above.
- No attackers can perform a Kaminsky attack.
- Standard DNS (not DNSSEC) is used unless otherwise stated.
- No private keys have been compromised unless otherwise stated.
- In each subpart, both EvanBot's cache and the local resolver's cache start empty.
- Each subpart is independent.

Clarification during exam: Assume that bailiwick checking is in use for this entire question.

In each subpart, EvanBot performs a DNS query for the address of `caltopia.com`.

Q2.1 (4 points) In this subpart only, assume the attackers only passively observe messages.

Which of the attackers would observe an `A` record with the IP address of `caltopia.com` as a result of EvanBot's query? Select all that apply.

■ Attacker 1 ☐ Attacker 3 ○ None of the above

☐ Attacker 2 ■ Attacker 4

Solution: The `A` type record is sent from the `caltopia.com` name server to the resolver, and then from the resolver to EvanBot.

Q2.2 (3 points) Which of the attackers can poison the local resolver's cached record for `cs161.org` by injecting a record into the additional section of the DNS response? Select all that apply.

Note: Attacker 1 has intentionally been left out as an answer choice.

- [x] Attacker 2
- [ ] Attacker 3
- [ ] Attacker 4
- ○ None of the above

Solution: `cs161.org` is in bailiwick for root, so Attacker 2 could add a record for `cs161.org` in the response from root.

However, `cs161.org` is not in bailiwick for `.com` or `caltopia.com`, so attackers 3 and 4 cannot add a record for `cs161.org` in the responses from `.com` or `caltopia.com`.

Q2.3 (4 points) Assume that the resolver and the name servers all validate DNSSEC, but EvanBot does not validate DNSSEC. Which of the attackers can poison EvanBot's cached record for `caltopia.com` by modifying the DNS response? Select all that apply.

- [x] Attacker 1
- [ ] Attacker 2
- [ ] Attacker 3
- [ ] Attacker 4
- ○ None of the above

Solution: Since the resolver and the name servers all validate DNSSEC, any attacker between the resolver and a name server can't do anything to inject malicious records. However, since EvanBot doesn't validate DNSSEC, Attacker 1 can inject a malicious `A` record.

Q2.4 (2 points) True or False: DNSSEC prevents Attacker 4 from learning the IP address of `caltopia.com`.

- ○ True
- ● False

Solution: DNSSEC provides no confidentiality over the DNSSEC records.