Important Instructions to examiners:

1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more Importance (Not applicable for subject English and Communication Skills).
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.

Q1 .A) a) List different types of attacks (1/2 mark for each point, 4 marks for 8 points)

1. Active & passive attacks

2. Denial of service attack

3. Backdoors & trapdoors

4. Sniffing

5. Spoofing

6. Man-in Middle attack

7. TCP/IP Hacking

8. Replay attack

9. Encryption attack.

10. Malware

Q.1 A] b) Describe piggybacking & shoulder surfing. (2-marks each)

Piggybacking is the simple process of following closely behind a person 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.

for example: Access of wireless internet connection by bringing one's own computer within range of another wireless connection & using that without explicit permission

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. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, exp

Q.1 A] c) State the goals of computer security.(1 mark for each goal,)

1. Confidentiality

The goal of confidentiality is to ensure that only those individuals who have the authority can view a piece of information.

2. Integrity : 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.

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

4. Authentication: Authentication deals with the desire to ensure that an individual is who they claim to be.

Q.1 A] d) Components of good password: (1 mark for each point, any four)

1. Password should be at least eight character in length.

2. Password should have at least three of the following four elements:

i. one or more uppercase letters(A-Z)
ii. one or more lowercase letters(a-z)
iii. one or more numerical (0 to9)
iv. one or more special character(!,@,#,$,&,:,.,;,?)
v. Password should not consist of dictionary words
vi. Password should not at all be the same as login name.
vii. Password should not consist of user's first or last name, family members name, birth dates, pet names.

Q1 B) a) Password selection strategies: (any two)(1 mark for listing & 2 ½ mark for each point ,any two points)

There are four basic strategies to select a password

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.

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.

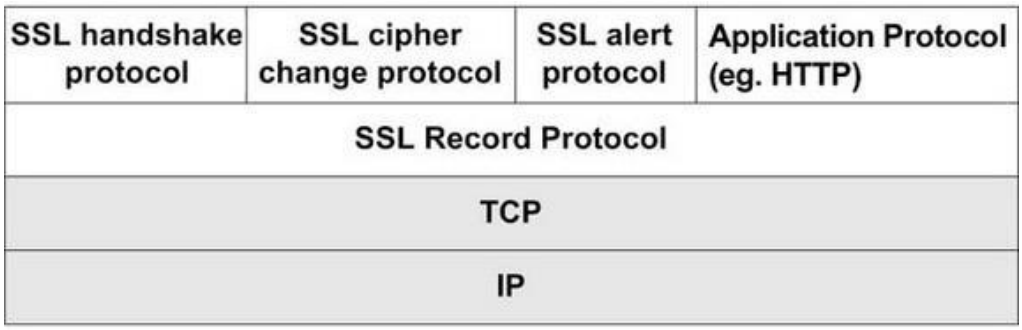
Proactive password checking

- 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.

- 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.

Q1.B) b) SSL Architecture & list all protocols. (4-marks for Architecture, 2-marks for protocols)



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, 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.

list of protocols:1)Handshake protocol 2)Cipher Change Protocol 3)Alert protocol 4)SSL Record Protocol

Q2. a) Explain Secure Electronic transaction (SET)with its requirement & participants.(3 marks for requirement & 5 marks for explanation of participants, Diagram Optional)

Requirements of SET:

1. Provide confidentiality of payment & ordering information.
2. Ensure the integrity of all transmitted data.
3. Provide authentication that cardholder is authorized user of credit card account.
4. Provide authentication to merchant can accept credit card authentication.

5. Ensure best security practices.

6.Facilitate & encourage inter-operatibilty among software & network providers.

Participants of SET:

1. Cardholder: By the internet ,consumers & corporate purchasers interact with merchant from computer over the internet.

-A cardholder is an authorized holder of card like mastercard, visa card that has been issued by issuer.

2. Merchant: A merchant is a person or organisation that has goods to sell to the cardholder. These goods are offered via web site or e-mail.

-A merchant that accept payment card must have relationship with acquirer.

2. Issuer: This is a financial institution like bank, that provides the cardholder with payment card.

-Issuer is very important that the issuer is ultimately responsible for the payment of the cardholder's transaction.

3. Acquirer: This is financial institution that establishes an account with a merchant & processes payment card authorizations & payments.

-The acquirer provides an assurance to the merchant that a given card account is active & that the purchase amount does not exceed the credit limit.

-It also provides electronic transfer of payments to the merchant's account.

4. Payment Gateway: This is a function operated by the acquirer or it can be taken up by an organization as debited function.

-The payment gateway process between SET and existing bankcard payment networks for authorization & payment function.

-The merchant exchanges SET message with the payment gateway over the internet. The payment gateway in turn connect to acquirer's system using dedicated network line.

5. Certification authority:

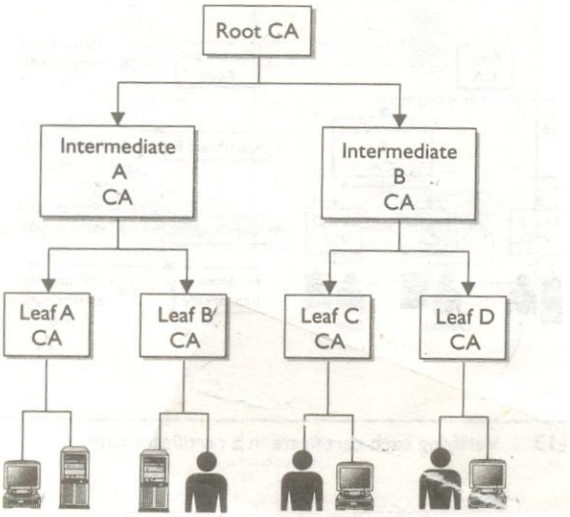
-this is an entity that is trusted to issue public key certificates for cardholders, merchants & payment gateways.

-The success of SET will depend on the existence of CA infrastructure for this purpose.

Q.2 b) What is trust model? Explain hierarchical & peer to peer trust model.(definition 1 mark, 3 ½ marks for each model)

A trust model is a construct of system, personnel, applications, protocols, technologies & policies that work together to provide a certain level of protection.

Hierarchical Model:



In Hierarchical structure contains a root CA, intermediate CAs & end-entities. The configuration is that of an inverted tree as shown in fig. The root CA is trust anchor for all other entities in this infrastructure & it generates certificates for the intermediate CAs ,which in turn generate certificates for the leaf CAs,& the leaf CAs generate certificates for end-entities like as users ,network devices, applications.

As shown in diagram there is no bidirectional trust-they are all unidirectional trusts as indicated by one-way arrow. Since no other entity can certify & generate certificates for the root CA. It creates a self-signed certificate. This means that the certificate issuer & subject fields hold the same information, both representing the root CA & root CA's public key is what will used to verify this certificate when that time comes.

This root CA certificate & public key is distributed to all entities within this trust model.

Peer to Peer trust model: In Peer-to-Peer trust model one CA is not subordinate to another CA & there is no established trusted anchor between the CAs involved.

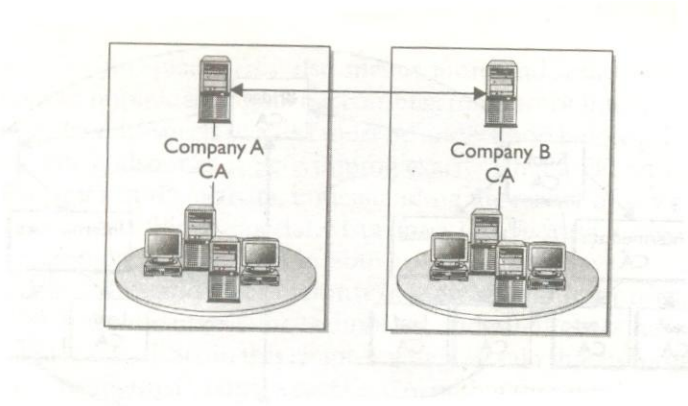


Fig. illustrates peer-to-peer trust model. The two different CAs will certify the public key for each other, which creates a bidirectional trust. This is referred to as cross certification, since the CAs are not receiving their certificates & public keys form superior CA, but instead they are creating them for each other.

-Main drawback of this model is scalability. Each CA must certify every other CA that is participating & bidirectional trust path must be implemented as shown in Figure.

-Figure represents a fully connected mesh –architecture that each CA is directly connected to & has a bidirectional trust relationship with every other CA.

Q.2 c)Ilustrate Diffie-Hellman key exchange algorithm.(Explanation 4 marks & example 4 marks)

Diffie-Hellman was created in 1976 by whitefield Diffie & Martin Hellman . This protocol is one of the most common encryption protocol.

In this ,two users agrees to use two numbers, P & G with P being a sufficiently large prime number & G being the generator.

Both users pick a secret number,a &b.Then both users compute their public number.

User 1 : $X=G^a$ mod P, with X being the public number.

User 2 : $Y=G^b$ mod P, with Y being the public number

The users then exchange public numbers.

User 1 computes $Ka=Y^a$ mod P

User 2 computes $Kb=X^b$ mod P

With Ka=Kb=K, now both users know the new shared secret K.

Which is used for further encryption/decryption process?

Ex. Consider 2 large prime numbers

P=11, G=7

User1 chooses a=3

$X=G^a \bmod P$

$=7^3 \bmod 11$

X=2

User1 sends 2 to User2

User2 chooses b=6

$Y=G^b \bmod P$

$=7^6 \bmod 11$

Y=4

User2 sends 4 to User1

$Ka=Y^a \bmod P$

$Ka=4^3 \bmod 11$

Ka=9

$Kb=X^b \bmod P$

$Kb=2^6 \bmod 11$

Kb=9

Ka=Kb=9

Q. 3. a) (2 marks - Physical security description, 2 marks – Access controls)

Ans. 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 person 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 a wireless 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. **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. 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.

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.

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:

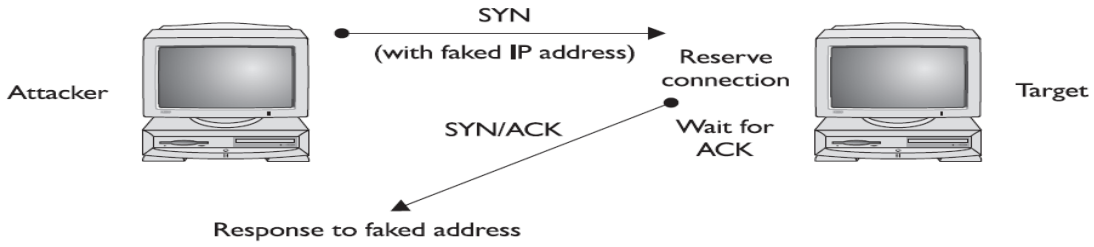
- **Discretionary Access control (DAC):** Restricting access to objects based on the identity of subjects and or groups to which they belongs to , It is conditional, basically used by military to control access on system. **UNIX based System** is common method to permit user for read/write and execute
- **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 can not 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. 3. B) (3 marks – Explanation with diagram, 1 marks – list types of DOS attack.)

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.



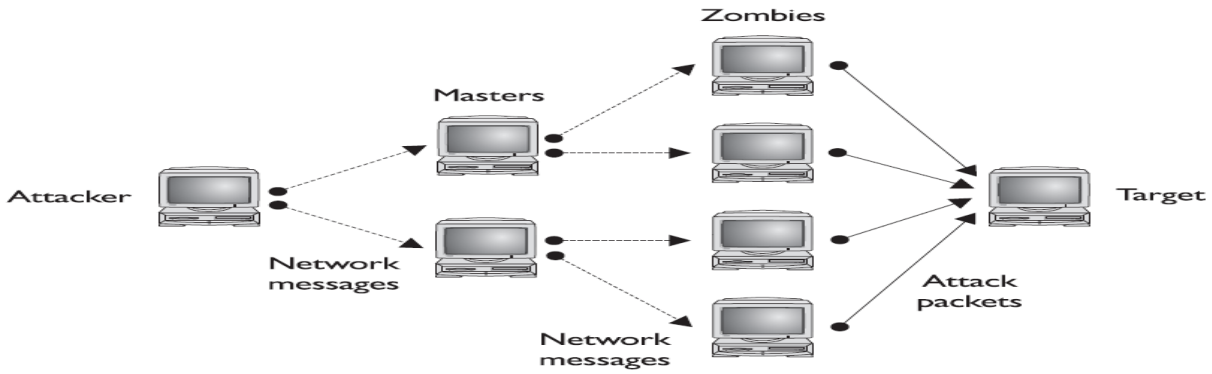
In a SYN flooding attack, the attacker sends fake communication requests to the targeted system. Each of these requests will be answered by the target system, which then waits for the third part of the handshake. Since the requests are fake (a nonexistent IP address is used in the requests, so the target 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 – 3 Marks)

Following are types of DOS (1 mark)

1.POD - ping-of-death : 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.

2. DDOS - Distributed Denial of Service attack POD : 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.



(Diagram is optional)

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. 3. c)(1 marks – Importance of individual user responsibilities, 3 marks- Explanation of procedures, policies to maintain security)

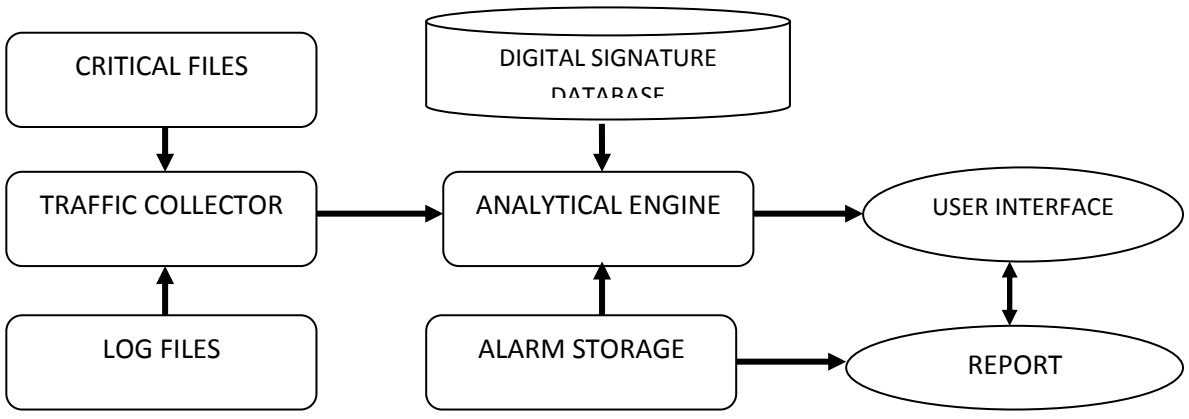
Major Security problems are because of users/ people involved in security,

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.3 d) (1 marks -Diagram of IDS, 2 Marks- component Explanation, 1 marks- List Types of IDS)



An IDS is intrusion detection system is process of monitoring the events occurring in computer system or network & analyzing tem for signs of possible incident which are threats of computer security.

IDS have following logical components

1) **Traffic collection**: collects activity as events from IDS to examine.
   On Host-based IDS, this can be log files, Audit logs or traffic coming to or leaving a system.
   On network based IDS, this is typically a mechanism for copying traffic of network link
2) **Analysis Engine**: examines collected network traffic & compares it to known patterns of suspicious or malicious activity stored in digital signature.
   The analysis engine act like a brain of IDS
3) **Signature database:** a collection of patterns & definitions' of known suspicious or malicious activity.
4) **User Interface & Reporting:** interfaces with human element, providing alerts when suitable & giving the user a means to interact with & operate the IDS.

IDS are mainly divided into two categories, depending on monitoring activity:

a) Host-based IDS:
b) Network based IDS:

(**1 mark** for listing **Log or activities optional**)

1) Host based IDS looks for certain activities in the log files are:

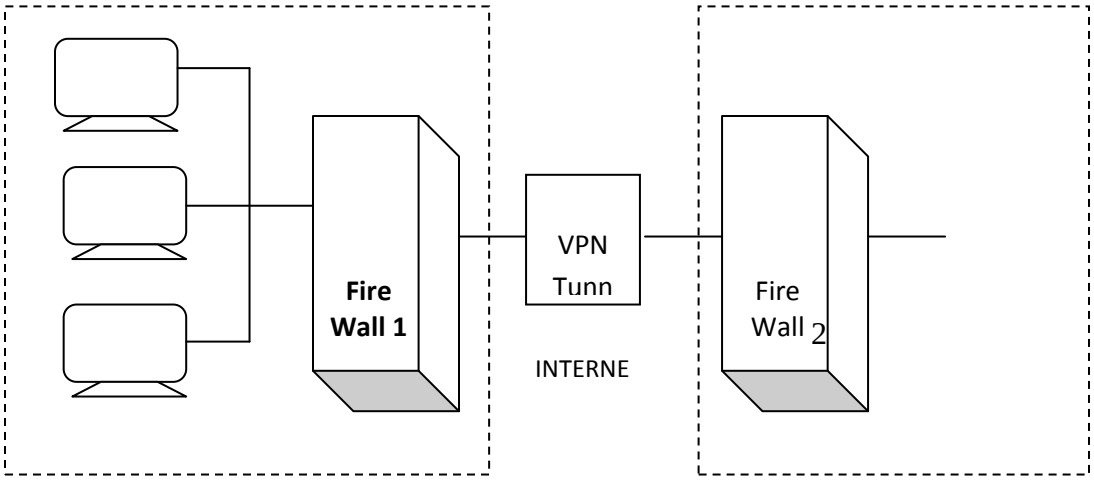
- Logins at odd hours
- Login authentication failure.
- Adding new user account
- Modification or access of critical systems files.
- Modification or removal of binary files
- Starting or stopping processes.
- Privilege escalation
- Use of certain program

2) Network based IDS looks for certain activities like:

- Denial of service attacks.
- Port scans or sweeps
- Malicious contents in the data payload of packet(s)
- Vulnerability of scanning
- Trojans, Viruses or worms
- Tunneling
- Brute force attacks.

Q.3. e) (1 Mark for Diagram , 2 Marks for Explanation, 1 Mark for steps performed while Transmission between two different networks.)

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.



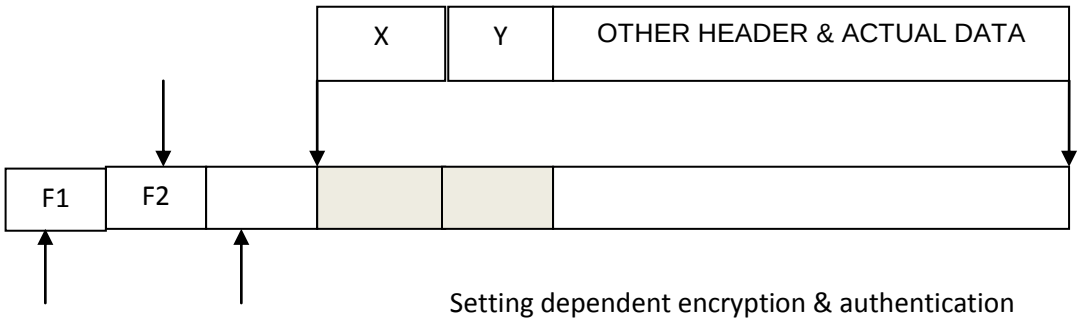
Above fig. shows that network1 connects to internet via firewall 1 & network 2 via firewall 2.

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

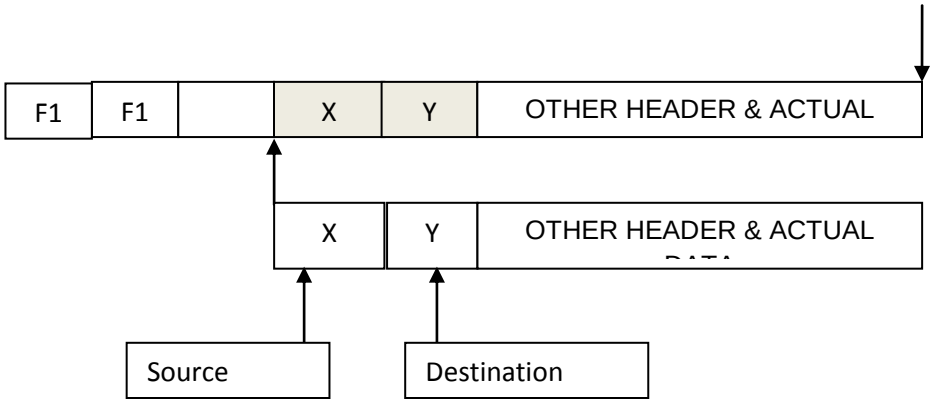
VPN protects traffic passing between two hosts or two different networks.

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.



Q.4.A- a) (1 Mark for explanation, 2 Marks for types, 1 Mark for Logic Bomb explanation)

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.

Logic bomb: are also type of malicious software that is deliberately installed, generally by authorized user. It is a Code Bomb is code embedded in some legimate program that is set to explode when certain condition occurred.

If event like not finding a specific name in the personal file., the code is refered to as Logic Bomb. If the event is a particularly date or time, program will often be refered as time bomb. They are difficult to detect.

Types of viruses:

- **Parasitic Viruses:** It attaches itself to executable code and replicates itself. Once it is infected it will find another program to infect.
- **Memory resident viruses:** lives in memory after its execution it becomes a part of operating system or application and can manipulate any file that is executed , copied or moved.
- **Non- resident viruses:** it executes itself and terminates or destroys after specific time.
- **Boot sector Viruses:** It infects boot sector and spread through a system when it is booted from disk containing virus.
- **Overwriting viruses:** It overwrites the code with its own code.
- **Stealth Virus:** This virus hides the modification it has made in the file or boot record.
- **Macro Viruses:** These are not executable. It affects Microsoft word like documents, they can spreads through email.
- **Polymorphic viruses:** it produces fully operational copies of itself, in an attempt to avoid signature detection.
- **Companion Viruses:** creates a program instead of modifying an existing file.
- **Email Viruses:** Virus gets executed when email attachment is open by recipient. Virus sends itself to every one on the mailing list of sender.
- **Metamorphic viruses:** keeps rewriting itself every time, it may change their behavior as well as appearance code.

Q.4.A- b) (1 Mark for each point of comparison or in descriptive format can be considered in paragraph or short note.)

Sr. No.	Intruders	Insiders
1	Extremely patient as time consuming	More dangerous than outsiders
2	Outsiders	Insiders
3	Keep trying attacks till success	As they have the access and knowledge to cause immediate damage to organization
4	Individual or a small group of attackers	They can be more in numbers who are directly or indirectly access the organization.
5	Next level of this group is script writers, i.e. elite hackers There are three types: 1. Masquerader 2. Misfeasor 3. Clandestine user are misuse of access given by insiders	They may give remote access to the organization.

Q.4.A- c) (2 Mark for each for sufficient explanation of both points in paragraph or short note.)

Web servers are Internet server -side application in use. These are mainly designed to provide remote access to users through web browser. They have different uses like news broadcasting, public sales, event visualization etc. They are popular targets for attackers. Nowadays web server setting is made extremely easy for vendors. Hardening server in not a difficult task. i.e. IIS.

Active directories. Allows single login access to multiple applications, data sources, and system. It is somewhat schema. It contains details about network objects like domains, servers, workstations, printers, groups and users. Active directories have ability to selectively push administrative control users in each domain. Active directory objects has an access control list(ACLs).which determine access for object with attributes and actions performed on it. Global catalog contents a subset of information on all the objects in the Active Directory database. Microsoft uses Lightweight Directory Access Protocol(LDAP) to update and query active directory. Each object has unique name for use in LDAP. It is encrypted protocol. To secure Active directories is careful planning and use of appropriate permissions. It is more secure system.

Q.4.A- d) (1 mark definition, 3 mark prevention)

Ans. 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.B- a) (3 Marks for basic mechanism 3 marks for explanation or comparison in tabular form.)

Authentication is Process of determining the identity of a user or other entity. It is performed during logon process, user-id, password; Job of authentication mechanism is to make sure validity of user.

There are three methods:

i) Something you know. i.e. User-id and password

ii) Something you have, i.e. for valid user only.

iii) Something about you i.e. unique like finger print, Retina DNA sample etc.

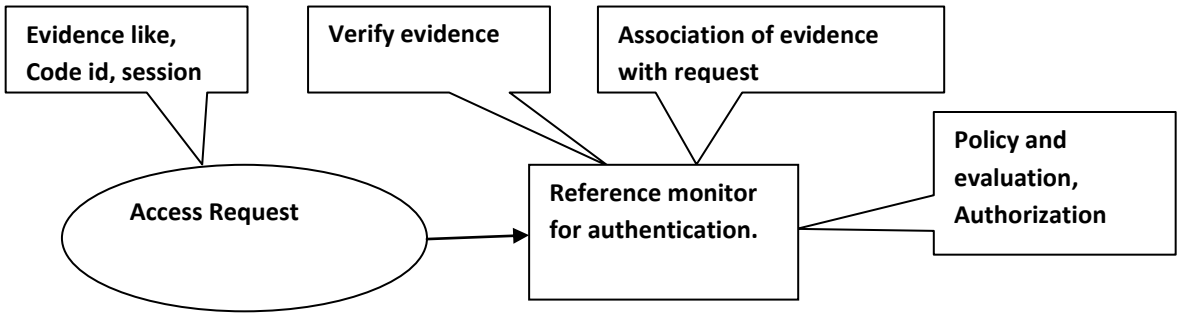


Fig. Basic mechanism

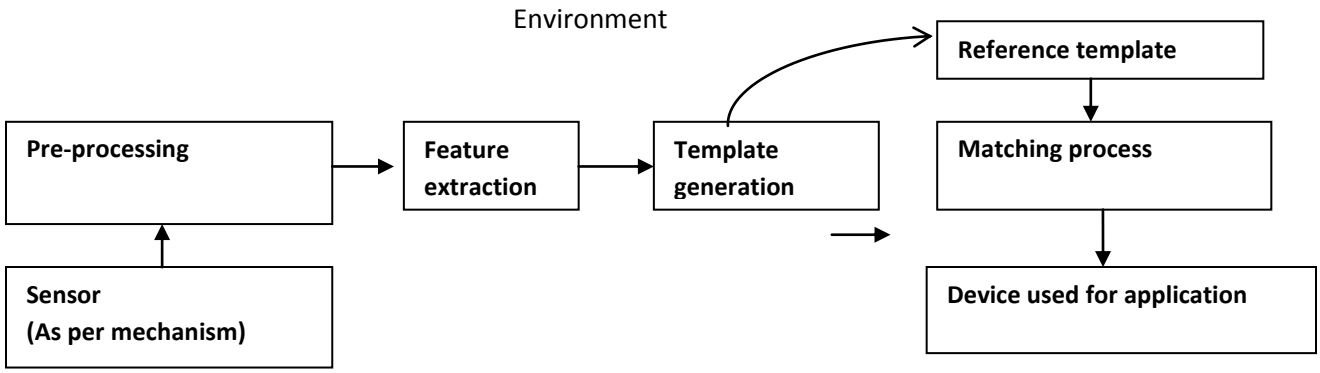


Fig. Basic Biometric system for Handprint, Retina, Voice recognition

Comparison of Handprint, Retina, Voice recognition (Minimum 4 parameters can be considered for comparison/ explanation)

Biometric	Verify	ID	Accuracy	Reliability	Error Rate	Errors	Security Level	User Acceptance	Ease of Use	Cost	Hardware
Handprint	Required	Not required	Average	Less	1 in 500	hand injury, age	Low	Low	High	High	Special, mid-price
Voice Recognition	Required	Not required	Less	Not reliable	1 in 50	noise, weather, colds	Low	High	High	Low	Common, cheap
Retina	Required	Required	High	More	1 in 131,000	poor lighting	High	Low	Medium	Low	Special, expensive

Q.4.B- b) (1-mark for each step)

The hardening of operating systems involves ensuring that the system is configured to limit the possibility of either internal or external attack. While the methods for hardening vary from one operating system to another, the concepts Involved are largely similar regardless of whether Windows, UNIX, Linux, Macros x or any other system is being base lined. Some basic hardening techniques are as follows:

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. It is important that an operating system only be configured to run the services required to perform the tasks for which it is assigned. For example, unless a host is functioning as a web or mall server, there is no need to have FITTP or SMTP services running on the system.

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. Access to files and directories must be strictly controlled through the use of Access Control Lists (ACLs) and file permissions. Some file systems provide support for encrypting files and folders. For additional protection of sensitive data, it is important to ensure that all disk partitions are formatted with a file system type with encryption features (NTFS in the case of Windows).

Enable Logging: It is important to ensure that the operating system is configured to log all activities, errors and warnings.

File Sharing: Disable any unnecessary File sharing

3. Password Management: Most operating systems today provide options for the enforcement of strong passwords. Utilization of these options will ensure that users are prevented from configuring weak, easily guessed passwords. As an additional level of security, it includes enforcing the regular changing of passwords and the disabling of user accounts after repeated failed login attempts.

4. Remove unnecessary programs: Any application which is not required should be removed. This reduces the chances of an attacker exploiting a weakness.

5. Apply latest patches and fixes: Make sure that the operating system and all applications have latest vendor-supplied patches. As an ongoing task, it is essential that all operating systems be updated with the latest vendor supplied patches and bug fixes (usually collectively referred to as security updates).

6. 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. All guest, unused and unnecessary user accounts must be disabled or removed from operating systems. it is also vital to keep track of employee turnover so that accounts can be disabled when employees leave an organization.

Q.5 a) (2-marks for Explanation, 4-marks for Types, 2-marks for Tunneling)

A Virtual Local Area Network (VLAN) is a logical network allowing systems on different physical networks to interact as if they were connected to the same physical network. A LAN is a set of devices with similar functionality and similar communication needs, typically co-located and operated off a single switch. This is the lowest level of a network hierarchy and defines the domain for a certain protocols at the data link layer for communication. A VLAN has many of the same characteristic attributes of a LAN and behaves much like a physical LAN, but it is being implemented using switches and software. This powerful technique allows administrators to perform network reconfigurations without having to physically relocate or recable systems.

Types of VLAN

1. Port based

All the traffic which arrives at a given port of switch is associated with some VLAN. In such manner you could connect several VLAN's to a single switch and have them operate concurrently.

In this when you use port based VLANs data frame received on give port is not altered but simply forwarded to correct output port.

2. MAC Based VLANs: All the traffic received is inspected for source and destination MAC addresses and then appropriate VLANs are determined.

In this all computers connect to all ports of switch and switch will associate each one to appropriate VLAN.

This types of VLAN are much easier to manage as it removes physical requirements of connecting a specific device to specific port.

Frames in VLANs may be edited to accommodate VLAN they belong to.

3. Protocol Based VLANs

This type is based upon protocol transmitted, each protocol can be assigned a different port, this allows flexibility across network

4. IP Subnet VLANs

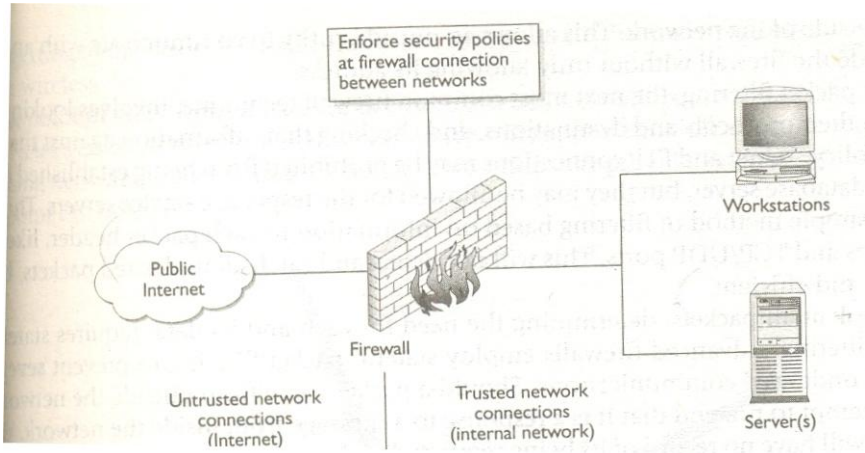
In this type VLAN is split according to IP Subnet of each source / destination.

This allows great flexibility as users are able to move computers from one location to different location.

Tunneling: Tunneling is a method of packaging packets so that they can traverse a network secure, confidential manner. This involves encapsulating packets within packet, enabling dissimilar protocols to coexist in a single communication stream as in IP traffic routed over Asynchronous Transfer Mode network. Tunneling also can provide significant measures of security and confidentiality through encryption and encapsulation methods. Because of ease of use, low cost hardware and strong security tunnels and intranet are a combination which are very much important for use in future.

Q.5 b)(3-marks for Working, 2-marks for Design Principles, 1 ½-mark for Capabilities, 1 ½-mark for Limitation)

A firewall is a network device – hardware, software or a combination thereof – whose purpose is to enforce a security policy across its connection. It is much like a wall that has a window: the wall serves to keep things out, except those permitted through the window



.

Working: Firewalls enforce the establishment security policies. Variety of mechanism include:

Network Address Translation (NAT)

Basic Packet Filtering

Stateful Packet Filtering

Access Control Lists (ACLs)

Application Layer Proxies.

One of the most basic security function provided by a firewall is Network Address Translation (NAT). this service allows you to mask significant amounts of information from outside of the network. This allows an outside entity to communicate with an entity inside the firewall without truly knowing its address.

Basic Packet Filtering, the most common firewall technique, looking at packets, their protocols and destinations and checking that information against the security policy.

Telnet and FTP connections may be prohibited from being established to a mail or database server, but they may be allowed for the respective service servers.

This is a fairly simple method of filtering based on information in each packet header, like IP addresses and TCP/UDP ports. This will not detect and catch all undesired packet but it is fast and efficient.

Capabilities:

1. all traffic from inside to outside and vice versa must pass through the firewall. To achieve this all access to local network must first be physically blocked and 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 to render attacks on it useless.

Limitations

1. firewall cannot protect against attacks that bypass the firewall
2. firewall does not protect against internal threats.
3. Firewall cannot protect against the transfer of virus infected programs or files.

Q.5 c)(4-marks for CA & RA, 4-marks for steps)

A Certificate Authority (CA) is a trusted authority that certifies individual's identities and creates electronics documents indicating that individuals are who they say they are. This electronic document is referred to as a "digital certificate", and it establishes an association between subjects identity and a public key. The private key that is associated or paired with the public key in the

certificate is stored separately. A 'CA' is made up of the software, hardware, procedure, policies and people who are involved in validating individual's identities and generating the certificates. The CA should have a certification practices statement (CPS) that outlines how the identities are verified; the steps the CA follows to generate maintain and transmit certificates, and why the CA can be trusted to fulfill its responsibilities. The CPS describes how keys are secured, what data is placed within a digital certificate and how revocations will be handles. The critical aspect is the trust between the user and the CA to ensure warranted level of trust.

Registration Authorities (RA) is the Public Key Infrastructure (PKI) component that accepts the request for a digital certificate and performs necessary steps of registering and authenticating the person requesting the certificate. The authentication requirements differ depending on the type of certificate being requested.

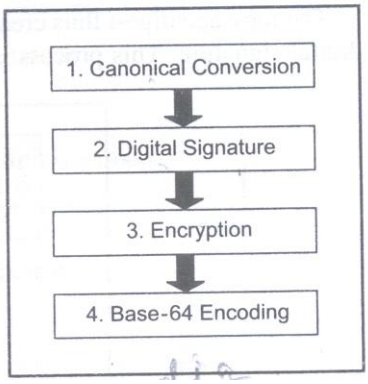
There are three classes of certificates. Class1 certificate is usually used to verify an individuals identity through email. A person who receives a Class 1 certificate can use his public /private key pair to digitally sign email and encrypt message contents. A Class 2 certificate can be used for software signing. A software vendor would register for this type of certificate, so that it could digitally sign its software. This provides integrity for the software after it is developed and released and it allows the receiver of the software to verify from where the software has actually come. A Class 3 certificate can be used by a company to set up its own CA, which will allow it to carry out its own identification verification and generate certificates internally.

Steps for obtaining a digital certificate:

1. The user registers for a digital certificate
2. Some method is used to determine random values.
3. An algorithm generates a public/private key pair.
4. The key pair is stored in a key store on the work station
5. A copy of the public key and other identifying information is sent to the CA
6. The CA generates a digital certificate containing the public key and other identifying information.
7. The new certificate is sent to the user.

Q.6 a) (1-mark for Diagram 3-marks for Explanation)

PEM Privacy Enhanced Mail (PEM) is an email security standard adapted by the Internet Architecture Board (IAB). To provide secure electronic mail communication over the internet. PEM supports three main cryptographic functions of encryption, non repudiation and message integrity. The broad level steps in PEM are as shown. PEM starts with canonical conversion which is followed by digital signature then by encryption and then finally Base 64 encoding.



PEM allows the three security options when sending an email message. These options are

Signature Only (Step 1 and 2)

Signature and Base 64 encoding (step 1, 2 and 4)

Signature, Encryption and Base 64 encoding (Steps 1 to 4)

Q.6 b) (1-mark each)

Operating system are large and complex mixes of interrelated software modules written by large number of separate individuals. With GUI based functionality OS systems continues to grow and expand. It is almost impossible for an OS vendor to test product on each and every possible platform under every possible circumstance. Hence functionality and security issues do arise after the release of OS. To an average user or system administrator it means a constant stream of updates designed to correct problems, replace sections of code or even add new features to an installed OS.

OS vendors typically follow a hierarchy for software update.

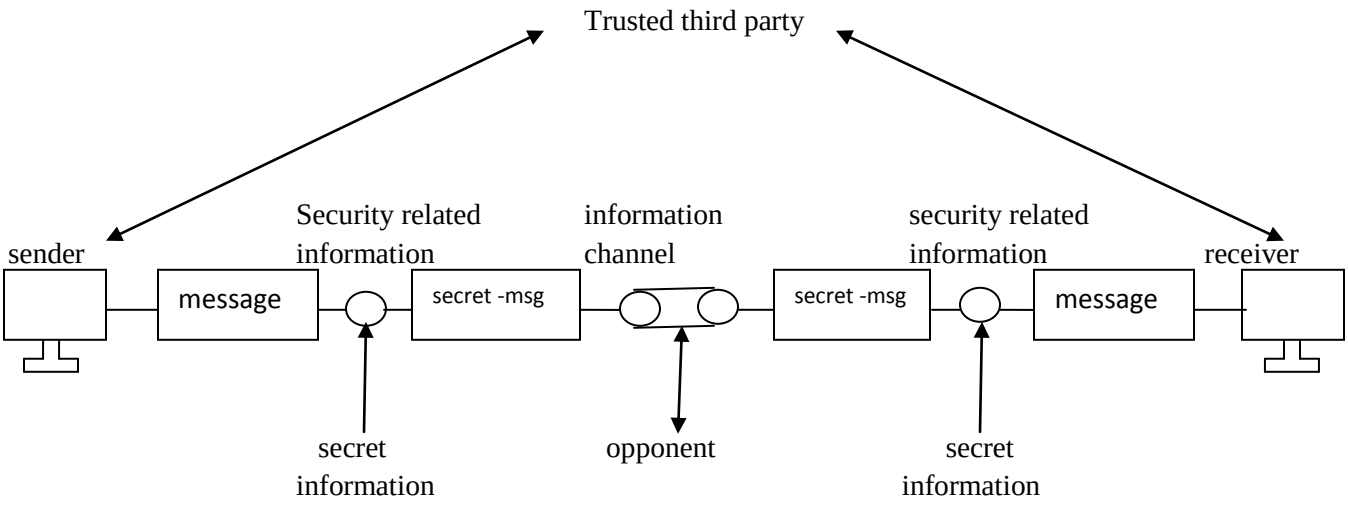
Hotfix: It is a small software update designed to address a specific software problem such as a buffer flow in an application that exposes the system to attacks. There are typically reactions to the developed problems and are produced and delivered quickly. Hotfixes address critical security related issues and should be applied to the affected application or OS as soon as possible.

Patch: This form is used to a more formal. Larger software update that may address several or many other software problems. Patches often contain enhancements or additional capabilities as well as fixes for known bugs. Patches are usually developed over a long period of time.

Service Pack: This form is given to a larger collection of patches and hotfixes rolled into a single one larger package. These are designed to bring system up to the latest known performance level. The administrator should download dozens of updates separately.

Q.6 c) (1-mark for diagram, 3-marks for explanation)

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:

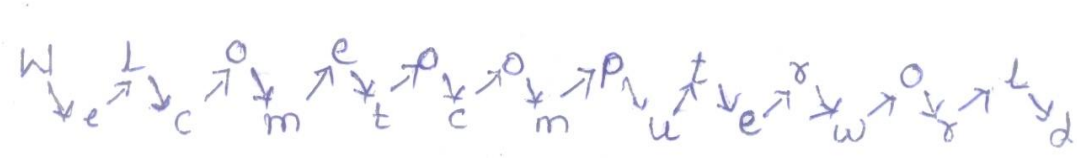
1. Design algorithm in such a way that an opponent cannot defeat its purpose. This algorithm is used for security related information.
2. Generate secret information that can be used with algorithm.
3. Develop method for distributing and sharing of secret information.
4. Specify a protocol which can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

Q.6] d)(1-mark for definition, 2-marks for Step 1, 1-mark for Step 2)

When plain text message is codified using any suitable scheme, the resulting message is called Cipher text or Cipher.

Plain text = Welcome to Computer World

1. Write down Plain text as sequence of diagonal.



2. Read Plain text written in Step 1 as sequence of rows.

   wloeooptrolecmtcmuewr = cipher text.

Q.6 e) (1-mark for definition, 1 ½ mark for Advantages & 1 ½ mark for drawbacks)

Steganography is a technique that facilitates hiding of message that is to kept secret inside other message.

Advantages:

1. With the help of steganography we can hide secret message within graphics images.
2. In modern Steganography, data is encrypted first and then inserted using special algorithm so that no one suspects its existence.

Drawbacks:

1. It requires lot of overhead to hide a relatively few bits of information.
2. Once the system is discovered, it becomes virtually worthless.