Midterm (1 hour)

1. Consider symmetric key encryption, public key encryption, hash function. Which encryption technique should you use for providing:

1) Confidentiality? (4 points)

Symmetric key encryption

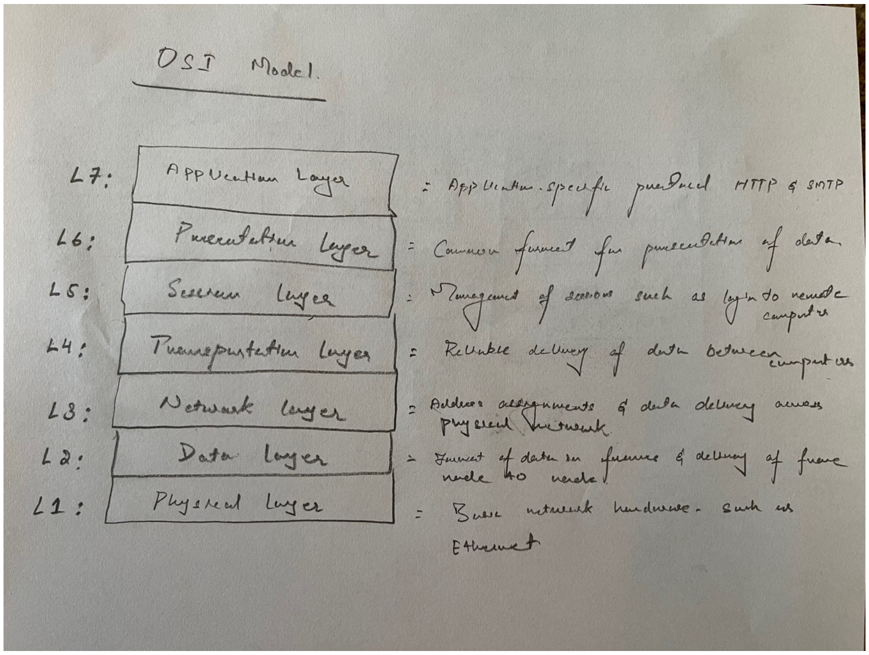
2) Message integrity? (3 points)

Hash function

3) Non-repudiation? (3 points)

Public key encryption

2. Draw the layered structures (including all layers' names) of OSI reference model and TCP/IP model. (10 points)



OSI Model.

L7: Application Layer : Application-specific protocol HTTP & SMTP

L6: Presentation Layer : Common format for presentation of data

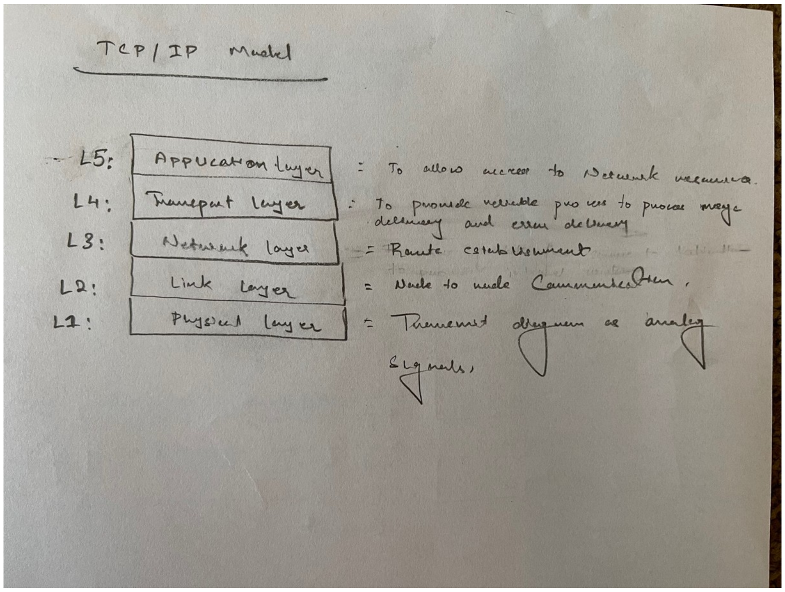
L5: Session Layer : Management of sessions such as login to remote computer

L4: Transportation Layer : Reliable delivery of data between computers

L3: Network Layer : Address assignments & data delivery across physical network

L2: Data Layer : Format of data in frame & delivery of frame node to node

L1: Physical Layer : Basic network hardware - such as Ethernet



TCP/IP Model

L5: Application layer : To allow access to Network resources.

L4: Transport layer : To provide reliable process to process message delivery and error delivery

L3: Network layer = Route establishment

L2: Link layer = Node to node Communication.

L1: Physical layer = Transmit digital or analog signals.

3. Alice needs to securely send a large amount of confidential video data to Bob. Since Alice's computer is slow, which of the following methods should she choose for achieving the best efficiency and confidentiality? RSA, AES-128, MD5, SHA1, cleartext. Why? (10 points)

AES-128 is the best method for symmetric key encryption as it is not feasible for hacker to compute the key. It can achieve confidentiality and encryption as well as efficiency. It is efficient because it's a slow computer and doesn't really require a lot of RAM.

4. Assume Alice would like to send message M with an one-time transmission. She encrypts in the following manner:

$$C1= Hash(M),\ C2= Enc\_{Kpub}(M)$$

Then ($C1,C2$) will be sent to Bob together. $Enc()$ denotes the encryption function. Kpub denotes the public key.

1) What security property, in terms of confidentiality, message integrity, and authenticity, could be achieved? (5 points)

-2

Hash provides integrity by ensuring the message hasn't been tampered with or modified and When it comes to security Bob will be able to decrypt the message using his Public key and Symmetric key. Alice uses her public key to encrypt the message. The public key provides Confidentiality.

2) In order to provide such security, whose public key is used. (5 points)

Public key is given to Alice by Bob. Bob's public key and Bob's private key is used to decrypt the message.

5. Assume Alice chooses a very uncommonly used encryption scheme to protect her message's confidentiality sent to Bob. She thinks since this scheme is not commonly used so there is no need to keep her key secret. Is her choice correct? If not, which of the '9-principles' is that against with. (10 points)

Open Design principle is violated. Alice is relying on her encryption scheme as secret rather than the key being secret. Open Design tells us that, security of a mechanism should not depend on secrecy of the design/implementation.

Least common Mechanism is also violated. Alice fails to protect her key by not keeping it secret. Least common mechanism is defined as a mechanism used to access resources should not be shared. Also has possible unsecured communication path.

6. A stream ciphertext received by Bob is this: 0010 1011 0101. The key is 1011 0101 1001. What is the plaintext? (10 points)

100111101100

7. A MySQL user account created for pulling records from a database doesn't need admin rights. Which 9-principles this is following? (10 points)

Principle of Least Privilege: An entity should be given only those privileges needed to complete its task.

8. TCP connect() port scanning will establish a connection with the target device. Such a behavior will be recorded by the target device. To avoid being recorded, what else **TCP** port scanning method could we use? (10 points)

Half Open Scan: Includes stealth through a SYN scanning or also known as half open scanning technique to develop the TCP connect() process. The SYN scan uses a changed handshake which includes a 2-Way communication channel while the TCP connect() method uses the complete 3-Way handshake to connect to a host port. The SYN search starts just as the TCP connect() method, by sending a packet with the SYN flag collection. In the same way, if the port is available, the server then returns a SYN/ACK packet to the recipient. When the port is unavailable, the recipient is given a RST (Reset) packet. Here the SYN and the TCP connect() method differ: the final ACK packet is never returned to the server to accept the SYN|ACK has been sent from the server from the client. Thus, the device avoid being recorded while also confirming if the server is listening on a particular port.

9. For the linux user login system, could an attacker figure out whether two users' passwords are the same? Why? Assume the attacker could have access to the system files that store user login information. (10 points)

-6

If the initial vector (IV) is known and the correct password is guessed than the attacker can figure out if the two users have the same password.

10. For Question 4, if Alice repeatedly sends different messages M1, M2, M3 .... to Bob using the same method, is there any security threat? If yes, why? (10 points)

Yes, because we could not establish authenticity. Bob is not able to confirm if the messages are really coming from Alice. Alice and Bob are vulnerable to man-in-the-middle attack. Alice should probably establish symmetric key encryption right after establishing public key encryption to share her private key. And now both Alice and Bob can communicate with each other securely.

-3