Name: Jaxson Billings

CSC 4200 Test 3
April **25th 5:30 PM** – April 2**8th 2023, 11:59 PM**
Total 75 Points

Q - 1. Determine the following statements if they are true or false. Right T (True) or F (False) on the Left Blank space. – 5 pts

1.1 __F___ Multimedia applications are less tolerant.

1.2 __T___ File transfer applications are delay tolerant.

1.3 __T___ Email application can tolerate loss.

1.4 __F___ Text messages need high bandwidth.

1.5 __F___ Efficient resource allocation would solve the congestion.

Q - 2. Short questions – 30 pts

a) What is min-max fair queuing in TCP? **- 3 pts**

Min-max fair queuing in TCP ensures that each flow is allocated a minimum guaranteed rate and can use additional bandwidth up to its maximum rate if available, preventing starvation and promoting fair bandwidth allocation.

b) In TCP slow start, why don't we start with a massive window? **– 3 pts**

In TCP slow start, we do not start with a massive window because it allows the sender to gradually increase its transmission rate and probe the network's capacity to avoid overwhelming it with a high initial transmission rate that could lead to congestion and packet loss.

c) If you had an insecure channel of communication where everything is intercepted, how would you use public key cryptography to secure your communication? - **3Pts**

Public key cryptography can secure communication in an insecure channel by using the recipient's public key to encrypt the message and ensuring only the recipient, with the corresponding private key, can decrypt it.

d) Difference between symmetric key cryptography and asymmetric key cryptography? Give one examples of each. **– 3 pts**

Symmetric key cryptography uses a single shared key for both encryption and decryption, making it faster and more efficient but requiring secure key distribution, while asymmetric key cryptography utilizes a pair of mathematically related keys (public and private) for encryption and decryption, providing secure key exchange but being slower computationally. An example of symmetric key cryptography is the Advanced Encryption Standard and asymmetric key cryptography is the RSA algorithm.

e) What are the four functions of network security? **– 3 pts**

The four functions of network security are prevention, detection, response , and recovery.

f) How does TCP congestion control differ from Flow control? – **3 pts**

TCP congestion control dynamically adjusts the sending rate to prevent network congestion, while TCP flow control regulates the transmission rate based on the receiver's buffer capacity to prevent overwhelming the receiver with data.

g) What is digital signature? Write the services provided by digital signature. – **3 pts**

A digital signature is a cryptographic technique that verifies a digital message or document. It provides services such as authentication, integrity, and prevents the signer from denying their involvement.

h) What service do the SSL, TLS and HTTPS protocols provide? In which Network layers do they work? – **3 pts**

The SSL and TLS protocols provide secure communication over the internet, ensuring encryption, authentication, and integrity of data transmitted between clients and servers. They primarily operate at the transport layer (Layer 4) of the network protocol stack, while HTTPS is an application layer (Layer 7) protocol that uses SSL or TLS for secure HTTP transactions.

i) Classify security attack. What is denial of service attack? – **3 pts**

A denial of service (DoS) attack is a security attack that aims to disrupt or disable the availability of a computer network, service, or website by overwhelming it with a flood of illegitimate requests or by exploiting vulnerabilities to consume system resources. It is typically carried out by flooding the target with excessive traffic or by exploiting weaknesses in the network or application infrastructure, rendering it inaccessible to legitimate users.

j) What DNS cache issues are involved in changing the IP address of, say, a web server host name? How might these be minimized? – **3 pts**

To minimize DNS cache issues when changing the IP address of a web server host name, lowering the TTL value of DNS records and instructing clients and resolvers to clear their caches can expedite the propagation of the new IP address.

Q – 3. If you have to divide 50Mbps available bandwidth between 5 clients, what would the allocation look like using min-max fair queuing? The client requests are: 20Mbps, 15Mbps, 10Mbps, 5Mbps, and 5Mbps. Write the numbers for each step. - **5pts**

Step 1

Client 1: 20Mbps - 10Mbps = 10Mbps (Deficit: 10Mbps)

Client 2: 15Mbps - 10Mbps = 5Mbps (Deficit: 5Mbps)

Client 3: 10Mbps - 10Mbps = 0Mbps (Deficit: 0Mbps)

Client 4: 5Mbps - 10Mbps = -5Mbps (Deficit: -5Mbps)

Client 5: 5Mbps - 10Mbps = -5Mbps (Deficit: -5Mbps)

Step 2

Client 1: 10Mbps + 5Mbps = 15Mbps

Client 2: 10Mbps

Client 3: 10Mbps

Client 4: 5Mbps

Client 5: 5Mbps

Q – 4. Find proper cipher text for **"Communication"** when $c = (p+6)$ – **5 pts**

C => I

o => u

m => s

m => s

u => a

n => t

i => o

c => i

a => g

t => p

i => o

o => u

n => t

The cipher is "Iusstagoout"

Q – 5. Suppose a congestion-control scheme results in a collection of competing flows that achieve the following throughput rates: 200 KBps, 160 KBps, 110 KBps, 95 KBps, and 150 KBps. **– 10 pts**

(a) Calculate the fairness index for this scheme**. – 5 pts**

Fairness Index = (sum of squared throughputs) / (sum of throughputs)

Sum of squared throughputs = (200^2 + 160^2 + 110^2 + 95^2 + 150^2) = 828,250 Kbps^2

Sum of throughputs = 200 + 160 + 110 + 95 + 150 = 715 Kbps

Fairness Index = 828,250 / (715^2) = 1.431

(b) Now add a flow with a throughput rate of 1000 Kbps to the above and recalculate the fairness index**. – 5pts**

Sum of squared throughputs = (200^2 + 160^2 + 110^2 + 95^2 + 150^2 + 1000^2) = 1,436,325 Kbps^2

Sum of throughputs = 200 + 160 + 110 + 95 + 150 + 1000 = 1715 Kbps

Fairness Index = 1,436,325 / (1715^2) = 0.485

Q – 6. What is *Originality* and *suppress-replay attack?* How can this attack be prevented? – **5 pts**

Originality refers to ensuring that messages or data exchanged between network entities are unique, untampered, and not replayed.

A suppress-relay attack refers to a type of cyber-attack where an one intercepts and prevents messages from reaching their intended destination while also relaying and possibly tampering with the intercepted communication.

To prevent suppress-replay attacks and ensure originality, measures such as using sequence numbers or timestamps, nonces, cryptographic techniques, session tokens or challenges, and time-based protections can be implemented.

Q – 7. Which of the following are sensitive to loss and/or delay? – 5 pts

a) file transfer
b) e-mail
c) Web documents
d) real-time audio/video
e) DNS query

Q – 8. Suppose that between A and B there is a router R. The A–R bandwidth is infinite (that is, packets are not delayed), but the R–B link introduces a bandwidth delay of 1 packet per second (that is, 2 packets take 2 seconds, etc.). Acknowledgments from B to R, though, are sent instantaneously. A sends data to B over a TCP connection, using slow start but with an arbitrarily large window size. R has a queue size of one, in addition to the packet it is sending. At each second, the sender first processes any arriving ACKs and then responds to any timeouts. **– 5 pts**

(a) Assuming a fixed TimeOut period of 2 seconds, what is sent and received for T = 0,1,...,6 seconds? Is the link ever idle due to timeouts? – 2.**5 pts**

At T = 0: A sends the first packet to R.

At T = 1: R receives the packet from A, and it immediately forwards it to B.

B sends an acknowledgment (ACK) to R.

A receives the ACK.

At T = 2: A sends two more packets to R.

At T = 3: R receives the first packet from A but can only forward it to B after the previous packet's delay.

B sends an ACK for the first packet to R.

A receives the ACK.

At T = 4: R receives the second packet from A and immediately forwards it to B.

B sends an ACK for the second packet to R.

A receives the ACK.

At T = 5: A sends four more packets to R.

At T = 6: R receives the first packet from the second batch but can only forward it to B after the previous packet's delay.

B sends an ACK for the third packet to R.

A receives the ACK.

The link is not idle due to timeouts because the Timeout period is set to 2 seconds, and all ACKs are received within that.

(b) What changes if TimeOut is 3 seconds instead? – 2.**5 pts**

At T = 3: R receives the first packet from A but can only forward it to B after the previous packet's delay.

B does not send an immediate ACK since it waits for the Timeout period of 3 seconds.

A does not receive the ACK.

At T = 4: R receives the second packet from A and immediately forwards it to B.

B still does not send an ACK for the first packet.

A does not receive the ACK.

At T = 5: A sends four more packets to R.

At T = 6: R receives the first packet from the second batch but can only forward it to B after the previous packet's delay.

B sends an ACK for the first packet and the second packet together to R, which is received instantly.

A receives the combined ACK.

The link has idle periods due to timeouts since B delays sending the ACK for the first packet, causing A to resend the packets after the Timeout period of 3 seconds has ended.

Q – 9. Discuss two problems or limitations of FIFO scheduling? How can you solve those issues? **– 5 pts**

Two problems of FIFO scheduling are the lack of prioritization and resource starvation. Both these can be solved by implementing priority-based scheduling algorithms. Techniques like Fair Scheduling or Round-Robin Scheduling can save resources better and prevent delays or resource starvation for tasks.