Q.1(a)i) Computer security is a branch of computer technology known as information security as applied to computers and networks. The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users. The term computer system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively. The strategies and methodologies of computer security often differ from most other computer technologies because of its somewhat elusive objective of preventing unwanted computer behavior instead of enabling wanted computer behavior. (Upto This Much – 1Marks)

The computer of computer security has been threefold:

1. confidentiality,
2. integrity, and
3. availability **(Listing 1-Marks)**

The purpose of **confidentiality** is to ensure that only those individuals who have the authority to dew a piece of information may dc so. No unauthorized individual should ever be able to view data they are not en titled to.

Integrity is a related concept but deals with the generation and modification of data. Only authorized individuals should ever be able to create or change (or delete) information.

The goal of **availability** s to ensure that the data, or the system itself, is available for use when the authorized user wants it.

As a result of the increased use of networks for commerce, two additional security goals have been added to the original three in the CIA of security.

4. Authentication
5. Nonrepudiation

Authentication deals with the desire to ensure that an individual is who they claim to be. The need for this in an online transaction is obvious.

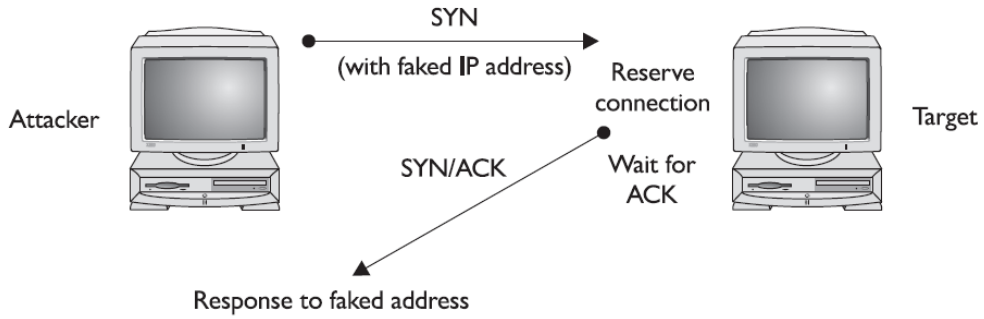
Nonrepudiation, which deals with the ability to verify that a message has been sent and received and that the sender can be identified and verified. The requirement for this capability in online transactions should also be readily apparent. **(Explanation – 2 Marks)**

Q.1 (a)ii) Denial of service (DOS) attacks can exploit a known vulnerability in a specific application or operating system, or they may attack features (or weaknesses) in specific protocols or services. In this form of attack, the attacker is attempting to deny authorized users access either to specific information or to the computer system or network itself.

The purpose of such an attack can be to simply prevent access to the target system, or the attack can be used in conjunction with other actions in order to gain unauthorized access to a computer or network. For example, a SYN flooding attack may be used to temporarily prevent service to a system in order to take advantage of a trusted relationship that exists between that system and another.

SYN flooding is an example of a DOS attack that takes advantage of the way TCP/IP networks were designed to function, and it can be used to illustrate the basic principles of any DOS attack. SYN flooding utilizes the TCP three-way handshake that is used to establish a connection between two systems.

In a SYN flooding attack, the attacker sends fake communication requests to the targeted system. Each of these requests will be answered by the target system, which then waits for the third part of the handshake. Since the requests are fake (a nonexistent IP address is used in the requests, so the target system is responding to a system that doesn't exist), the target will wait for responses that will never come, as shown in Figure .



The target system will drop these connections after a specific time-out period, but if the attacker sends requests faster than the time-out period eliminates them, the system will quickly be filled with requests. The number of connections a system can support is finite, so when more requests come in than can be processed, the system will soon be reserving all its connections for fake requests. At this point, any further requests are simply dropped (ignored), and legitimate users who want to connect to the target system will not be able to. Use of the system has thus been denied to them. **(upto This – 2 Marks)**

Following are types if Dos

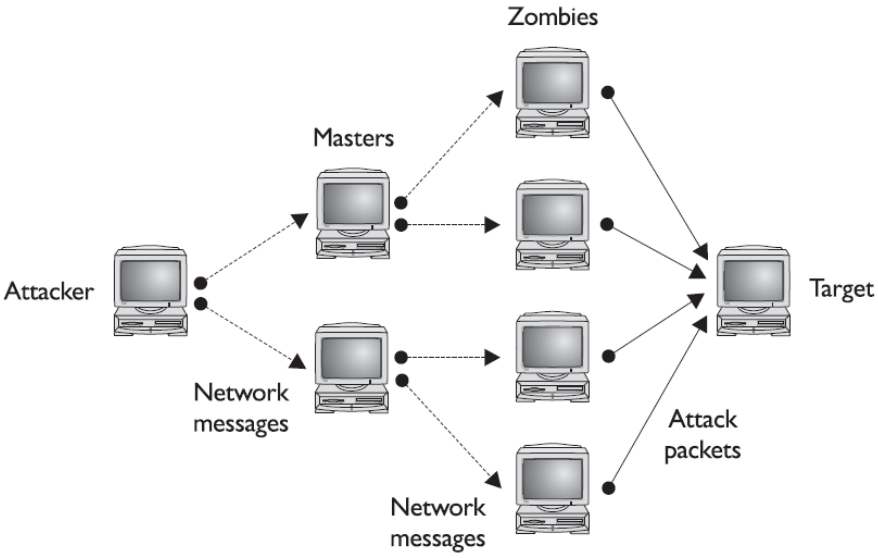
1.POD - ping-of-death

2. DDOS - Distributed Denial of Service attack

POD : In the POD attack, the attacker sends an Internet Control Message Protocol (ICMP) "ping" packet equal to, or exceeding 64KB (which is to say, greater than 64 * 1024 = 65,536 bytes). This type of packet should not occur naturally (there is no reason for a ping packet to be larger than 64KB). Certain systems were not able to handle this size of packet, and the system would hang or crash.

DDOS: DOS attacks are conducted using a single attacking system. A denial of service attack employing multiple attacking systems is known as a distributed denial of service (DDOS) attack. The goal of a DDOS attack is the same: to deny the use of or access to a specific service or system. DDOS attacks were made famous in 2000 with the highly publicized attacks on eBay, CNN, Amazon, and Yahoo.

In a DDOS attack, the method used to deny service is simply to overwhelm the target with traffic from many different systems. A network of attack agents (sometimes called zombies) is created by the attacker, and upon receiving the attack command from the attacker, the attack agents commence sending a specific type of traffic against the target. If the attack network is large enough, even ordinary web traffic can quickly overwhelm the largest of sites, such as the ones targeted in 2000. **(1Marks Each for POD and DDOS)**



Q.1 (a)iii)People are often in a hurry and will frequently not follow good physical security practices and procedures. Attackers know this and may attempt to exploit this characteristic in human behavior, **Piggybacking** is the simple tactic of following closely behind a per son who has just used their own access card or PIN to gain physical access to a room or building. An attacker can thus gain access to the facility without having to know the access code or having to acquire an access card.

Piggybacking, in a wireless communications context, is the unauthorized access of awireless LAN. Piggybacking is sometimes referred to as "Wi-Fi squatting."

The usual purpose of piggybacking is simply to gain free network access rather than any malicious intent, but it can slow down data transfer for legitimate users of the network. Furthermore, a network that is vulnerable to piggybacking for network access is equally vulnerable when the purpose is data theft, dissemination of viruses, or some other illicit activity.

To protect your network from piggybacking, ensure that encryption is enabled for your router. Use Wireless Encryption Protocol (WEP) if that's your only option, but if possible use Wireless Protected Access (WPA) or WPA2. Use a strong password for your encryption key, consisting of at least 14 characters and mixing letters and numbers.

Shoulder surfing is a similar procedure in which attackers position themselves in such away as -to be-able to observe the authorized user entering the correct access code. Both of these attack techniques can be easily countered by using simple procedures to ensure nobody follows you too closely or is in a position to observe your actions.

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand.

Q.1 (a)iv) (1mark for Each correct policy)

If users are assigned passwords consisting of eight randomly selected printable characters, password cracking is effectively impossible. But it is impossible for many users to remember their passwords. Even if we limit the password up to the strings of characters that are unforgettable, then the size is still too large to allow practical cracking.

There are four basic techniques are in use to reduce guessable passwords while allowing the user to select a password that is memorable.

a. **User Education**
b. **Computer generated password**
c. **Reactive password checking**
d. **Proactive password checking**

User Education

- Tell the importance of hard-to-guess passwords to the users and provide guidelines for selecting strong passwords.
- This strategy is unlikely to be successful at most installations, particularly where there is a large user population or a lot of turnover.
- Many users will simply ignore the guidelines, which may not be good judgment of what is a strong password. For example, many users think that reversing a word or making a last letter capital makes a password un-guessable.

Computer generated password

- Computer-generated passwords also have some problems. If the passwords are reasonably random in nature, users will not be able to remember it.
- Even though the password is pronounceable, the user may have difficulty in remembering it and so many times they write it down.
- Normally these schemes are less accepted by users. MIPS hug 279 defines one of the best-designed automated password generators. This standard includes not only a description of the approach but also a complete listing of the C source code of the algorithm.
- The algorithm generates words by forming pronounceable syllables and concatenating them to form a word. To produce a random number of characters, a random number generator is used, which construct the syllables and words.

Reactive password checking

- In this scheme the system periodically runs its own password cracker program to find out guessable passwords.
- If the systems find any such a password, then system cancels it and notifies the user.
- This method has a number of drawbacks - It is resource intensive if the job is done right. Because a strong-minded opponent who is able to steal a password file can dedicate full CPU time to the task for hours or even days.
- Furthermore, any existing passwords remain vulnerable until the reactive password checker finds them.

Proactive password checking

- It is the most promising approach to improved password security. In this scheme, a user is allowed to select his/her own password.
- However, at the time of selection, the system checks the password if the password is allowable then allow or reject it.
- Such checkers are based on the philosophy of enough guidance from the system; users can select memorable passwords from a fairly large password space that are not likely to be guessed in a dictionary attack.
- The trick with a proactive password checker is to strike a balance between acceptability and strength of user.
- If the system continuously rejects many passwords, then users will complain that it is very hard to select a password.
- If the system uses some simple algorithm to define what is acceptable, then it
- provides direction to password crackers to process their guessing technique.

Following are two possible approaches to proactive password checking.

1. The first approach is a simple system for rule enforcement, like:
   - All passwords must be at least eight characters long
   - In the password, there should be at least one uppercase, lowercase,
   - numeric digits, and punctuation marks
   - These rules will be attached with the help of user. Though this
   - approach is superior for educating users but it may not be sufficient to avoid password crackers. This scheme alerts crackers to not to try but still make it possible to do password cracking.
2. Another possible procedure is to compile a large dictionary of possible bad
   - passwords. When a user selects a password, then system checks the
   - password to make sure that it is not on the disapproved list. There are two problems with this approach
   - **Space:** The dictionary must be very large to be effective. For example, the dictionary used may occupy more than 30 megabytes of storage.
   - **Time:** More time is required to search a large dictionary. In addition, to check for likely variations of dictionary words, either those words more included in the dictionary, making it truly huge, or each search must also involve considerable processing.

Q.1 (b)i) Security threats to web sites and web applications (webapps) come in many forms. Data centres and other assets used for hosting web sites and their associated systems need to be protected from all types of threat. Threats should be identified using application threat modelling and then evaluated with a vulnerability assessment. Vulnerabilities can be removed or reduced and countermeasures put in place to mitigate the effects of an incident should the threat be realised. The main types of threats to web systems are listed below:

Physical

Physical threats include loss or damage to equipment through fire, smoke, water & other fire suppressants, dust, theft and physical impact. Physical impact may be due to collision or the result of malicious or accidental damage by people. Power loss will affect the ability for servers and network equipment to operate depending upon the type of back-up power available and how robust it is.

Human error

Errors caused by people include operator/user error such as accidental deletion of data or destruction of software programs, configurations or hardware. The other major error caused by people is leaving weaknesses (vulnerabilities) in software. This can include escalation of priviledges, authentication which can be bypassed, incorrect implementation of encryption, failure to validate input and output data, weak session management, failure to handle errors correctly, etc. Good programming practices can reduce the vulnerabilities which human error can exploit.

Malfunction

Both equipment and software malfunction threats can impact upon the operations of a website or web application. All assets required for the operation of the web system must be identified to be able to evaluate the threats. Malfunction of software is usually due to poor development practices where security has not been built into the software development life cycle.

Malware

Malware, or malicious software, comes in many guises. Web servers are popular targets to aid distribution of such code and sites which have vulnerabilities that allow this are popular targets.

Spoofing

Spoofing where a computer assumes the identity of another and masquerading where a user pretends to be another, usually with higher privileges, can be used to attack web systems to poison data, deny service or damage systems.

Scanning

Scanning of web systems are usually part of network or application fingerprinting prior to an attack, but also include brute force and dictionary attacks on username, passwords and encryption keys.

Eavesdropping

Monitoring of data (on the network, or on user's screens) may be used to uncover passwords or other sensitive data.

Scavenging

Examining 'found' data from accessible sources such as the network, search engines and waste. The actual target information could be found, but more often scavenging is used as a way to select other threats for vulnerabilities that are known to exist for the web system (e.g. operating system, firewall type, server software, application software).

Spamming

Overloading a system through excessive traffic can lead to denial of service for other users or system failure.

Out of band

Network attack techniques such as tunneling to access low level system functions can mean the target such as a router or server can be taken over. Once an attacker has control, this can be used to attack other assets required for the continued operation of a web site.

(Any 6points, 6-Marks)

The following table shows the type of security threats faced in using the web

	Threats	Consequences	Countermeasures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerability to all other threats	Cryptographic Checksums
Confidentiality	• Eavesdropping on the Net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	Encryption, Web Proxies
Denial of Service	• Killing of user threads • Flooding machine with bogus threats • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	Difficult to prevent
Authentication	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic Techniques

Q.1 (b)ii)

An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network.

IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. There are IDS that detect based on looking for specific signatures of known threats- similar to the way antivirus software typically detects and protects against malware- and there are IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat. We'll cover each of these briefly.

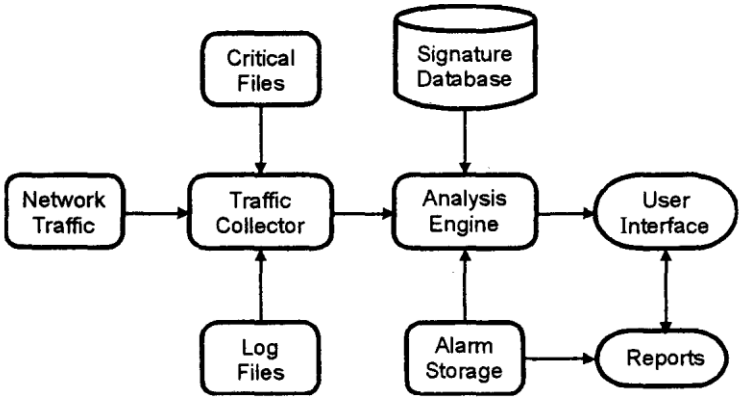
NIDS

Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. Ideally you would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network.

HIDS

Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected

Basic Components intrusion detection system (HIDS)



1.Traffic collector:

- This component collects activity or events from the IDS to examine.
- On **Host-based IDS**, this can be log files, audit logs, or traffic coming to or leaving a specific system.
- On **Network-based IDS**, this is typically a mechanism for copying traffic of the network link.

2. Analysis Engine:

- This component examines the collected network traffic & compares it to known patterns of suspicious or malicious activity stored in the signature database.
- The analysis engine act like a brain of the IDS.

3. Signature database:

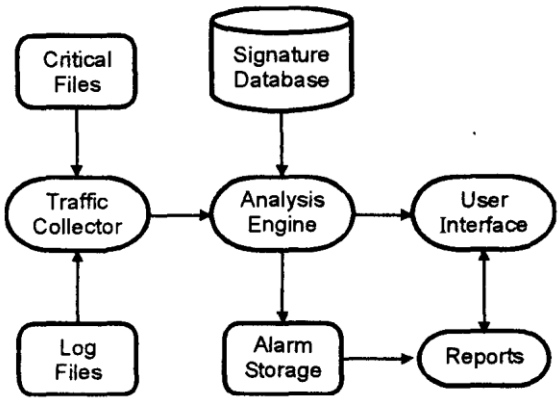
- It is a collection of patterns & definitions of known suspicious or malicious activity.

4. User Interface & Reporting:

- This is the component that interfaces with the human element, providing alerts when suitable & giving the user a means to interact with & operate the IDS.

(3 marks upto this)

Host based IDS



A host based IDS check log files, audit trails & network traffic coming into or leaving a specific host.

- HIDS can operate in real time, looking for activity as it arises, or batch mode, looking for activity on a periodic basis.
- Many host-based IDS focus on the log files or audit trails produced by local operating system. On windows systems, the examined logs are typically Application, System, & Security event logs. On Unix system, the examined logs are generally message, kernel & error logs.
- Some host based IDSs have the ability to cover specific applications by examining the logs produced by that specific applications or examining the traffic from the services themselves like FTP, or web services.

- HIDS is looking for certain activities in the log file are -
  - Logins at odd hours
  - Login authentication failure
  - Adding new user account
  - Modification or access of critical system files
  - Modification or removal of binary files
  - Starting or stopping processes
  - Privilege escalation
  - Use of certain programs

(11/2 Marks for HIDS)

Network Based IDS

- Network-based IDS focuses on network traffic — the bits & bytes traveling along the cables & wires that interconnect the system.
- A network IDS should check the network traffic when it passes & it is able to analyze traffic according to protocol, type, amount, source, destination, content, traffic already seen etc.
- Such an analysis must occur quickly, & the IDS must be able to handle traffic at any speed the network operates on to be effective.
- Network-based IDSs are generally deployed so that they can monitor traffic in & out of an organization's major links like connection to the Internet, remote offices, partner etc.
- Network-based IDSs looks for certain activities like:
  - Denial of service attacks
  - Port scans or sw'eeps
  - Malicious content in the data payload of a packet or packets
  - Vulnerability scanning
  - Trojans, viruses, or worms
  - Tunneling
  - Brute-force attacks **(11/2 Marks for NIDS)**

Q.2 (a)

A digital certificate combines an individual's identity to a public key. Digital certificate contains all the information a receiver needs to be assured about the public key owners identity. The certificate are created and formatted based on the x.509 standard. This standard which tell the necessary fields of a certificate and possible values that can be inserted into the field.

Certificate Authority (CA)

- CA is the trusted authority for certifying individuals identities and creating an electronic document known as a digital certificate, which indicate that individuals are who they say they are.
- Digital certificate establishes an association between the subject's identity and a public key. The certificate's public key and private key is stored separately.
- The CA is made up of the software, hardware, procedures, policies, and people who are involved in validating individuals' identities and generating the certificates.
- If any one of above components is compromised, it can affect the CA negatively and can threaten the integrity of the certificates it produces.

- Certificate practices statement (CPS) outlines how to verify identity, the steps that the CA must follows to generate, maintain, and transmit certificates, and why the CA can be trusted to fulfill its responsibilities.
- CPS describes how keys are secured, what data is placed within a digital certificate, and how revocations will be handled.
- The company's security officers, administrators, and legal department should examine the CA's CPS to ensure that it will properly meet the company's needs when a company is going to use and depend upon a public CA. To make sure that the level of security claimed by the CA is highly enough for companies use and environment.
- The trust between the user and CA is the critical part of PKI , thus CPS should be reviewed and understood to ensure the level of the trust.
- The server construct and populates the digital certificates with the necessary information, it combines the user's public key with the resulting certificates, The certificate is then digitally signed with CA's private key.

(2 Marks upto here)

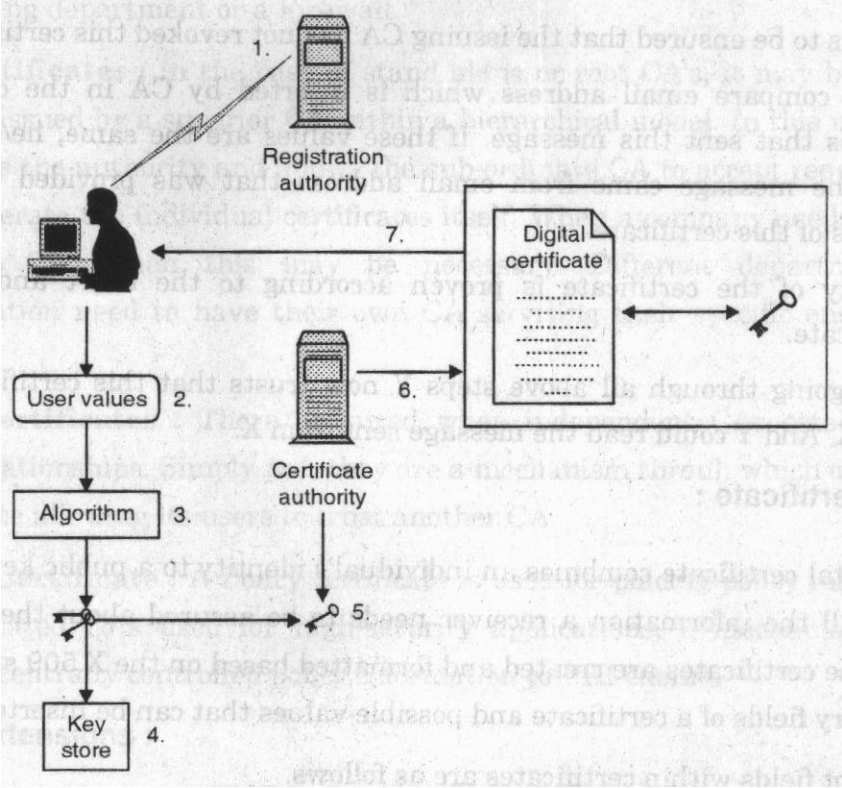
Registration Authority (RA)

- This component accepts a request for a d certificate and it performs the necessary steps for registering and authenticating the person requesting the certificate. The authentication requirements are depend on the type of certificate being requested and these can vary between different CAs. Generally there are following three different types -
- **Class 1:** Generally this is used to verify an individual's identity through e-mail. A person who receives a Class 1 certificate can use their public/private key pair to digitally sign e-mail and encrypt message contents.
- **Class 2:** This may be used for software signing. Generally software vendors will register for this type of certificate so they can digitally sign their software. This will provide integrity for the software after it is developed and released, and it will allow the receiver of the software to verify originality of the software.
- **Class 3:** This type of certificate may be used by a company to set up its own certificate authority, which will allow them to carry out their own identification verification and generate certificates internally.

Every higher class can carry out more critical and powerful tasks so the different classes have different requirements -

- Class 1 — Name, Email Address and physical address ate necessary.
- For Class 2 — It require additional data like Driving licence, Passport and company information.
- For Class 3 — It may require more information and person may need to visit RA's office for face to face meetings.
- Every CA will summarize the certification classes it provides and the identification requirements that must be meet to obtain each type of certificate.

(4 Marks upto Here)



(6Marks Diagram)

Steps involved in obtaining digital certificate

1. The user registers for a digital certificate through a Web Based form.
2. Once all data is inserted into the form. The browser initiates key generation process. This will often require random input values (This may be acquired by Random Mouse Movements, keystrokes Or by extracting specific information from within the system itself.
3. These random values are inserted into cryptographic algorithm that used to generate a public/private key pair.
4. The key pair is stored in a key store on the workstation. If the key is being created for the first time, the application should request a password from the user that will be used to access and use the keys.
5. The public key is attached to the certificate registration form and both are forwarded to the RA(Registration Authority) for processing. HA is only responsible for Registration process. Once RA is done with his processing copy of the public key and other identifying information is sent to the CA(Certificate Authority).
6. The CA generates the Digital Certificate containing the public key and the other identifying information.
7. The new certificate is sent to the user.

(8 Marks upto here)

Q.2 (b)

The SSL protocol was originally developed by Netscape, to ensure security of data transported and routed through HTTP, LDAP or POP3 application layers. SSL is designed to make use of TCP as a communication layer to provide a reliable end-to-end secure and authenticated connection between two points over a network (for example between the service client and the server). Notwithstanding this SSL can be used for protection of data in transit in situations related to any network service, it is used mostly in HTTP server and client applications. Today, almost each available HTTP server can support an SSL session, whilst IE or Netscape Navigator browsers are provided with SSL-enabled client software.

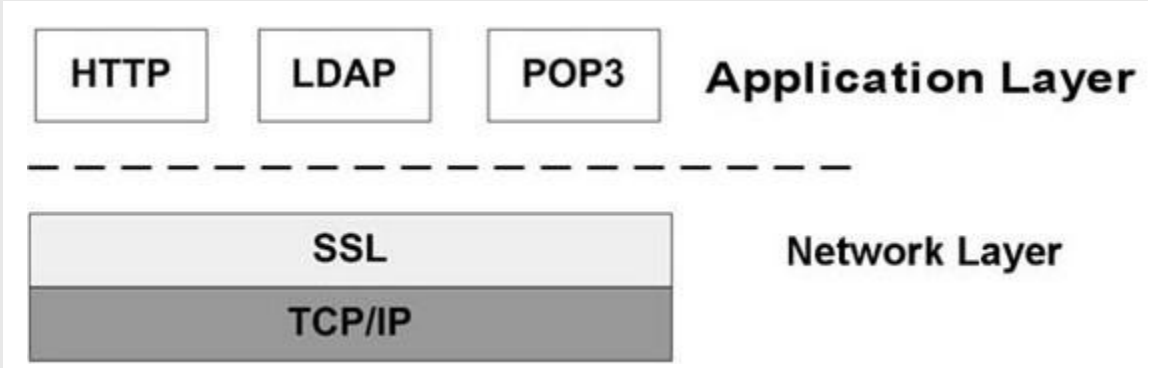


Figure 1 SSL between application protocols and TCP/IP

SSL protocol stack

The SSL protocol stack is illustrated in Figure 2.

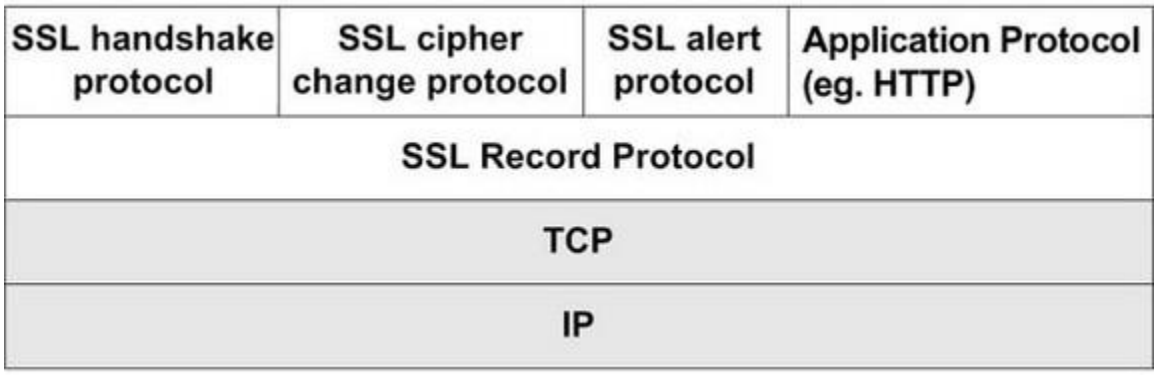


Figure 2

The SSL protocol stack

SSL uses these protocols to address the tasks as described above. The SSL record protocol is responsible for data encryption and integrity. As can be seen in Figure 2, it is also used to encapsulate data sent by other SSL protocols, and therefore, it is also involved in the tasks associated with the SSL check data. The other three protocols cover the areas of session management, cryptographic parameter management and transfer of SSL messages between the client and the server. Prior to going into a more detailed discussion of the role of individual protocols and their functions let us describe two fundamental concepts related to the use of SSL.
The concepts as mentioned above are fundamental for a connection between the client and the server, and they also encompass a series of attributes. Let's try to give some more details:

- **connection:** this is a logical client/server link, associated with the provision of a suitable type of service. In SSL terms, it must be a peer-to-peer connection with two network nodes.

- **session:** this is an association between a client and a server that defines a set of parameters such as algorithms used, session number etc. An SSL session is created by the Handshake Protocol that allows parameters to be shared among the connections made between the server and the client, and sessions are used to avoid negotiation of new parameters for each connection. This means that a single session is shared among multiple SSL connections between the client and the server.

  In theory, it may also be possible that multiple sessions are shared by a single connection, but this feature is not used in practice. The concepts of a SSL session and connection involve several parameters that are used for SSL-enabled communication between the client and the server. During the negotiations of the handshake protocol, the encryption methods are established and a series of parameters of the Session State are subsequently used within the session

(4Marks till this point)

The SSL Record Protocol

The SSL record protocol involves using SSL in a secure manner and with message integrity ensured. To this end it is used by upper layer SSL protocols. The purpose of the SSL record protocol is to take an application message to be transmitted, fragment the data which needs to be sent, encapsulate it with appropriate headers and create an object just called a record, which is encrypted and can be forwarded for sending under the TCP protocol. The first step in the preparation of transmission of the application data consists in its fragmentation i.e. breaking up the data stream to be transmitted into 16Kb (or smaller) data fragments followed by the process of their conversion in a record. These data fragments may be further compressed, although the SSL 3.0 protocol specification includes no compression protocol, thus at present, no data compression is used.

At this moment, creation of the record is started for each data portion by adding a header to it, possible information to complete the required data size and the MAC. The record header that is added to each data portion contains two elementary pieces of information, namely the length of the record and the length of the data block added to the original data.

The SSL protocol stack

The SSL Record protocol
The SSL record protocol is used to transfer any data within a session - both messages and other SSL protocols (for example the handshake protocol), as well as for any application data.

The Alert Protocol
The Alert Protocol is used by parties to convey session messages associated with data exchange and functioning of the protocol. Each message in the alert protocol consists of two bytes. The first byte always takes a value, “warning” (1) or “fatal” (2) , that determines the severity of the message sent. Sending a message having a „fatal” status by either party will result in an immediate termination of the SSL session. The next byte of the message contains one of the defined error codes, which may occur during an SSL communication session.

The ChangeCipher Spec protocol

This protocol is the simplest SSL protocol. It consists of a single message that carries the value of 1. The sole purpose of this message is to cause the pending session state to be established as a fixed state, which results, for example, in defining the used set of protocols. This type of message must be sent by the client to the server and vice versa. After exchange of messages, the session state is considered agreed. This message and any other SSL messages are transferred using the SSL record protocol.

The handshake protocol

The handshake protocol constitutes the most complex part of the SSL protocol. It is used to initiate a session between the server and the client. Within the message of this protocol, various components such as algorithms and keys used for data encryption are negotiated. Due to this protocol, it is possible to authenticate the parties to each other and negotiate appropriate parameters of the session between them.

The process of negotiations between the client and the server is illustrated in Figure 4. It can be divided into 4 phases separated with horizontal broken lines. During the first phase, a logical connection must be initiated between the client and the server followed by the negotiation on the connection parameters. The client sends the server a client_hello message containing data such as:

- **Version:** The highest SSL version supported by the client,
- **Random:** data consisting of a 32-bit timestamp and 28 bytes of randomly generated data. This data is used to protect the key exchange session between the parties of the connection.
- **Session ID:** a number that defines the session identifier. A nonzero value of this field indicates that the client wishes to update the parameters of an existing connection or establish a new connection on this session. A zero value in this field indicates that the client wishes to establish a new connection.
- **CipherSuite:** a list of encryption algorithms and key exchange method supported by the client.
  The server, in response to the client_hello message sends a server_hello message, containing the same set of fields as the client message, placing the following data:
- **Version:** the lowest version number of the SSL protocol supported by the server,
- random data: the same fashion as used by the client, but the data generated is completely independent,
- **session ID:** if the client field was nonzero, the same value is sent back; otherwise the server's session ID field contains the value for a new session,
- **CipherSuite :** the server uses this field to send a single set of protocols selected by the server from those proposed by the client. The first element of this field is a chosen method of exchange of cryptographic keys between the client and the server. The next element is the specification of encryption algorithms and hash functions, which will be used within the session being initiated, along with all specific parameters.

(8 Marks upto this point)

Q.2 (c) Explain Deffie-Heilman Key-exchange algorithm?

Ans. Diffie–Hellman key exchange (**D–H**)[nb 1] is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

The scheme was first published by Whitfield Diffie and Martin Hellman in 1976. In 2002, Hellman suggested the algorithm be called **Diffie–Hellman–Merkle key exchange** in recognition of Ralph Merkle's contribution to the invention of public-key cryptography (Hellman, 2002).

Although Diffie–Hellman key agreement itself is an *anonymous* (non-*authenticated*) key-agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide perfect forward secrecy in Transport Layer Security's ephemeral modes (referred to as EDH or DHE depending on the cipher suite).

The method was followed shortly afterwards by RSA, an implementation of public key cryptography using asymmetric algorithms.

Before going in depth of Diffie Hellman Algorithm,we define primitive root of a prime number 'p' as one whose powers generate all the integers from 1 to p-1, i.e. if 'a' is the primitive root of a prime no 'p', then, a mod p , a^2 mod p , a^3 mod p, ... a^{p-1} mod p generate all distinct integers from 1 to (p-1) in some permutation.

The steps for Diffie Hellman key exchange algorithm are:

Step 1 : GLOBAL PUBLIC ELEMENTS
Select any prime no : 'q'
Calculate the primitive root of q : 'a' such that a<q

Step 2 : ASYMMETRIC KEY GENERATION BY USER 'A'
Select a random number as the private key X_A where $X_A < q$
Calculate the public key Y_A where $Y_A = a^{X}{}_A \bmod q$

Step 3 : KEY GENERATION BY USER 'B'
Select a random number as the private key X_B where $X_B < q$
Calculate the public key Y_B where $Y_B = a^{X}{}_B \bmod q$

Step 4 : Exchange the values of public key between A & B

Step 5 : SYMMETRIC KEY (K) GENERATION BY USER 'A'
$K = Y_B{}^{X}{}_A \bmod q$

Step 6 : SYMMETRIC KEY (K) GENERATION BY USER 'B'
$K = Y_A{}^{X}{}_B \bmod q$

It can be easily be proved that the key K generated by this algorithm by both parties are the same.

(4 marks upto this)

Example

1. Alice and Bob agree to use a prime number p=23 and base g=5.
2. Alice chooses a secret integer ***a*=6**, then sends Bob A = g^a mod p
   - A = $5^{\mathbf{6}}$ mod 23
   - A = **15,625** mod 23
   - A = 8
3. Bob chooses a secret integer ***b*=15**, then sends Alice B = g^b mod p
   - B = $5^{\mathbf{15}}$ mod 23
   - B = **30,517,578,125** mod 23
   - B = 19
4. Alice computes **s** = B^a mod p
   - **s** = $19^{\mathbf{6}}$ mod 23
   - **s** = **47,045,881** mod 23
   - **s** = **2**
5. Bob computes **s** = A^b mod p
   - **s** = $8^{\mathbf{15}}$ mod 23
   - **s** = **35,184,372,088,832** mod 23
   - **s** = **2**
6. Alice and Bob now share a secret: **s** = **2**. This is because 6*15 is the same as 15*6. So somebody who had known both these private integers might also have calculated sas follows:
   - **s** = $5^{\mathbf{6*15}}$ mod 23
   - **s** = $5^{\mathbf{15*6}}$ mod 23
   - **s** = $5^{\mathbf{90}}$ mod 23
   - **s** = **807,793,566,946,316,088,741,610,050,849,573,099,185,363,389,551,639,556,884,765,625** mod 23
   - **s** = **2**

Both Alice and Bob have arrived at the same value, because $(g^a)^b$ and $(g^b)^a$ are equal mod p. Note that only a, b and $g^{ab} = g^{ba}$ mod p are kept secret. All the other values – p, g,g^a *mod* p, and g^b *mod* p – are sent in the clear. Once Alice and Bob compute the shared secret they can use it as an encryption key, known only to them, for sending messages across the same open communications channel. Of course, much larger values of a, b, and p would be needed to make this example secure, since it is easy to try all the possible values of g^{ab} mod 23. There are only 23 possible integers as the result of mod 23. If p were a prime of at least 300 digits, and a and b were at least 100 digits long, then even the best algorithms known today could not find a given only g, p, g^b mod p and g^a mod p, even using all of mankind's computing power. The problem is known as the discrete logarithm problem. Note that g need not be large at all, and in practice is usually either 2, 3 or 5.**(8 marks upto this)**

Note : In example two name are used which can be any thing, any prime value of key can be taken. Instead of name any variable can be considered. The example is for reference purpose

Q.3 (a) **(2 marks or (1 mark and /diagram 1 mark) explanation) for each**

Sniffing: This is software or hardware that is used to observe traffic as it passes through a network on shared broadcast media. It can be used to view all traffic or target specific protocol, service, or string of characters like logins. Some network sniffers are not just designed to observe the all traffic but also modify the traffic. Network administrators use sniffers for monitoring traffic. They can also used for network bandwidth analysis and to troubleshoot certain problems such as duplicate MAC addresses**.**

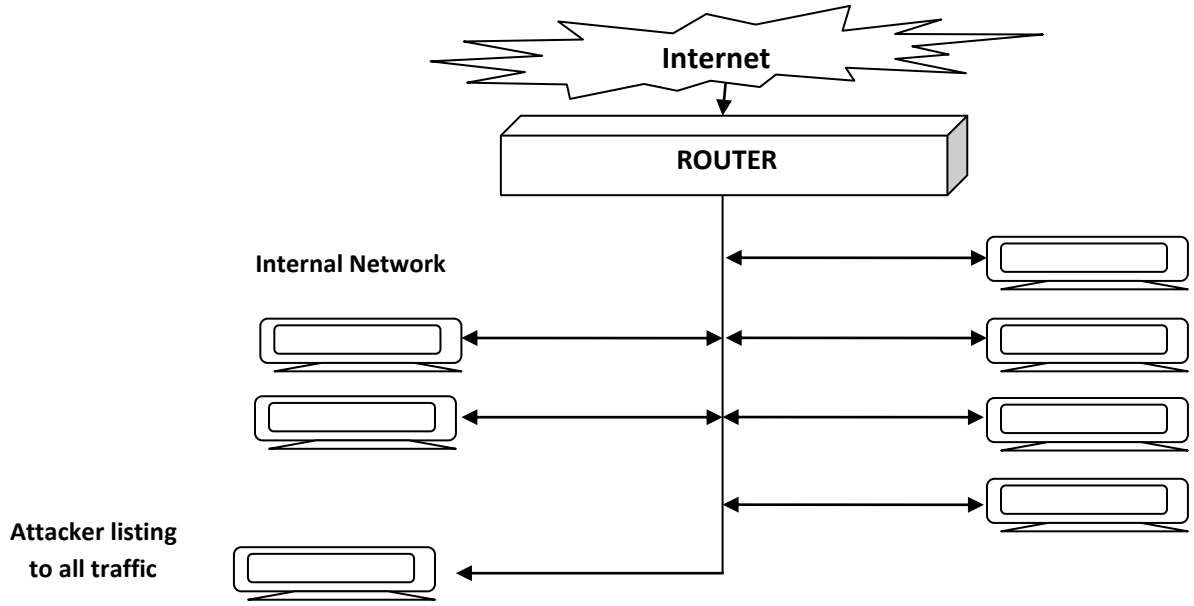


Fig. Network Sniffer

Spoofing is making data similar to it has come from a different source. This is possible in TCP/IP because of friendly assumptions behind the protocols.
When packet is sent from one system to another, it includes not only IP address and port of destination but the source IP address as well. This is one of the several forms of spoofing.

1. Spoofing E-mail: can be easily accomplished. Here email that appears to have been originated from one source but it was actually send from another source.
Best of Email spoofing is Spam Email& junk mails.
A simple method of spoofing an email address is to telnet to port 25 , the port is associated with email on system from where one can fill **From** and **To** sections of messages, whether the addresses are yours and are exist or not. Sometimes attacker acquires URL like ABC organization has owned ABC.com but attacker might gain access to the URL ABC.Corp.com

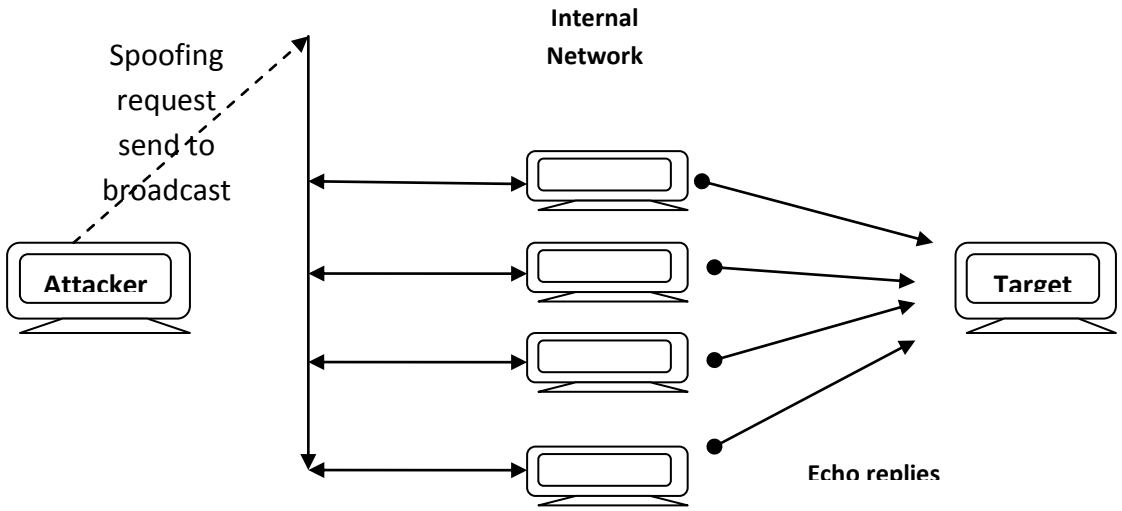


Fig. Spoofing used in Smurf

2. IP Address spoofing: IP protocol is designed to work i.e. to have the originators own IP address in FRO portion of packet. There is nothing that prevents a system from inserting a different address in the FROM portion of the packet is known as IP address Spoofing.

There are many reasons fro spoofing IP address, Specific DOS attack, (Smurf attack), the attacker sends spoofed packet to the broadcast address for a network, which distributes the packet to all systems on that network.

Here echo request with fake FROM address so that it appears that another system has made the echo request.

In smurf attack, the request is send to all system on the network, so all systems will respond with an echo reply to the target system.

- Spoofing can take advantage of trusted relationship between two systems.

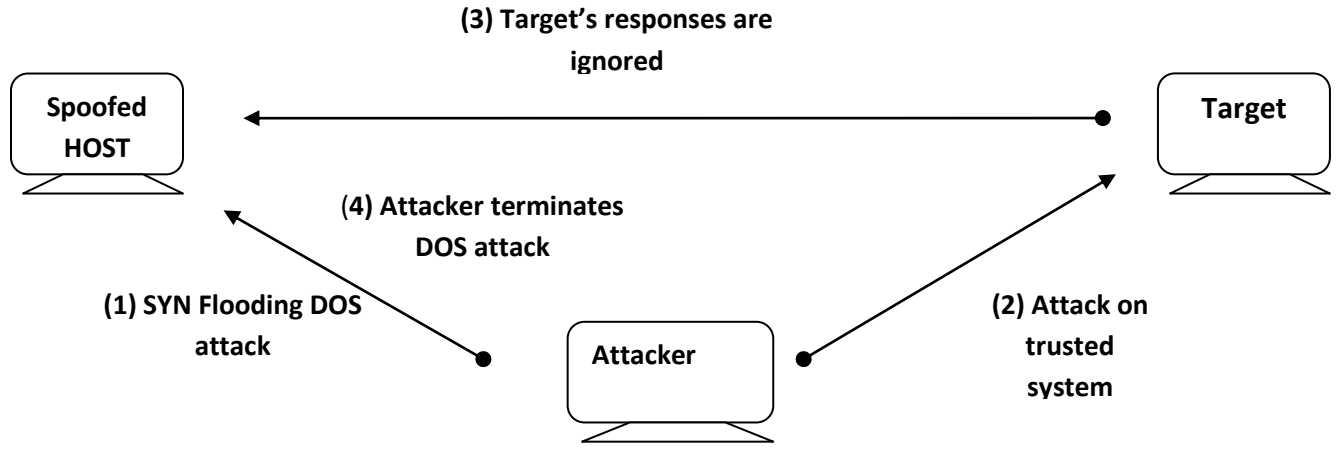
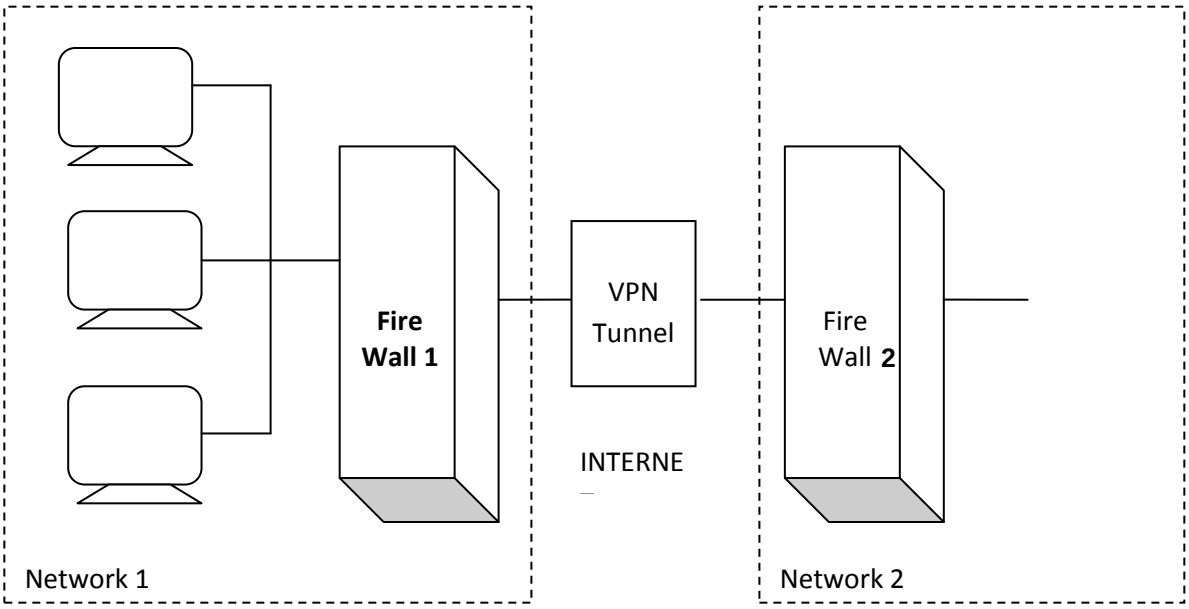


Fig. Spoofing Attack

Q.3 (b) (**3 mark diagram and explanation(with packet details optional), 1 mark Benefits)**

VPN is a Virtual Private Network that uses a public telecommunication infrastructure such as internet with secure access to their organizations network. VPN is a mechanism to create a private network over a public network like internet.



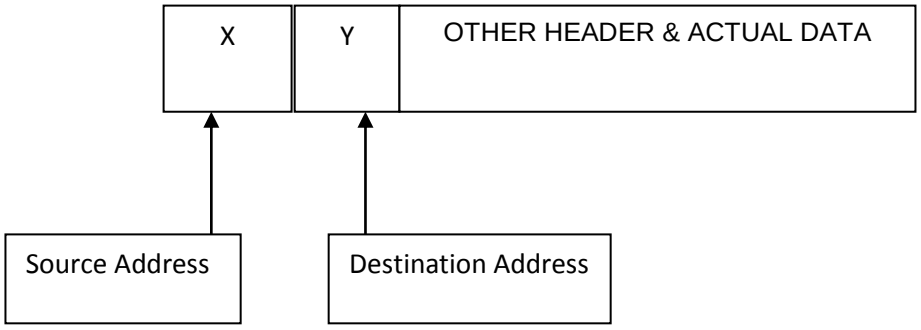
Above fig. shows that network1 connects to internet via firewall 1 & network 2 via firewall 2.

Here two firewalls are virtually connected to each other through internet with the help of VPN tunnel.

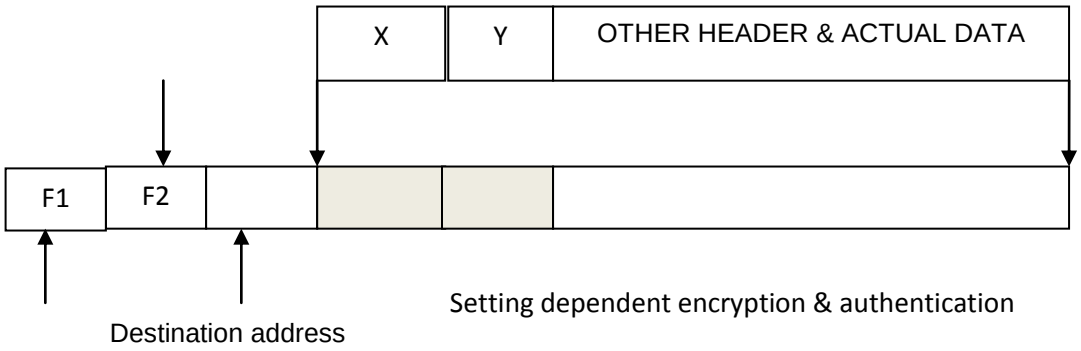
VPN protects traffic passing between two hosts or two different networks.

The transmission between two networks takes following steps:

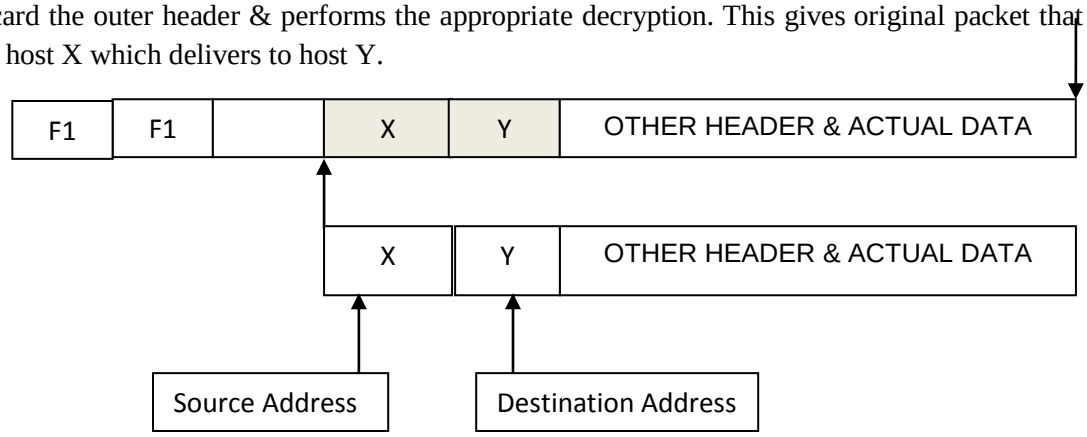
1. Let us assume that network's host X wants to send a packet to network's host Y.
2. Then host X creates packet, insert its own IP address as source address & IP address of host Y as destination address.



3. Then this packet reaches firewall, here firewall will add new headers. In these new headers, it changes the source IP address of packet from that of host X to its own address i.e. IP address of firewall & it again changes destination address from that of host Y to IP address of firewall2.It also performs encryption & authentication.



4. Now, this packet reaches to firewall 2 over internet via one or more routers . Here firewall 2 will discard the outer header & performs the appropriate decryption. This gives original packet that is created by host X which delivers to host Y.



Benefits of VPN are:

1) As Name indicates, it employing encryption, authentication and integration it can be used as private or public network.
2) It can be allowed to travelling users, remote access.
3) There connections are connected temporary, and does not have any physical presence.

Q.3 (c) **(1 mark definition, 2 mark importance and 1 marks uses)**

Security consists of all mechanisms to guarantee that access to computer system & network is to only for authorized users. When physical security is taking into account, access from all sides should be considered.

To provide physical security following methods are there.

1) Access controls- use of physical access controls is same as that of computer & network access controls to restrict access to unauthorized users. Most common access control mechanisms are security guard & lock and key combination

2) Biometrics- Biometrics is idea to map measurement s of human physical characteristics to human uniqueness. The major biometrics forms are:

- Handprint
- Fingerprint
- Retina
- Voice/speech
- Handwriting/signature
- Face

3) Physical Barriers : Physical barriers helps in implementing physical world equivalent of layered security.

Q.3 (d) **(2 marks and 2 marks for prevention criteria)**

Dumpster diving: Process of going through target's trash in order to find little bit information, which is further used to retrieve information could be used to carry out an attack on a computer network**.**
It can use access codes, sticky notes phone list, calendar, and organization chart to assist attacker to gain access to the network.

To prevent dumpster diving from learning anything valuable for social engineering attacks:

1. Establish a disposal policy where papers, printouts, are shredded in cross cut shredder, before recycled,
2. All storage media is erased
3. All staff is educated about the danger of untracked trash.
4. Security procedures should be strong enough.
5. Passwords can be changed periodically.

Q.3 (e) **(2 marks explanation and two marks for reasons (minimum two reasons expected)**

Operating systems is basic software which handles all most all highly detailed tasks to support the user environment and associated applications.

- Developers and manufactures of operating systems face common problems of configurations and variations that group require from their product.
- Hence thy provide default settings and installations for that product which usually contain the base of operating system, drivers, utilities and enhancements. hence Developers and manufactures will not provide security as that product can be used for variety of purposes

General steps provides are:

- **Disable all unnecessary services;** Windows serves one main purpose (web server, mail server, DNS server, Domain/ Login server etc.) which improves speed.
- **Restrict permissions on files and access to the registry:** it is tedious and time consuming job, but provide more needed security, As registries are protected to ensure that entries are not modified or deleted.
- **Remove unnecessary user accounts and ensure password guidelines are in place.**
  Default accounts should be disabled or removed. Password guidelines should be enabled and enforces to check that a user chose appropriate password.

Avoid unauthorized access.

- **Remove unnecessary programs:** Any application or utility not required should be removed; this reduces the chances of an attacker exploiting a weakness or enabling unneeded services. It helps to improve storage space management
- **Apply latest patches and fix:** It provides up gradation of software.

Q.4 (i) **(1 mark definition, 1 mark access metrix or list 2 marks types (minimum two types)**

Access is the ability of a subject to interest with an object. Authentication deals with verifying the identity of a subject. It is ability to specify, control and limit the access to the host system or application, which prevents unauthorized use to access or modify data or resources.

It can be represented using **Access Control matrix or List**:

	Process 1	**Process 2**	**File 1**	**File 2**	**Printer**
Process 1	Read, Write, Execute	---	Read	Read	Write
Process 2	Execute	Read, Write, Execute	Read	Read, Write	Write

Various access controls are:

- **Discretionary Access control (DAC):** Restricting access to objects based on the identity of subjects and or groups to which they belongs to , It is conditional, basically used by military to control access on system. **UNIX based System** is common method to permit user for read/write and execute
- **Mandatory Access control (MAC):** It is used in environments where different levels of security are classified. It is much more restrictive. It is sensitivity based restriction, formal authorization subject to sensitivity. In MAC the owner or User can not determine whether access is granted to or not. i.e. **Operating system rights.** Security mechanism controls access to all objects and individual cannot change that access.
- **Role Based Access Control (RBAC):** Each user can be assigned specific access permission for objects associated with computer or network. Set of roles are defined. Role in-turn assigns access permissions which are necessary to perform role.

Different User will be granted different permissions to do specific duties as per their classification.

Q.4 (ii) **(1 mark definition, 3 mark Phases of viruses)**

Ans. Virus is a program which attaches itself to another program and causes damage to the computer system or the network; It is loaded onto your computer without your knowledge and runs against your wishes. They can replicate themselves, all computer viruses are manmade. Even a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt.

During the life cycle of virus it goes through the following four phases:

1. **Dormant phase:** The virus is idle and activated by some event
2. **Propagation phase:** It places an identical copy of itself into other programs or into certain system areas on the disk.
3. **Triggering phase:** The virus is activated to perform the function for which it was intended.
4. **Execution phase:** The function of virus is performed.

Types of viruses **:(Optional)**

- Parasitic Viruses
- Memory resident viruses
- Non- resident viruses
- Boot sector Viruses
- Overwriting viruses
- Metamorphic viruses
- Stealth Virus
- Macro Viruses
- Polymorphic viruses
- Companion Viruses
- Email Viruses

Q.4(iii) **(1 mark definition, 3 mark prevention)**

Code injection is a risky behavior to a function without validation. or it is invalidated input. It changes the function in unintended way rather that appropriate for function.

SQL injection attack is a form of code injection, which aims SQL databases, It alters the SQL statement to one in which the part of query

For preventing code injection:

- Protection method is validating all inputs, rather validating length validate for contents.
- Pass the user input before use through an HTML encode function.
- Use of vulnerabilities by good programming practices, where code is reviewed and tested to catch programming errors.
- use software development process to find type of errors and cause of those errors. insert safeguards to prevent broadcast.

Q.4 (iv) **(1 mark each , any minimum four)**

Good software development process consists of:

- Select appropriate development lifecycle process to project. Spiral instead of Waterfall model
- Requirement analysis has major impact on application architecture, design, performance. Functional requirements are documented using use cases whereas nonfunctional requirements are described in terms of performance and system characteristics.
- Use modern software design approaches like object oriented analysis and design.
- Best practice for coding include built-in smoke test , peers review is important in terms of planning, requirement , designing coding, testing, etc.
- Testing is very important phase of software development different types of testing should be applied to the application.
- Use of deployment checklist
- List and define security requirements, with necessary procedures.

Q.4 (b)i) **(1 marks Explanation , 2 marks for policies for password management, 3 marks for elements of good password)**

Ans.: The username and password challenge is arguably the most popular security mechanism in use today. Unfortunately,

It's also the most poorly configured, neglected, and easily circumvented.

- The first step in addressing the password issue is to create an effective and manageable password policy that both system administrators and users can work with..
- What level of risk is acceptable?
- How secure does the system need to be?
- How often should users change their passwords?
- Should you ever lock accounts?
- What guidelines should users use when selecting passwords?

  list of questions will vary greatly, but the key is to spend time identifying your concerns and addressing them specifically in your password policy.

Those setting password requirements must remember that making the password rules too difficult may actually decrease security if users decide the rules are impossible or too difficult to meet.

The following password requirements will be set by the IT security department:

1. Password should have minimum and maximum limit
    1. Minimum Length - 8 characters recommended
    2. Maximum Length - 14 characters
    3. Minimum complexity - No dictionary words included.

Passwords should use three of four of the following four types of characters:

1. Lowercase
2. Uppercase
3. Numbers
4. Special characters such as !@#$%^&*(){}[]

2. Passwords are case sensitive and the user name or login ID is not case sensitive.

3. Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 24.

1. Maximum password age - 60 days
2. Minimum password age - 2 days

4. Store passwords using reversible encryption - This should not be done without special authorization by the IT department since it would reduce the security of the user's password.
5. Account lockout threshold - 4 failed login attempts
6. Depending on the situation, the account lockout should be between 30 minutes and 2 hours.
7. Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. they can press the CTRL-ALT-DEL keys and select "Lock Computer".
8. Rules that apply to passwords apply to pass phrases which are used for public/private key authentication.

Q.4 (b) ii) **(Description 2-marks & 4 marks for different category of people involved in security-minimum 4)**

Ans. Major Security problems are because of users involved in security, following established policies or processes as there is lack of security policies, procedures or trainings within organization.

- **Password Selection:**
- To make job of attackers difficult user select difficult password combining Upper, lower numeric special characters
- Password should not be username, family member name, pet name etc.
- Frequently change in password, which gives less time to guess the attacker.
- **Piggy Backing:** simple Approach of following closely behind a person , either PIN code, or Physical access to building. Here attacker unknowingly gain access to facility and acquire control .
- **Shoulder surfing:** Similar procedure where attackers position themselves in such a way that they are able to observe the authorized user entering correct code, It is direct observation technique.
- **Dumpster diving:** going through target's trash in order to find little bit information, which is further used to retrieve information could be used to carry out an attack on a computer network**.**
- Destroy or Remove unused/used information from premises, which prevent dumpster divers from learning anything.
- **Installing Unauthorized software / Hardware**: like internet connection, wireless access, Bluetooth, access etc. which may give chance to attackers.
- **Access by non employees:** If an attacker can get physical access to a facility then there are many chances of obtaining information to enter computer system and network, wearing ID cards, Cell phones, built-in cameras, use of social website from organization.
- **Security awareness:** It is most effective way to prevent social engineering attacks.
- **Individual user responsibilities:** specific duties that user should follow be expected to perform vary between organizations and type of business, lock the office, computer, don't leave sensitive information in free access, secure storage media, discard used papers, protect laptops, enforce corporate access control methods.

Q.5 (a) (1 ½ mark for each point & 1 mark for right order)

Security topology is a logical map that depicts the interconnectivity between security devices and security domains that host these networks.(1M)

Internet explorer includes five predefined zone:

Internet, local Intranet, trusted sites, restricted sites & my computers

Types of security zone

1. **Internet zone**
   This zone contains web sites. These sites are not on your computer or on your local internet or that are not already assigned to another zone. The default security level is medium.
2. **Local Internet zone**
   By default, the local internet zone contains all network connection that were established by using a universal naming convention (UNC) path example: http:// local.

   The default security level for local internet is set to medium.
3. **Trusted sites zone**
   - This zone contains web sites that you trust as safe
   - When you add web sites to trusted sites zone, you believe that files you download or that you run from the web sites will not damage your computer r data.
   - But there are no web sites that are assigned to trusted site zone. So security level is set to low.
4. **Restricted site zone:**
   This zone contains web site to restricted sites zone, you believe that you download or run from website may damage your computer or your data.
   By default, there are no web sites that are assigned to restricted sites zone & security level is high. The restricted sites zone contains web sites that are not on your computer or on your local internet. The default security zone is medium.

Q.5 (b)(Each definition 2-marks, Technique 2-marks)

- Data that can be read & understood without any special measures is called plain text.
- The result of encryption performed on plaintext using an algorithm called as cipher text
  OR

- Encrypted or Encoded message or information is also known as cipher text.
  Caesar Cipher Substitution Technique:
  Caesar cipher is one of the simplest and most widely known encryption technique.
  In this each letter in plain text is replaced by a letter some fixed number of position down the alphabet.

Ex:- plain text: Computer security is important.
Take shift of 3 or key=3
So cipher text:- drpxwhu vhfxulwb lv lpsruwdqw.
(Use any shift but as per shift check the answer)

Q.5 (c) (Explanation 2- marks, Advantages 2- marks, Diagrams 1-mark each, Authentication 2-marks)
The IP packets contain data in plain text form. Anyone can access them, read their contains & even change them. To avoid such type of attack the higher level security mechanism used in this scheme.

First offer security at the IP packet level itself.

Continue implementing higher level security mechanism, depending on requirement as shown in fig.

The outcome of study & IAB's report is the protocol for providing security at IP level cancel as IP security. (IPSec)

In 1994, Internet Architecture Board proposed a report called security in the internet Architecture. This report state that, internet was a very (large) open network, which was unprotected from hostile attack.

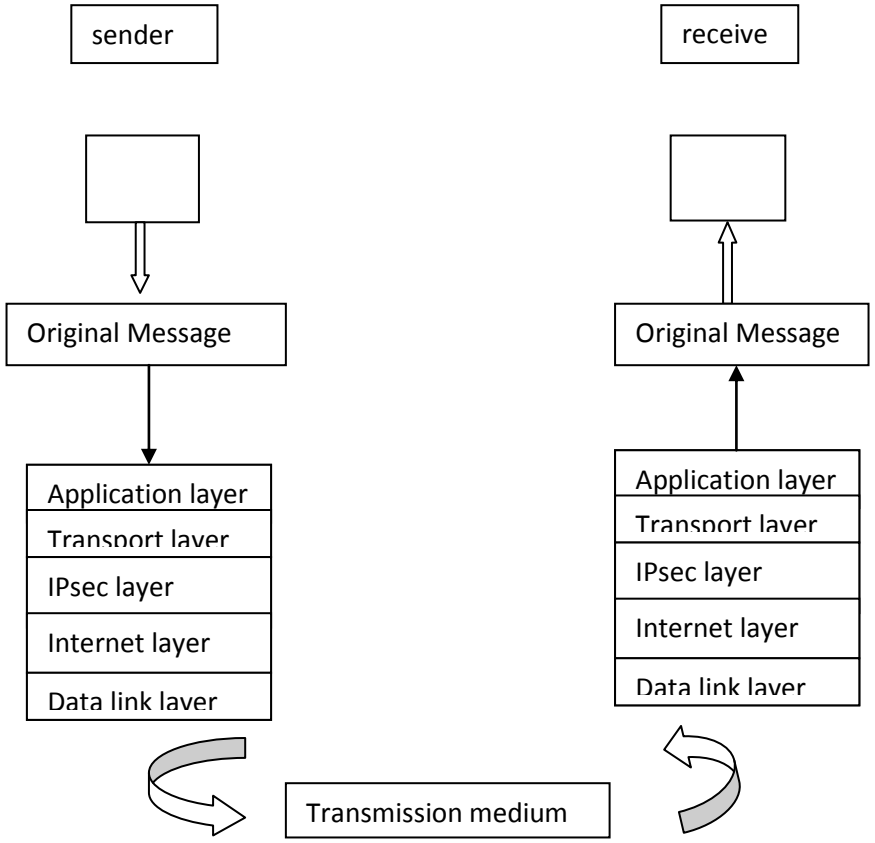
Therefore, internet needs better security measures, in terms of authentication, integrity & confidentially.

So, IAB decide that authentication, integrity & encryption must be part of next version of IP new generation (IPng).

But these versions of IP were taken some years to released & implemented. So, the designer's devised ways to incorporate these security measures in current version of IP, called IP version 9(IPV9)

The overall idea of IPsec is to encryption & seals the transport & application layer during transmission. it also offers integrity protection for internet layers. However, the internet header itself is not encrypted, because of which the intermediate router can deliver encrypted IPsec message to intended recipients.

Sender & receiver look at IPsec as shown in fig as another layer in TCP/IP protocol stack



IP sec overview:

Advantages & application: let us first list of application

1. **Secure remote internet access:**
   Using IPsec, we can make a local call to our internet services provider (ISP) so as to connect to our organization network in a secure fashion from our house or hotel from there; we can access the corporate network facilities or access remote desktop/servers.
2. **Secure branch office connectivity:**

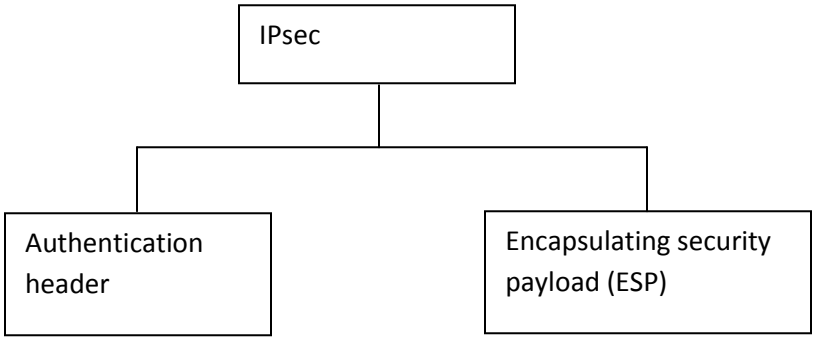
   Rather than subscribing to an expensive leased line for connecting its branches across cities, an organization can set up an IPsec enabled network to securely can't all its branches over internet.

3. **Set up communication with other organization:**
   Just as IPsec allow connectivity between various branches of an organization, it can also be used to connect the network of different organization together in a secure & inexpensive fashion.
   Main advantages of IPsec:
   - ✓ IPsec is transparent to end users.
     There is no need for an user training key, key issuance or revocation.
   - ✓ When IPsec is configured to work with firewall, it becomes the only entry-exit paint for all traffic, making it extra secure.
   - ✓ IPsec works at network layer. Hence no change are needed to upper layers or router, all outgoing & incoming traffic gets protected.
   - ✓ IPsec allow travelling staff to have secure access to the corporate network
   - ✓ IPsec allows interconnectivity between branches/ offices in a very inexpensive manner.

Basic Concept of IPsec Protocol:

As we know, IP packet consist two position IP header & actual data IPsec feature are implemented in the form of additional headers called as extension header to the standard, default IP header. IPsec offers two main services authentication & confidentially. Each of these requires its own extension header. Therefore, to support these two main services, IPsec defines two IP extension header one for authentication & another for confidentiality.

It consists of two main protocols.

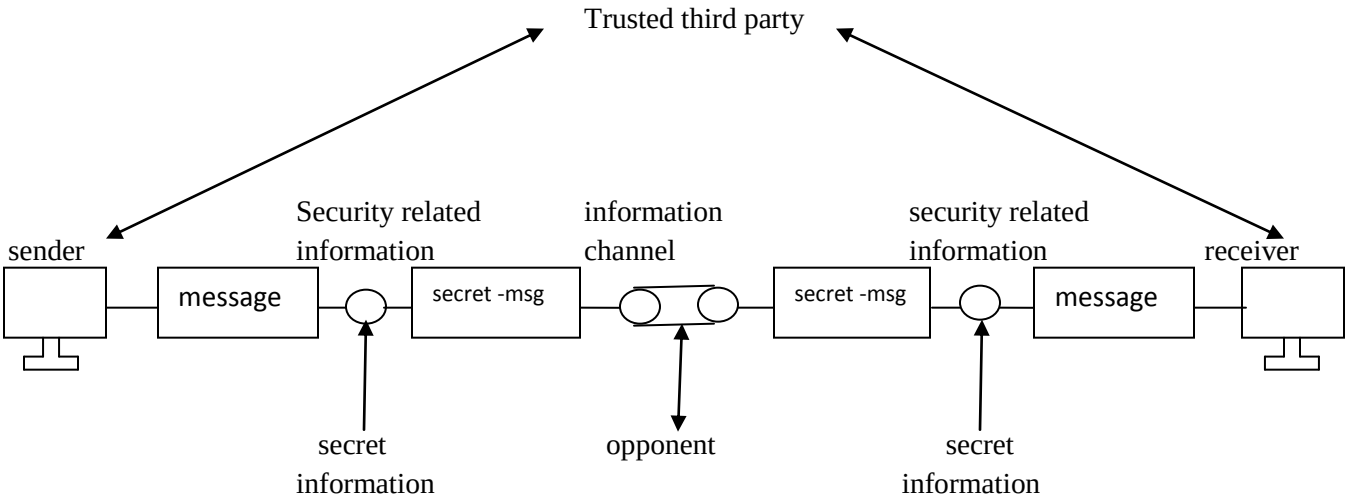


Authentication header(AH):

Authentication header is an IP Packet (AH) protocol provides authentication, integrity & an optional anti-reply service. The IPsec AH is a header in an IP packet. The AH is simply inserted between IP header & any subsequent packet contents no changes are required to data contents of packet. Security resides completing in content of AH. (2 Marks)

Q.6 (a) (Enlisting layer 1-mark, Model 3-marks)
OSI standard for security model defines seven layers of security in the form of:
1. Authentication
2. Access Control
3. Non-repudiation
4. Data Integrity
5. Confidentiality
6. Assurance or Availability
7. Signature.

Model for Network Security



- A message is to be transferred from one party to another via Internet.
- Sender & receiver are principals of transaction and must cooperate for exchange to take place.
- An information channel is established by defining a route through Internet from source to destination with the help of communication protocol like TCP/IP.
- Techniques for providing security have following components:-
    - A security related transformation on information to be sent.
    - The secret information shared by two principals should be secret.
- A trusted party is required to achieve secure transmission.
- This is responsible for distributing secret information between two principals.

Model shows four basic tasks:

1. Design algorithm in such a way that an opponent cannot defeat its purpose. This algorithm is used for security related information.
2. Generate secret information that can be used with algorithm.
3. Develop method for distributing and sharing of secret information.
4. Specify a protocol which can be used by two principals that make use of security algorithm and secret information to achieve a security service.

Q.6 (b) (Explanation 3-marks, Types 1-mark)

Internet we used always anywhere we can connect any computer in the world to any other computer & now matters how far the two are located from each other.

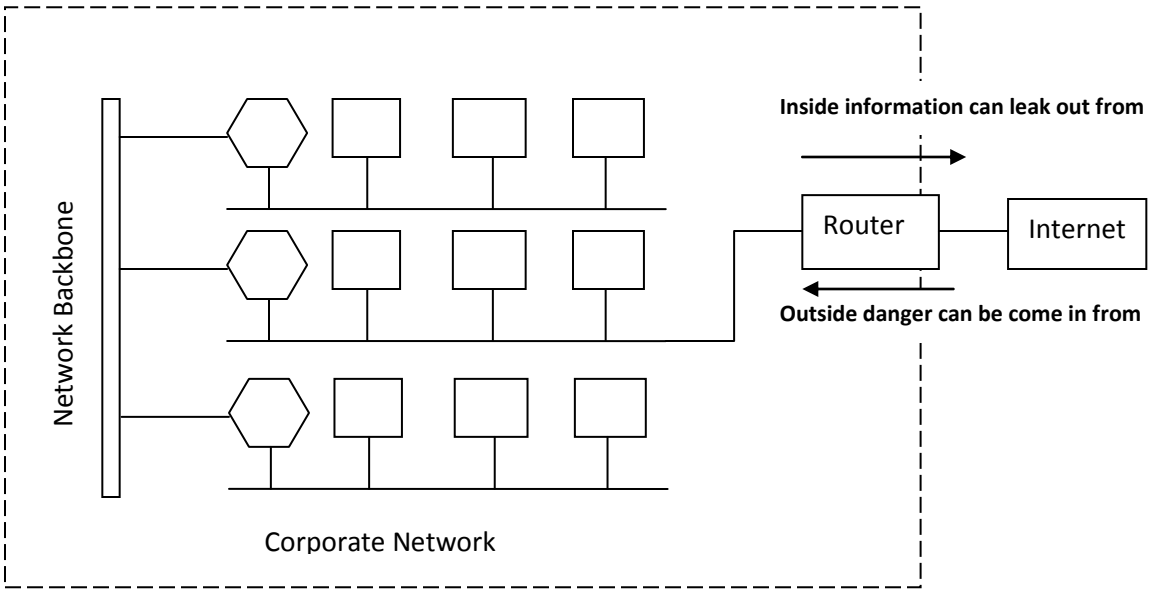
When we use internet availability of that internet for us is very easy. But it's very difficult job to protect corporate network from variety of attacks.

What is attack?

There are two kinds of attacks:

1. Most corporation have large amount of valuable & confidential data in these network hacking of this critical information to competitors can create difficulty. Example bank or any big IT organizations suppose confidential data comes out then it creates difficulty to themselves & its advantages to other competitors.
2. Apart from the danger of insider's information leaking out, there is great danger of outside elements (such as virus, worms).

As a result of these dangers, we must have mechanism which can ensure that inside information remain inside & also prevent the outsider attackers from entering inside.



Threats from inside & outside a corporate network.

It suppose, we pass message or data in encrypted from outsiders cannot makes any sense of it.

What is this encryption?

Means our data that means particular message we have to send through network converted into same other from or in code. There are various methods for that like Caesar cipher, substitution suffer. But attackers can still try to break corporate network.

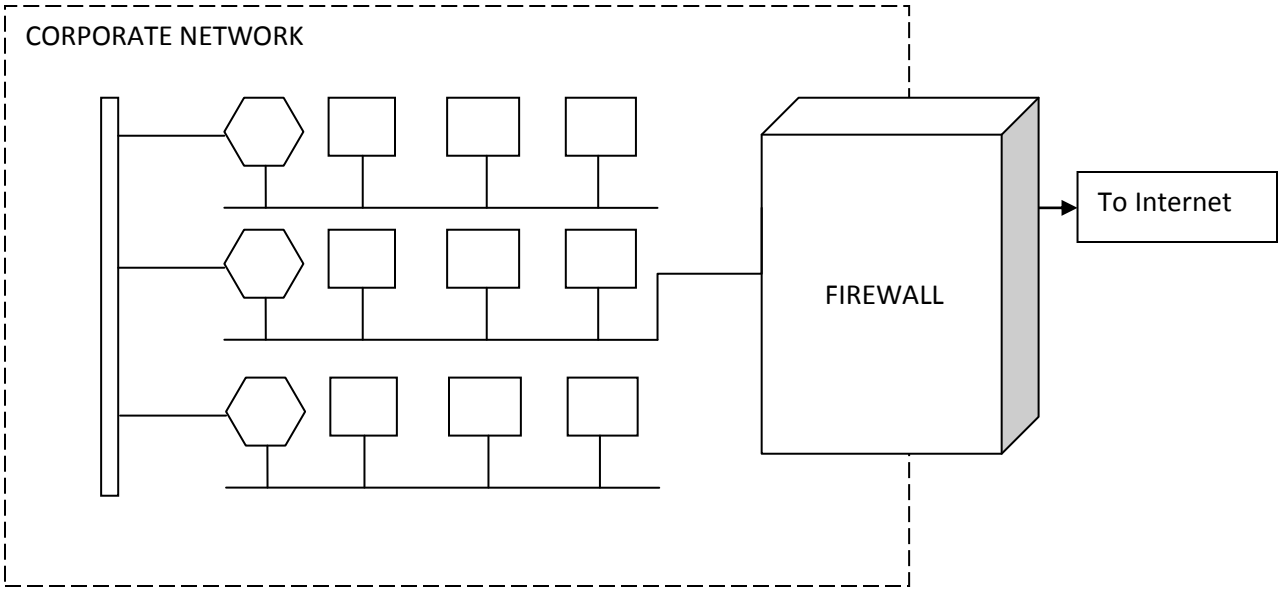
So, for better scheme firewall is used. So to protect the corporate network firewall is used.

Firewall is just like as sentry means like as watchmen. Sentry standing outside an important person's house (CM,PM) any VIP person this sentry usually keeps eyes on & physically checks every person that enterers house or someone having any suspicious object sentry banned to enter house.

A firewall act like a sentry firewall stands between network & outside world.

All traffic between network & the internet in either direction must pass through the firewall & then firewall decides traffic can be allowed to flow further or it must be stopped from proceeding further.

This is shown in the figure.



1. All traffic from inside to outside& vice versa, must pass through the firewall. To achieve this all access to local network must first physically blocked & access only via the firewall should be permitted.
2. As per local security policy traffic should be permitted.
3. The firewall itself must be strong enough, so as ender attacks on it useless.

TYPES OF FIREWALLS:

Firewalls classified into two types:

1.Packet Filter

2.Application Gateway.

3.Circuit Level Gateway.

Q.6 (c) (Explanation 4-marks)

As windows 2000 and windows XP are most commonly used for business and desktops. So we are going to focus on this so that general guidelines for securing windows operating system as follows:

1. Disable all unnecessary services:- Windows system will serve one main purpose. Once you have strong with what main purpose of the system will be, and then disable a service which is not necessary for that purpose.
2. Restrict permissions on files and access to the registry:- This step may take some time to restrict who can read, write and execute certain files and can provide some more needed security. Additionally windows registry must be protected to ensure that entries are not modified or deleted.
3. Remove unnecessary programs: Any application which is not required should be removed. This reduces the chances of an attacker exploiting a weakness.
4. Apply latest patches and fixes: Make sure that the operating system and all applications have latest vendor-supplied patches.
5. Remove unnecessary user account and ensure password guidelines are in place: -Default account like should be disabled or removed. Password guidelines should be enabled and enforced to check that a user chooses appropriate password.

Q.6 (d) (Correct differences Symmetric& Asymmetric 4-marks)

SYMMETRIC KEY CRYPTOGRAPHY:

1. In symmetric key cryptography same key is used for encryption & decryption .

2. Key has to be kept secret for sender & receiver.

3. Symmetric key cryptography is faster than asymmetric key cryptography.

4. The sender & receiver must agree on use before communication.

5. Also called as secret key cryptography.

ASYMMETRIC KEY CRYPTOGRAPHY

1. In asymmetric key cryptography different keys are used for encryption & decryption.

2. Asymmetric cryptography allows for distribution of your public key to anyone with which they can encrypt the data they want to send securely and then it can only be decoded by the person having the private key.

3. Asymmetric cryptography is about 1000 times slower than symmetric cryptography.

4. Also called as public key cryptography.

Q.6 (e) (Diagram-1 marks, Types- 2 marks, Explaination-1 mark)

- In symmetric algorithm, same key is used for encryption and decryption, hence known as single key or secret key algorithm.
- This key has to kept secret between sender & receiver.
- Sender & receiver must agree on a key before they communicate.

Encryption algorithm is divided into:

1. Block Cipher
2. Stream Cipher.

1. Block Cipher: - A block cipher encrypts larger blocks of data typically 64-bit blocks with complex encryption function.
   - A block cipher encrypts blocks belonging to same document all under same key.
2. Stream Cipher:- A stream cipher encrypts smaller block of data typically bits or bytes with simple encryption function.