Weaver
Spring 2022

CS 161
Computer Security

Exam Prep 10

Q1 *DNS over TCP* (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.

☐ (A) Confidentiality ☐ (C) Authenticity ☐ (E) ——

☐ (B) Integrity ■ (D) None of the above ☐ (F) ——

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?

○ (G) More attacks ○ (I) Fewer attacks ○ (K) ——

● (H) Same amount of attacks ○ (J) —— ○ (L) ——

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.

■ (A) TCP sequence numbers ■ (C) Recursive resolver port ☐ (E) DNS NS records

☐ (B) Name server port ☐ (D) DNS A records ☐ (F) 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.

○ (G) Yes, because the attacker only needs to guess the DNS Query ID

● (H) Yes, but we consider it infeasible for modern attackers

○ (I) No, because the attacker cannot force the victim to generate a lot of DNS over TCP requests

○ (J) No, because TCP has integrity guarantees

○ (K) ——

○ (L) ——

Solution: The attacker would have to guess at least 32 bits of sequence numbers, which is the same defense as source port randomization in standard DNS.

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?

○ (A) Yes, the attack causes the victim to consume more bandwidth than the standard DNS attack

○ (B) Yes, the attack causes the victim to consume less bandwidth than the standard DNS attack

○ (C) No, because the DNS responses no longer provide enough amplification

● (D) No, because the attacker cannot force the server to send DNS responses to the victim

○ (E) ——

○ (F) ——

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 *DNSSEC-ZZSK* (38 points)

Several employees at Piazzzzza are gather to discuss the security of their DNS records. For the next 3 subparts, assume that all name servers use classical DNSSEC, as taught in lecture:

Q2.1 (3 points) Jinan, an employee, queries the root nameserver for the address of `piazzzzza.edu` and receives the following response:

```
edu.                 NS  a.edu-servers.net.
a.edu-servers.net.   A   6.14.6.03
```

TRUE or FALSE: Assume that DNSSEC records (not shown) are validated successfully. We can be sure that `a.edu-servers.net` may provide IP addresses for any domain ending in `.net`. Briefly justify your answer. I would turn this into potpourri.

○ (A) True ● (B) False ○ (C) —— ○ (D) —— ○ (E) —— ○ (F) ——

Solution: False. `.net` is just part of the domain name of the name server, not the types of records that the server provides.

Q2.2 (3 points) Suppose an attacker has obtained access to Piazzzzza's local firewall and may conduct **only** RST injection attacks.

TRUE or FALSE: The attacker has the ability to interfere with inbound and outbound requests that use DNSSEC. Briefly justify your answer. I would turn this into potpourri.

○ (G) True ● (H) False ○ (I) —— ○ (J) —— ○ (K) —— ○ (L) ——

Solution: False. DNSSEC uses UDP, not TCP

Jinan proposes to the CEO of Piazzzzza, Dr. Yang, a modified DNSSEC scheme called DNSSEC-ZZSK. Compared to the classical DNSSEC, DNSSEC-ZZSK adds in an extra key for each zone called the "zone-zone signing key" (ZZSK) and an additional DNSKEY2 record type that contains ZZSKs. Under this scheme:

- A zone's KSK is used to sign DNSKEY records which contain the zone's KSK and ZSKs (like classical DNSSEC).
- A zone's ZSK is used to sign DNSKEY2 records which contain the zone's ZZSK.
- A zone's ZZSK is used to sign the zone's other records, such as A records (like the ZSK in classical DNSSEC).

For the following subparts, assume DNSSEC-ZZSK is enabled. Suppose there are 3 name servers responsible for 3 zones: . (root server), .com, and piazzzzza.com, respectively.

I'd like to have some kind of question that has students reason about the path of trust. Maybe a question that says "fill in this table" similar to what is in lecture slides? And a question about "How many digital signatures need to be verified?" and "How many hashes need to be verified for DS records"

Q2.3 (5 points) How many digital signatures need to be verified when the resolver makes one request to root name server?

Solution: 3 signatures: one on KSK & ZSK, one on ZZSK, and one on records)

Q2.4 (5 points) How many digital signatures does the resolver need to verify to look up the IP address of www.piazzzzza.com (which is under the piazzzza.com zone)?

Solution: 9 signatures: for each name server: one on KSK & ZSK, one on ZZSK, and one on records). There are 3 name servers so 3*3=9

Q2.5 (5 points) How many hashes does the resolver need to verify to look up the IP address of www.piazzzzza.com (which is under the piazzzza.com zone)?

Solution: 2 hashes: since there are 2 designated signer (DS) records, one for .com, one for .piazzzza.com

Q2.6 (3 points) TRUE or FALSE: A Kaminsky attack is less likely to succeed against DNSSEC-ZZSK compared to classical DNSSEC. Briefly justify your answer.

○ (G) True ● (H) False ○ (I) —— ○ (J) —— ○ (K) —— ○ (L) ——

Solution: False. The Kaminsky attack relies on non-existant domain lookups, an extra key does not change that process at all. In particular, on-path attackers still just need to race the response, and an off-path attacker still need to guess the same number of bits (16 if no source port randomization, and 32 if yes)

Q2.7 (3 points) TRUE or FALSE: The NSEC3 protocol can still be implemented securely under DNSSEC-ZZSK, in a way that does not require the ZSK to sign anything other than the ZZSK. Briefly justify your answer.

● (A) True ○ (B) False ○ (C) —— ○ (D) —— ○ (E) —— ○ (F) ——

Solution: True. Just use ZZSK instead.

Q2.8 (3 points) TRUE or FALSE: It is still possible to enforce bailiwick checking under this scheme. Briefly justify your answer.

● (G) True ○ (H) False ○ (I) —— ○ (J) —— ○ (K) —— ○ (L) ——

Solution: True. The extra key does not change the bailiwick checking process

Q2.9 (3 points) True or False: DNSSEC-ZZSK defends against a greater number of attacks than classical DNSSEC. If you answer True, describe an attack that DNSSEC-ZZSK defends against that DNSSEC does not. If you answer False, briefly justify your answer.

○ (A) True ● (B) False ○ (C) —— ○ (D) —— ○ (E) —— ○ (F) ——

Solution: False. If KSK is compromised, both ZSK and ZZSK are compromised. If ZSK is compromised, ZZSK is compromised. In either case, we cannot trust the query result anymore. DNSSEC-ZZSK actually widens the attack surface. As a result, this protocol is not going to change the world at all :(

Q2.10 (5 points) Alice is making queries for `www.piazzzzza.com`. Which of the following keys, when only by itself compromised by an attacker, makes it such that Alice cannot trust the query result anymore? Assume that no records are cached, other than the KSK of the root nameserver. Select all that apply.

■ (G) ZZSK of the `piazzzzza.com` name server

■ (H) KSK of the `piazzzzza.com` name server

■ (I) ZZSK of the `.com` name server

■ (J) ZSK of the `.com` name server

■ (K) KSK of the root name server

□ (L) None of the above

Solution: TODO

This is the end of Q2. Leave the remaining subparts of Q2 blank on Gradescope, if there are any. You have reached the end of the exam.