CSc 361: Computer Communication and Networks (10:30-11:20 am, Oct 6, 2023)

Midterm Exam 1

Name: Student ID:

Closed-book exam. Nevertheless, a letter-sized, double-sided cheat sheet is allowed. Please read all questions [marks] on all the **three** pages first. **Duration: 50 minutes**

1. Please answer if the following statements are true or false. **Just answer true or false.**

   F (a) HTTP is a connection-oriented protocol. [3]

   F (b) HTTP messages must be sent over a TCP connection. [3]

   F (c) A reliable service must be connection-oriented service. [3]

   F (d) Connection-less services cannot be reliable services. [3]

   T (e) To achieve reliable service with TCP, the receiver must use ACK to confirm its correct reception of a segment to the sender. [3]

   F (f) In TCP socket programming in Python, the client program must call bind() before sending data to the server. [3]

   T (g) From the client point of view, the client does not know whether or not its TCP connection to a server uses TCP handoff. [3]

   F (h) Transport-layer protocols must provide end-to-end reliable service. [3]

   F (i) Every DNS root name server must use a globally unique IP address so that it can be discovered from any place in the world. [3]

   T (j) In any real-world TCP flow, if a segment's ACK flag bit is set to 1, the acknowledgment number in this segment should not be zero. [3]

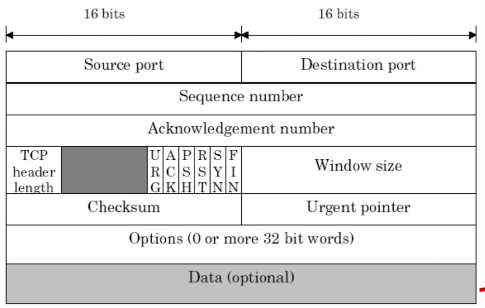
2. Assume that a web server received a TCP segment from a client having the TCP header shown in Figure 1. Answer the following questions:

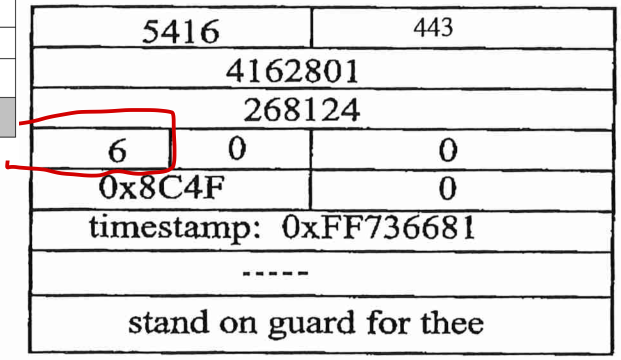
   (a) What is the size of the TCP header in terms of bytes? [5]

   24

   (b) After the server received this segment, will the server immediately send the next TCP segment to the client? If yes, what is the sequence number in the next TCP segment? If not, why? [10]

   NO. Window size = 0 means the Client cannot accept any data at this moment. The server thus cannot send any data to the Client until the server receives a segment from the Client that has the window size larger than 0.





5416		443
4162801		
268124		
6	0	0
0x8C4F		0
timestamp: 0xFF736681		
-----		
stand on guard for thee		

Figure 1: The content in the received TCP segment

(c) Is this segment for a https request? **Only answer yes or no.** [10]

Yes

(d) From this segment, can we tell the number of bytes that have been successfully received by the server for this TCP flow (i.e., the TCP flow which this segment belongs to)? It yes, write down the number. If not, just answer "unknown". [10]

unknown

3. Figure 2 shows TCP three-way handshake for establishing a connection. Fill the values at the places marked by "*". [10]

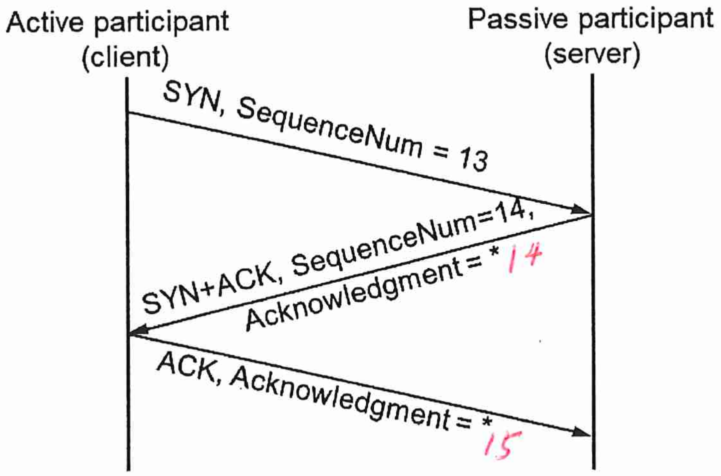


Figure 2: TCP three-way handshake

4. Figure 3 shows the flow of a DNS cache poisoning attack.

(a) Is Query 2*b* iterative or recursive ? [5]

iterative

(b) Assume that the victim nameserver receives the response 5 before all messages in 2*a*. Based on the response 5, will the victim nameserver cache a type A resource record (RR) for *www12345678.bankofsteve.com*? (**only answer yes or no**). [10]

NO

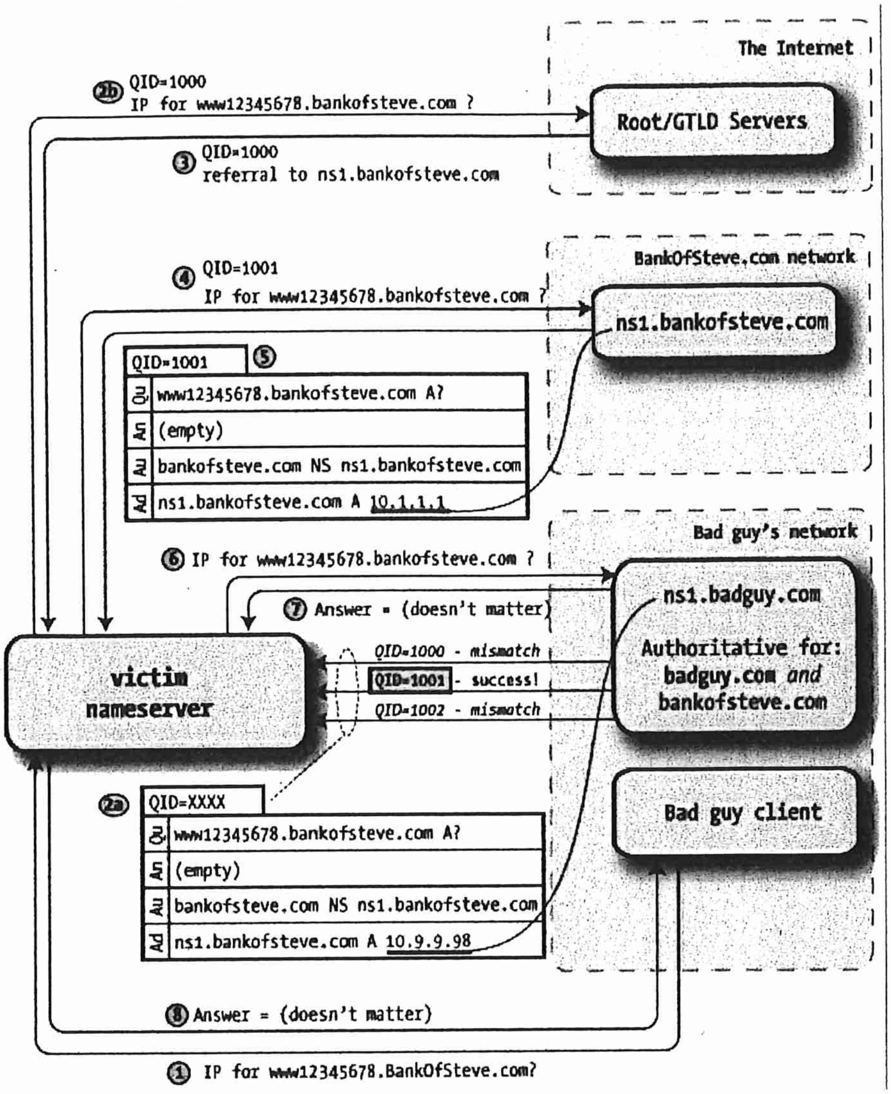

The Internet
Root/GTLD Servers
2b QID=1000
IP for www12345678.bankofsteve.com ?
3 QID=1000
referral to ns1.bankofsteve.com
BankOfSteve.com network
ns1.bankofsteve.com
4 QID=1001
IP for www12345678.bankofsteve.com ?
QID=1001 5
Qu www12345678.bankofsteve.com A?
An (empty)
Au bankofsteve.com NS ns1.bankofsteve.com
Ad ns1.bankofsteve.com A 10.1.1.1
Bad guy's network
ns1.badguy.com
Authoritative for:
badguy.com and
bankofsteve.com
6 IP for www12345678.bankofsteve.com ?
7 Answer = (doesn't matter)
victim
nameserver
QID=1000 - mismatch
QID=1001 - success!
QID=1002 - mismatch
Bad guy client
2a QID=XXXX
Qu www12345678.bankofsteve.com A?
An (empty)
Au bankofsteve.com NS ns1.bankofsteve.com
Ad ns1.bankofsteve.com A 10.9.9.98
8 Answer = (doesn't matter)
1 IP for www12345678.BankOfSteve.com?

Figure 3: Flow a DNS cache poisoning attack.

(c) Assume that the victim nameserver receives the response 5 after the messages in 2*a*. Write the missing part (marked by "-") in type A RR for ns1.bankofsteve.com. Ignore TTL marked by "*" [5]

(ns1.bankofsteve.com, 10.9.9.98 , A , *)

(d) If the attacker wants to hijack the traffic for *www.bankofsteve.com* to the fake server (IP address 10.9.9.98), what is the additional *Ad* entry that should also be included in the messages in 2*a* [5]

(www.bankofsteve.com A 10.9.9.98)