MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17514 **Model Answer**

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.
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) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.

Q.1) a) Attempt any three of the following: 12

1) Describe security principles based on CIA.

(Meaning of CIA-1M, explanation of each point-1M, example optional)

Ans.

The security principles based on CIA are : confidentiality, integrity, and authentication—the "CIA" of security.

1. Confidentiality: The principle of confidentiality specifies that only sender and intended recipients should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the contents of a message.

Example of compromising the Confidentiality of a message is shown in fig.

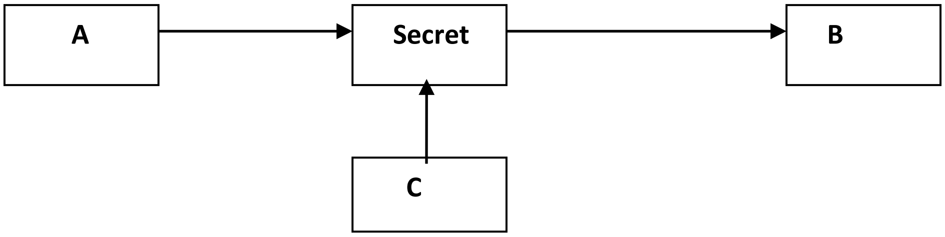


Fig. Loss of confidentiality

Here, the user of a computer A send a message to user of computer B. another user C gets access to this message, which is not desired and therefore, defeats the purpose of Confidentiality.
This type of attack is also called as interception.

2. Authentication: Authentication helps to establish proof of identities. The Authentication process ensures that the origin of a message is correctly identified.
For example, suppose that user C sends a message over the internet to user B. however, the trouble is that user C had posed as user A when he sent a message to user B. how would user B know that the message has come from user C, who posing as user A? This concept is shown in fig. below.
This type of attack is called as fabrication.

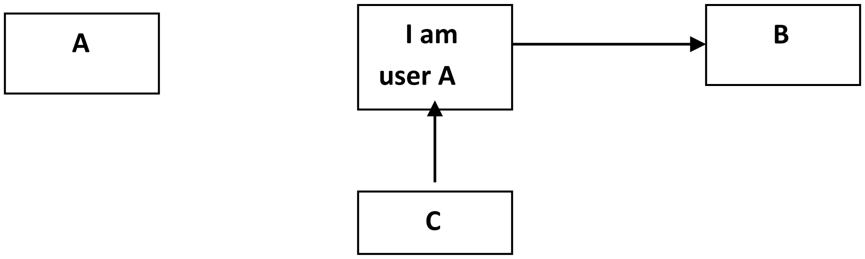


Fig. Absence of authentication

3. Integrity: when the contents of the message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost.
For example, here user C tampers with a message originally sent by user A, which is actually destined for user B. user C somehow manages to access it, change its contents and send the changed message to user B. user B has no way of knowing that the contents of the message were changed after user A had sent it. User A also does not know about this change.

This type of attack is called as **modification**.

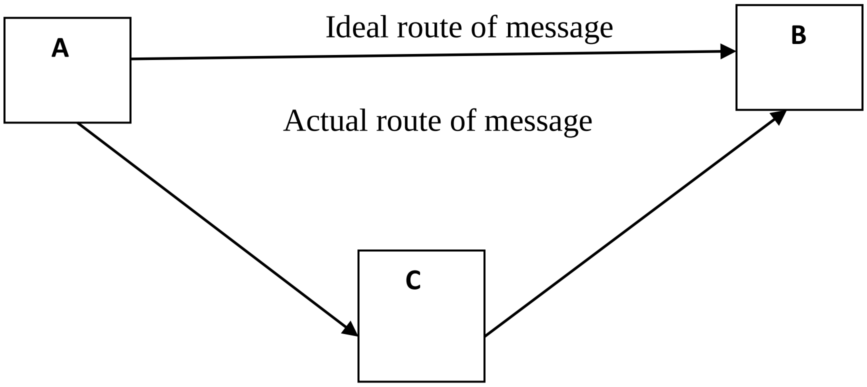


Fig. Loss of Integrity

2) **Explain piggybacking.**
(Explanation -2M, example- 2M)

Ans.

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.

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. 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.

Example: Access of wireless internet connection by bringing one's own computer within the range of another wireless network & using that without explicit permission.

3) **Compare symmetric and asymmetric key cryptography.**
(Each comparison point- 1M, any four points)

Ans.

Categories	Symmetric key Cryptography	Asymmetric key Cryptography
Key used for encryption /decryption	Same key is used for encryption & decryption.	One key is used for encryption & another different key is used for decryption.
Key process	Ke=Kd	Ke# Kd
Speed of encryption/decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original clear text size.	More than the original clear text size.
Key agreement/exchange	A big problem	No problem at all.
Usage	Mainly used for encryption and decryption, cannot be used for digital signatures.	Can be used for encryption and decryption as well as for digital signatures.
Efficiency in usage	Symmetric key cryptography is often used for long messages.	Asymmetric key cryptography are more efficient for short messages.

4) **Describe terms regarding computer security.**
i) Assets **ii) Vulnerability**
iii) Threats **iv) Risk**
(1M for each term)

Ans.

i. Assets: Asset is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware, software and confidential information.

ii. Vulnerability: It is a weakness in computer system & network.

iii. Threats: It is a set of things which has potential to loss or harm to computer system & network.

iv. Risk: Risk is probability of threats that may occur because of presence of vulnerability in a system.

Q.1) b) Attempt any one of the following: **6**

1) **Explain model of security with block diagram.**
(Explanation of each point with diagram- 2M)

Ans.

CIA Model for security:

1. Confidentiality: The principle of confidentiality specifies that only sender and intended recipients should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the contents of a message.

Example of compromising the Confidentiality of a message is shown in fig:

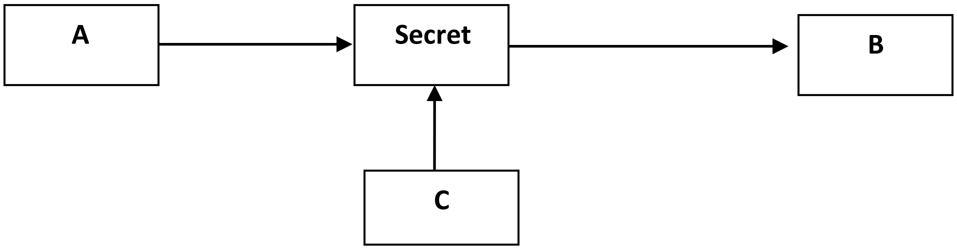


Fig. Loss of confidentiality

Here, the user of a computer A send a message to user of computer B. another user C gets access to this message, which is not desired and therefore, defeats the purpose of Confidentiality.

This type of attack is also called as **interception.**

2. Authentication: Authentication helps to establish proof of identities. The Authentication process ensures that the origin of a message is correctly identified.

For example, suppose that user C sends a message over the internet to user B. however, the trouble is that user C had posed as user A when he sent a message to user B. how would user B know that the message has come from user C, who posing as user A? This concept is shown in fig. below.

This type of attack is called as **fabrication.**

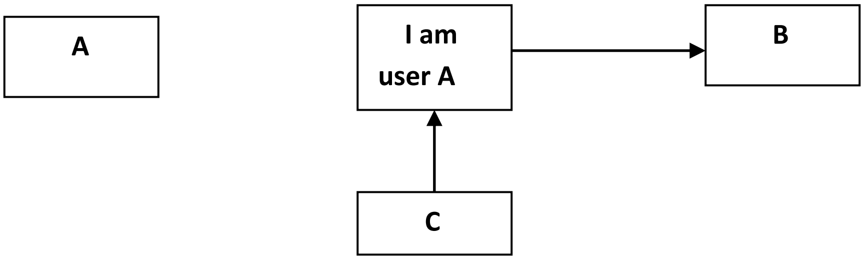


Fig. Absence of authentication

3. Integrity: when the contents of the message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost.

For example, here user C tampers with a message originally sent by user A, which is actually destined for user B. user C somehow manages to access it, change its contents and send the changed message to user B. user B has no way of knowing that the contents of the message were changed after user A had sent it. User A also does not know about this change.

This type of attack is called as **modification**.

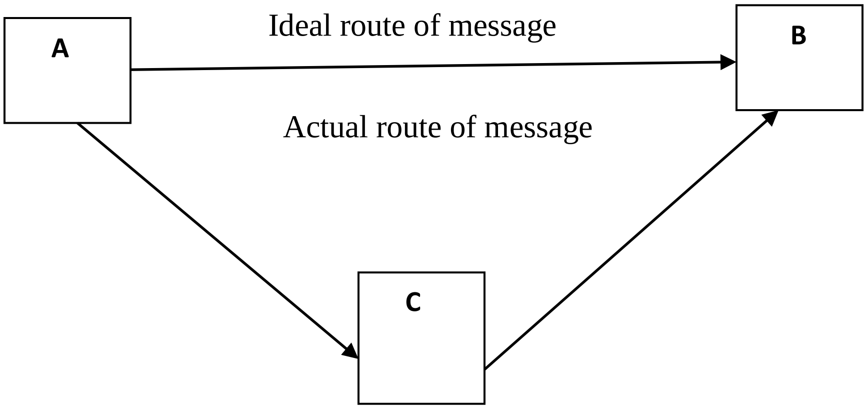


Fig. Loss of Integrity

2) Explain data recovery tools and procedures.
(Explanation of data recovery 4M, procedures-2M)

Ans.

Data recovery: All computer users need to be aware of backup and recovery procedures to protect their data. Data Protection can be taken seriously as its important for financial, legal or personal reasons.

These are various formatted partition recovery tool available .Although every tool will have different GUI & method of recovery.

Steps of data recovery:

Step1: If you cannot boot the computer, please use data recovery bootable disk.

Step 2: Select the file types you want to recover & volume where the formatted hard drive is. The tool will automatically scan the selected volume.

Step 3: Then the founded data will be displayed on the screen & you can get a preview of it. Then select the file or directory that you want to recover & save them to a healthy drive.

Data recovery procedures:

- A computer data recovery procedure is an important part for any computer literate personality that cannot be neglected. Computer professional or computer forensic expert who uses data recovery should maintain the secrecy and privacy of the client.

- Any action or activity that leads to disclosure of privacy of the client should be avoided.
- The values such as integrity, accuracy & authenticity should be exercised in an ethical environment. The evidence that is produced before the court should be fairly examined & analyzed. There should not be any carelessness and ignorance regarding the handling of evidence. The case evidence should be examined in detail based upon validated principles.

Q.2) Attempt any two of the following: 16

1) Explain any four attacks on computer systems security.
(Explanation of each attack- 2M, any four attacks)

Ans.

Different types of attacks are as follows:

i. Denial-of-service attacks
ii. Backdoors and Trapdoors
iii. Sniffing
iv. Spoofing
v. Spoofing E-mail
vi. Man In middle attack
vii. Replay attacks
viii. TCP/ IP Hijacking

ix. Attacks on Encryption
x. Malware or malicious code such as viruses

1. Denial-of-service attacks can exploit a known vulnerability in a specific application or o.s, or may attack features in specific protocols or services. In this form attacker is trying to deny authorized users access either to specific information or to the computer system or either network. The purpose of such an attack is to simply prevent access to target system or the attack may be used in conjunction with other action in order to gain unauthorized access to system or network. SYN flooding attack is one of the examples of this type.

2. Backdoors and Trapdoors: They are the methods used by software developers to ensure that they could gain access to an application even if something were to happen in the future to prevent normal access methods. For e.g. A hard coded password that could be used to gain access to the program in the event that administrator forgot their own system password. The problem with this sort password (sometimes referred to as trapdoor) is that since the password is hard coded it cannot be removed. If the attacker learns about the backdoor, all systems running the software would be vulnerable.

3. Sniffing: A network sniffer is a software or hardware device that is used to observe the traffic as it passes through the network on shared broadcast media. The device can be used to view all traffic, all it can target a specific protocol, service or even string of characters. Normally the network device that connects a computer to a network is designed to ignore all traffic that is not destined for that computer. Network sniffers ignore this friendly agreement and observe all traffic on the network whether destined for that computer or others.

4. Spoofing: It makes the data look like it has come from other source. This is possible in TCP/IP because of the friendly assumptions behind the protocols. When a packet is sent from one system to another, it includes not only the destination IP address but the source IP address. The user is supposed to fill in the source with your own address, but there is nothing that stops you from filling in another system's address.

2) Explain at least four roles of peoples in security.
(Explanation of each role – 2M, any four roles, examples optional)

Ans.

Role of people in security

1. Password selection:

1) User should be able to create their own easy to remember passwords, but should not be easy for someone else to guess or obtain using password cracking utilities.

2) Password should meet some essential guidelines for eg.pw should contain some special characters etc.
3) It should not consist of dictionary words. Etc

2. 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.

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. 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.

Example: Access of wireless internet connection by bringing one's own computer within the range of another wireless network & using that without explicit permission.

3. Shoulder surfing is a similar procedure in which attackers position themselves in such a way as-to be-able to observe the authorized user entering the correct access code or data.

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 idea of binoculars or other vision-enhancing devices.

To prevent shoulder surfing, experts recommend that you shield paper work or your keypad from view by using your body or cupping your hand.

4. Dumpster diving:-Dumpster is diving is the process of going through a target's trash in order to find little bits of information.

In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. The search is carried out in waste paper, electronic waste such as old HDD, floppy and CD media recycle and trash bins on the systems etc.

To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company should establish disposal policy.

5. Installing Unauthorized Software/Hardware: because of possible risks, many organizations do not allow their users to load software or install new hardware without the information and help of administrators. Organizations also restrict what an individual do by received e-mails.

6. **Access by non-employees**: If attacker can get physical access to a facility then there are many chances of obtaining enough information to enter into computer systems and networks. Many organizations restrict their employees to wear identification symbols at work.

7. **Security awareness**: Security awareness program is most effective method to oppose potential social engineering attacks when organization's security goals and policies are established. An important element that should concentrate in training is which information is sensitive for organization and which may be the target of a social engineering attack.

8. Individual user responsibilities:

i) Lock the door of office or workspace.

ii) Do not leave sensitive information inside your car unprotected.

iii) Secure storage media which contains sensitive information.

iv) Shredding paper containing organizational information before discarding it. (More points can be added).

3) Explain SHA-1 algorithm with diagram.

(Explanation -6M, Diagram- 2M)

*****Note: Relevant answer shall be considered***

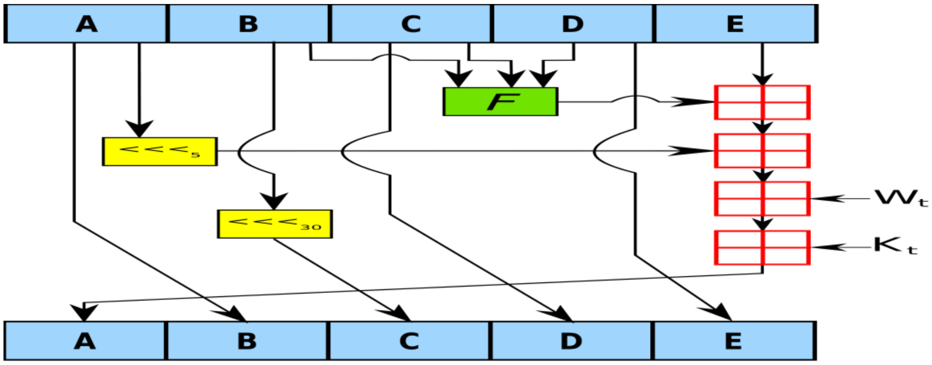
Ans.

SHA-1 is secure hashing algorithm. It is used create message digest or hash value of original message. SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function .

A hash is a special function that performs one way encryption meaning that once the algorithm is processed, there is no feasible way to take the cipher text and retrieve the plain text that was used to generate it.

Algorithm steps:

- Hashing starts with 160-bit seed as hash value.
- A sequence of non-linear operation is carried out on the first message block 512-bits.
- The sequence is cyclically repeated 80 times and a 160 bit hash value is generated.
- The cyclic sequence is repeated for the second message block of 512 bits.
- The process is continued until all the N message block have been hashed and the final 160bit hash value is generated.



Q.3) Attempt any four of the following: 16

1) Explain the concept of Kerberos.

(1M Concept, 3M –Diagram/ Explanation of Kerberos)

Ans.

Kerberos is a network authentication protocol. This is developed by MIT. It's taken from mythology; Kerberos was a three headed dog who guards gates of Hades. It is secure method for authentication of request for a service in a computer network. It provides strong authentication for client/server application by using secret-key cryptography. From Kerberos allows a user request an encrypted "Ticket" from an Authentication process that can be used to request a particular service from server. The user password does not have to pass through the network.

It Consists of:

- User
- Authentication service and
- Ticket granting server
- Service server

Working of Kerberos:

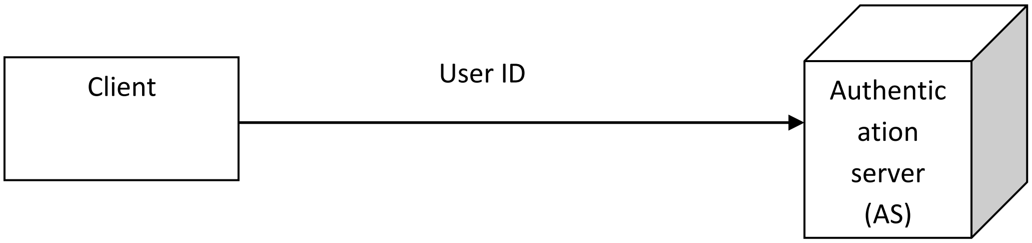
User want to access server, it needs a Kerberos ticket before request.

- Request Authentication from request Authentication server (AS), It creates "session key-encryption key "based on your password, its effectively a Ticket-granting ticket.
- User sends his/her ticket granting ticket to ticket granting server(TGS), it may be physically same server as Authentication server, Now TGT returns the ticket that can be sent to the server for the requested service.
- The service rejects the ticket or accepts it to perform service.

- Ticket received from TGT is a Time-stamped, It allows user to make additional request using same ticket within a certain time period without re-authentication. This improves security as ticket is granted for limited time period.

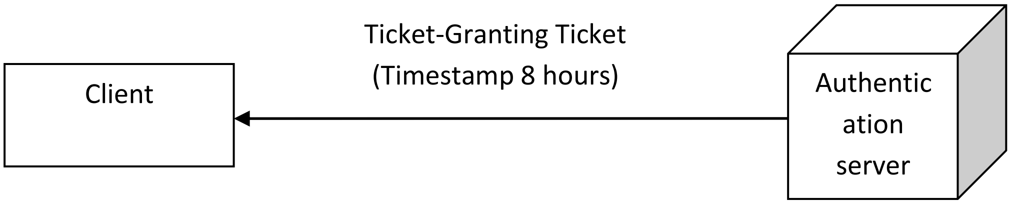
- **Following diagrams optional**

a)

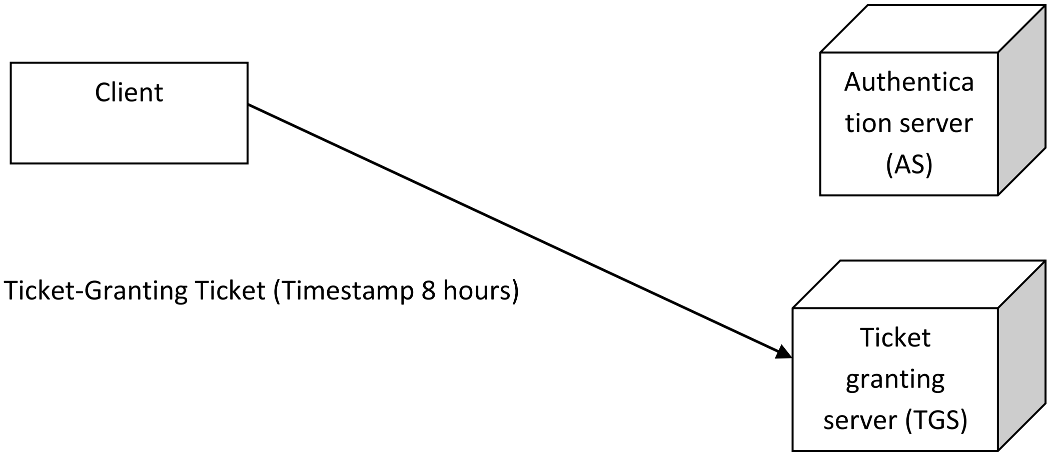


Authentication service receives the request by client and verifies that the client is indeed the authentic computer. It's valid for time-stamp allotted (i.e. 8 hours).

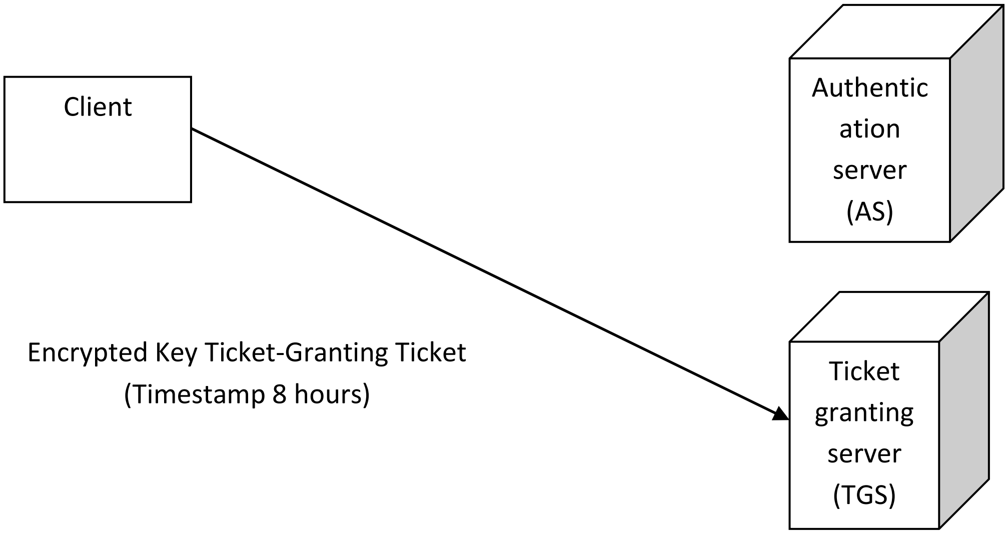
b)



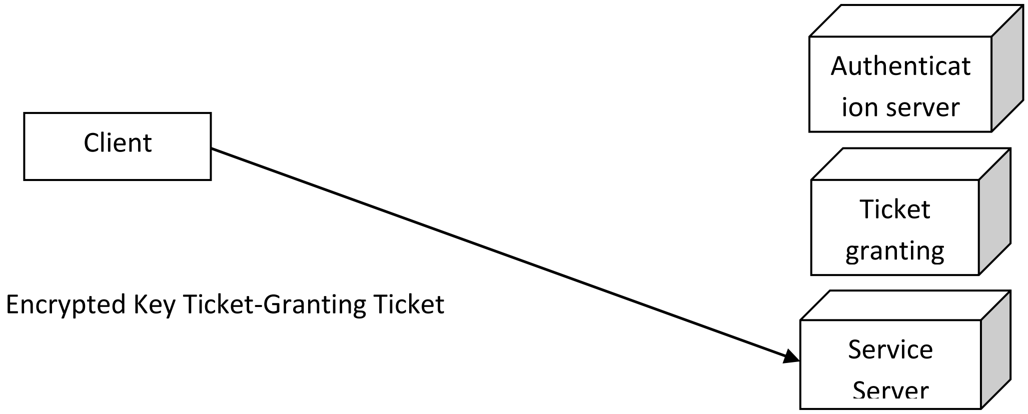
c)


Client
Authentication server (AS)
Ticket-Granting Ticket (Timestamp 8 hours)
Ticket granting server (TGS)

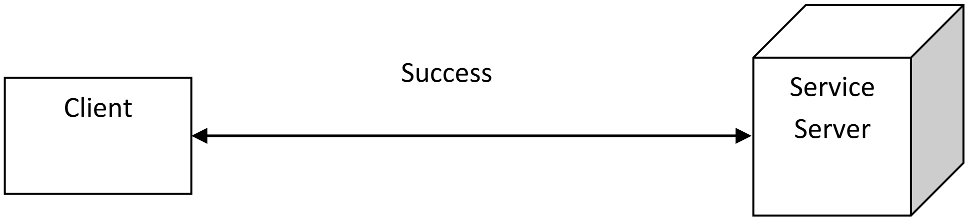
d)


Client
Authentication server (AS)
Encrypted Key Ticket-Granting Ticket
(Timestamp 8 hours)
Ticket granting server (TGS)

e)


Authentication server
Client
Ticket granting
Encrypted Key Ticket-Granting Ticket
Service Server

f)


Success
Client
Service Server

2) Describe the process of biometric authentication with neat labelled diagram for finger print.

(Basic Diagram of biometric authentication 2M, explanation of process 2M)

Ans.

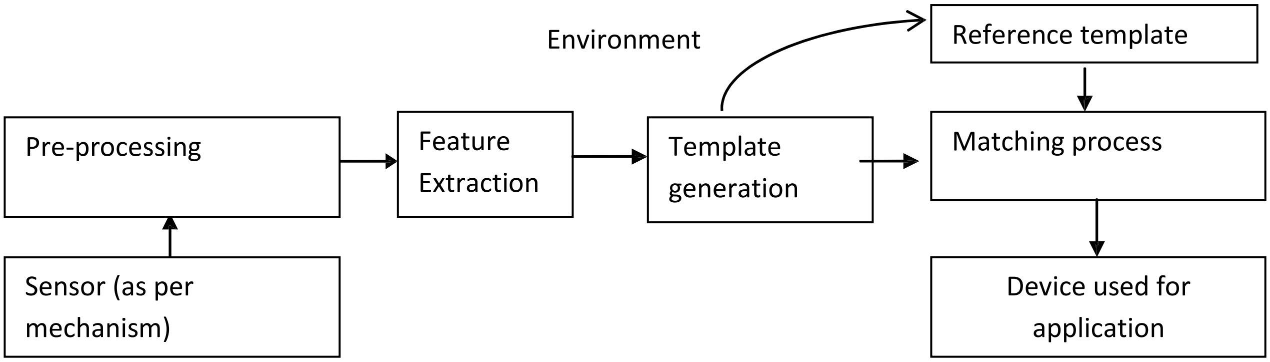


Fig. Basic Biometric system

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: A physical barrier helps in implementing physical world equivalent of layered security.

3) Explain use of S-Box in implementation of DES algorithm.

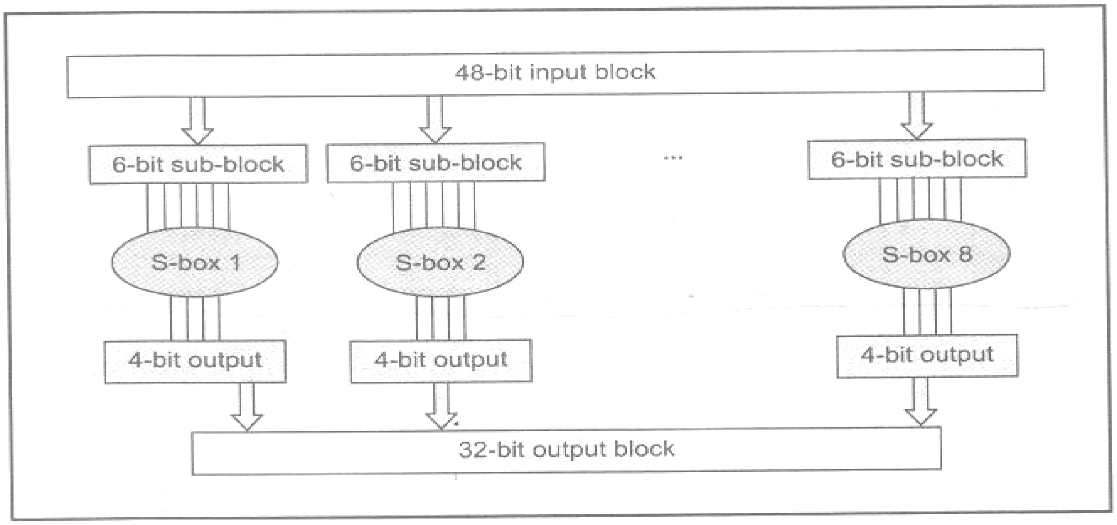
(2M Explanation of S-box Substitution, 2M diagram, steps of DES optional)

Ans.

The Data Encryption Standard is generally used in the ECB, CBC, or the CFB mode. DES is a block cipher. It encrypts data in blocks of size 64 bits each. That is, 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. DES is based on the two fundamental attributes of cryptography:

Substitution and transposition

S-box substitution: it accepts the 48-bits input from the XOR operation involving the compressed key and expanded RPT and produces 32-bit output using the substitution techniques. Each of the 8 S-boxes has a 6-bit input and a 4-bit output. The output of each S-box then combined to form a 32-bit block, which is given to the last stage of a round.



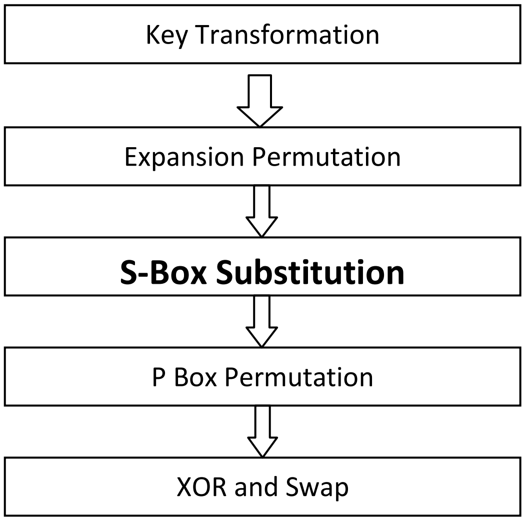


Fig. Details of one round in DES

4) **Explain working of PGP email security.**
(2M Explanation, 2M working)

Ans.

Pretty Good Privacy is a popular program used to encrypt and decrypt email over the internet. It becomes a standard for e-mail security. It is used to send encrypted code (digital signature) that lets the receiver verify the sender's identity and takes care that the route of message should not change. PGP can be used to encrypt files being stored so that they are in unreadable form and not readable by users or intruders It is available in Low cost and Freeware version. It is most widely used privacy ensuring program used by individuals as well as many corporations.

Working of PGP:

1. **Authentication:** Here sender creates message, SHA-1 used to generate 160 bit hash table of message. The hash code is encrypted using the sender's private key and the result is pretended to the message. Receiver uses senders public key to decrypt and recover the hash table. Receiver generates new hash code and is compared with decrypted hash code. If match found then message is authentic.
2. **Confidentiality:**
   This is Basic service provided by PGP. It provides an encrypted message to be transmitted or stored locally as file. Sender generates a message and random 128 bit no. used as a session key only for this message, which is encrypted. Session key is used to decrypt the message.

5) **Explain the steps for hardening applications.**
(Explanation 4M)

Ans.

Application Hardening is a security feature designed to avoid/prevent exploitation of various types of vulnerabilities in software application. It also secures against local and internet attacks. Vulnerabilities are introduced by programmers who fail to check the properly the input data entering into the application. If there are vulnerabilities in application then it can be exploited by an attacker.

Hardening application is fairly similar to hardening operating system- you remove the functions or components you do not need, restrict access where you can and make sure that the application is kept up to date with patches & maintain application patches.

Application hardening has following mechanisms:

a) Process spawning Control: uses fact that in most cases the application does not need the ability to launch other executable for proper functioning. By taking away the process spawning ability from the application, hackers will not be able to perform the process spawning attack.

b) EXE file protection: another method to break into system is to trick the vulnerable application into modifying or creating executable file protection defense is based on in most of the cases, the application does not need to create or modify executable files. Hackers will not be able to perform attacks tampering with executable files on the system.

c) System tampering protection: Another possibility to break into the system is to trick the vulnerable application into modifying special sensitive area of the operating system and taking advantage of those modifications. Those sensitive areas include Windows registry keys used to control launching of application on system startup the system.ini and win.ini files… The system tampering protection defense is based on the fact that in almost all cases normal applications do not need to perform such operations for their proper function, by preventing applications to modify special areas of Operating system. Hackers will not be able to attack by tampering with sensitive special areas of the system.

Application Patches will be helpful in this case like Hotfixes, Patches, and upgrades.

Q.4) a) Attempt any three of the following: 12

1) Explain concept of Hashing with example and properties.

(Explanation 2M, properties of hash function 2M)

Ans.

Hashing:

- Hashing functions are one of the most commonly used encryption methods.
- A hash is a special function that performs one-way encryption, meaning that once the algorithm is processed, there is no feasible way to take the cipher text and retrieve the plain text that was used to generate it.
- The hash code is a function of all bits of the message and provides as error detection capability. A change in any bit or bits results in a change of hash value.
- A hash value h is generated by a function H of the form

  h = H(M)

  where,

  M is variable length message and
  H(M) is the fixed length hash value.

- The hash value is appended to the message at the source at a time when the message is assumed or known to be correct.
- The receiver authenticates that message by re-computing the hash value. Hash value is not considered to be secret so something is required to protect the hash value.
- The message plus concatenated Hash code is encrypted using symmetric encryption. Sender and receiver share the same secret key. The message must have come from authorized sender and has not been altered is checked by recomputing and comparing hash code by receiver.

Hash value should have following **properties** for message authentication:

1. H can be applied to a block of data of any size.
2. H produces a fixed length output.
3. H(X) is relatively easy to compute for any given x making both hardware and software implementation practical.
4. For any given value of h , it is computationally infeasible to find x such that H(X) = h This is referred to as the one way property.
5. For any given block of x, it is computationally infeasible to find y $\neq$ x with H(y) = H(x)
6. This is referred to as weak collision resistance.

2) Describe following term:

i) DMZ **ii) Internet**

iii) Intranet **iv) IDS**

(1M for each point, explanation in short)

Ans.

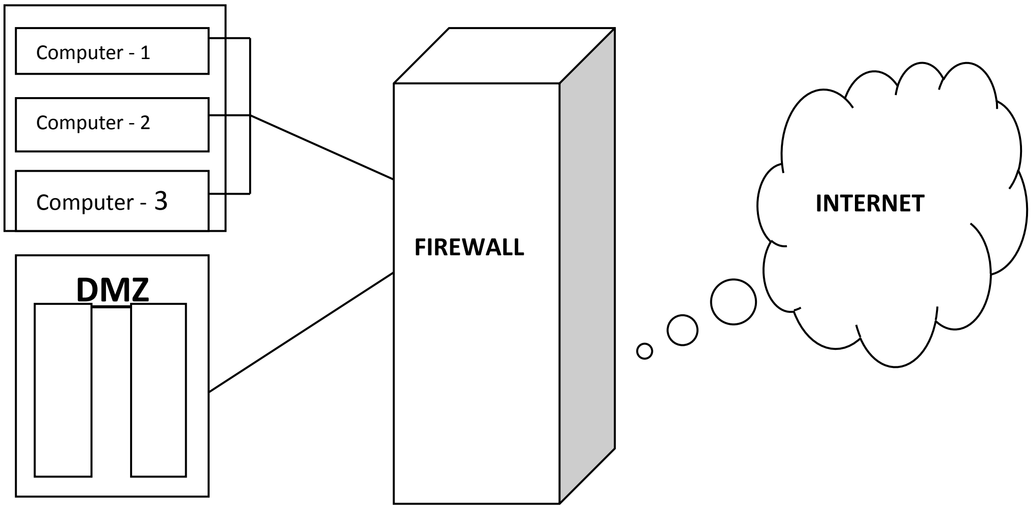
i) DMZ (Demilitarized Zone):

It is a Computer host or small network inserted as a neutral zone between a company private network and public network. It prevents outside users from getting direct access to a server that has company data. A DMZ is an optional and more secure approach to a firewall and effectively acts as proxy server. In DMZ a separate computer or host in network terms receives requests from users within the private network to provide access to web sites or other companies accessible on the public network. DMZ host initiates sessions for request on public networks. DMZ host is not able to initiate a session back into the private network. It only forward packets that have already been requested. Users of the public network outside the company can access only the DMZ host.

DMZ may also have the company’s web pages so these could be served to the outside world. DMZ provides access to no other company data.

CISCOS are the leading makers of routers those facilitate for setup of DMZ.

(Diagram or description (Any one can be considered) 1 Mark)



ii) Internet:

Internet is a network that can be used to transfer email , financial records, files, remote access etc. from one network to another network.

It is not a single network it is series of interconnected network, that allows protocol to operate to make possible a data flow across network. WWW (World Wide Web) term is used with internet. It is based on HTTP (Hypertext Transfer Protocol service) This can have different actual services and contents, including files, images, audio, video and even viruses and worms.

iii) Intranet:

Intranet is a private network that is contained within an organization/enterprise. It may consists of interlinked local area networks also use leased lines in the wide area network. It includes connections through one or more gateway computers to the outside Internet. The main purpose is to share company information and computing resources among employees. It facilitates working in groups and for teleconferences. Intranet uses TCP/IP, HTTP, and other Internet protocol.

When part of an intranet is made accessible to customer, partners suppliers or outside the company, then it becomes part of an extranet.

iv) IDS (Intrusion Detection system):

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 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.

3) Explain cyber crime.
(Relevant Explanation of cybercrime -4M)

Ans.

Crimes against people are a category of crime that consists of offenses that usually involve causing or attempting to cause bodily harm or a threat of bodily harm. These actions are taken without the consent of the individual the crime is committed against, or the victim. These types of crimes do not have to result in actual harm - the fact that bodily harm could have resulted and that the victim is put in fear for their safety is sufficient.
i.e. Assault, Domestic Violence, Stalking

Cybercrime is a bigger risk now than ever before due to the sheer number of connected people and devices. 'Cybercrime, as it's a bigger risk now than ever before due to the sheer number of connected people and devices. it is simply a crime that has some kind of computer or cyber aspect to it. To go into more detail is not as straightforward, as it takes shape in a variety of different formats.

Cybercrime:

- Cybercrime has now surpassed illegal drug trafficking as a criminal moneymaker
- Somebody's identity is stolen every 3 seconds as a result of cybercrime
- Without a sophisticated security package, your unprotected PC can become infected within four minutes of connecting to the Internet.

Criminals committing cybercrime use a number of methods, depending on their skill-set and their goal. Here are some of the **different ways cybercrime can take shape:**

- Theft of personal data
- Copyright infringement
- Fraud
- Child pornography
- Cyber stalking
- Bullying

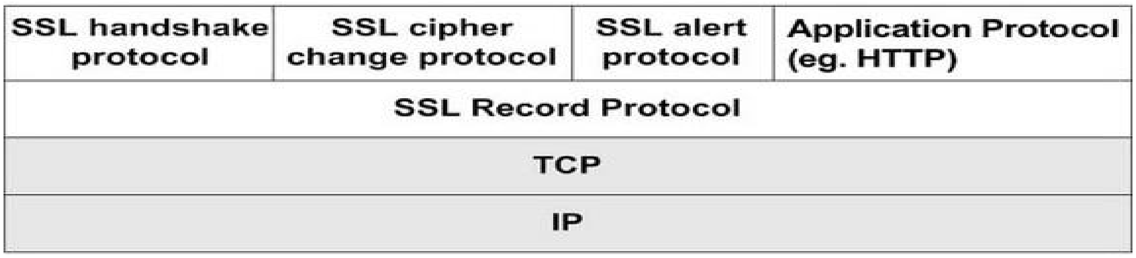
Cybercrime covers a wide range of different attacks, that all deserve their own unique approach when it comes to improving our computer's safety and protecting ourselves. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. The crime may take place on the computer alone or in addition to other locations. The broad range of cybercrime can be better understood by dividing it into two overall categories.

4) Explain working of Handshake protocol in SSL.
(Explanation of Handshake protocol 2M, Listing four phases 2M)

Ans.

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). Netscape Navigator browser provided with SSL-enabled client software.

SSL protocol stack:
The SSL protocol stack is illustrated in Figure



<table>
<tr><td>SSL handshake protocol</td><td>SSL cipher change protocol</td><td>SSL alert protocol</td><td>Application Protocol (eg. HTTP)</td></tr>
<tr><td colspan="4">SSL Record Protocol</td></tr>
<tr><td colspan="4">TCP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

The SSL Protocol Stack:
Message types are:
Hello request, Client hello, Server hello, Certificate, server key exchange, Certificate request, Server hello done, Certificate verify, Client-key exchange, finished.

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.

It can be **divided into 4 phases** separated with horizontal broken lines.

- **Establish security capabilities**
  Client hello, then server replies hello
- **Server authentication and key exchange**
  Certificate, Server key exchange, Certificate request, Server hello done
- **Client authentication and key exchange**
  Certificate, client key exchange, Certificate verify
- **Finish**
  Change cipher specification, finished,

Q.4) b) Attempt any one of the following: 6

1) Define attack. Explain steps in attack.
(Definition 2M, Steps 4M)

Ans.

Attack on computer system is either by specifically targeted by attacker, or an opportunistic target.

Attacks may have having following steps:

Interception: concept of confidentiality, Here an unauthorized party has gained access to a resource, it can be person, program, or computer based system. i.e. copying of data or programs, listening to network traffic.

Fabrication: concept of authorization, It involves the creation of illegal objects on a computer system. i.e. attacker adds fake records to data base.

Modification: Its under Integrity, Here attacker may modify the values in the database.

Interruption: It’s related to availability, Here Resources become unavailable, Lost or unusable, i.e. denial of service, problem causing to a hardware device, erasing program, data, or operating system components.

2) Define virus. Explain atleast 5 types of viruses.
(Definition 1M, Five types of virus with explanation 1M each)

Ans.

Viruses: A program designated to spread from file to file on a single PC , it does not intentionally try to move to another PC and it must replicate and execute itself. Used as delivery tool for hacking.

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 everyone on the mailing list of sender.
- **Metamorphic viruses:** keeps rewriting itself every time, it may change their behavior as well as appearance code.

Q.5) Attempt any two of the following: 16

1) Explain what are components of good password and four password selection strategies.

(Any four components: 1M each, Four Strategies: 1M each)

Ans.

Components of good password:

1. It should be at least eight characters long.
2. It should include uppercase and lowercase letters, numbers, special characters or punctuation marks.
3. It should not contain dictionary words.
4. It should not contain the user's personal information such as their name, family member's name, birth date, pet name, phone number or any other detail that can easily be identified.

5. It should not be the same as the user's login name.
6. It should not be the default passwords as supplied by the system vendor such as password, guest, and admin and so on.

Four Password selection strategies:

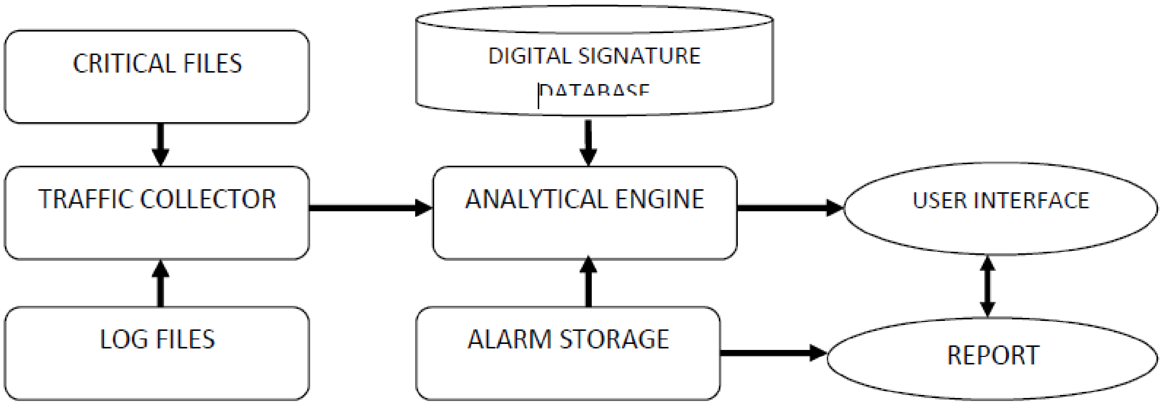
1. **User education:** Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords. This user education strategy is unlikely to succeed at most installations, particularly where there is a large user population or a lot of turn over. Many users will simply ignore the guidelines. Others may not be good judges of what is a strong password. For example, many users believe that reversing a word or capitalizing the last letter makes a password un-guessable.
2. **Computer-generated passwords:** Passwords are quite random in nature. Computer-generated passwords also have problems. If the passwords are quite random in nature, users will not be able to remember them. Even if the password is pronounceable, the user may have difficulty remembering it and so be tempted to write it down. In general, computer-generated password schemes have a history of poor acceptance by users. FIPS PUB 181 defines one of the best-designed automated password generators. The 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. A random number generator produces a random stream of characters used to construct the syllables and words.
3. **Reactive password checking:** A reactive password checking strategy is one in which the system periodically runs its own password cracker to find guessable passwords. The system cancels any passwords that are guessed and notifies the user. This tactic has a number of drawbacks. First it is resource intensive, if the job is done right. Because a determined opponent who is able to steal a password file can devote full CPU time to the task for hours or even days an effective reactive password checker is at a distinct disadvantage. Furthermore, any existing passwords remain vulnerable until the reactive password checker finds them.
4. **Proactive password checking:** The most promising approach to improved password security is a proactive password checker. In this scheme, a user is allowed to select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and if not, rejects it. Such checkers are based on the philosophy that with sufficient 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 user acceptability and strength. If the system rejects too many passwords, users will complain that it is too hard to select a password. If the system uses some simple algorithm to define what is acceptable, this provides guidance to password crackers to refine their guessing technique. In the remainder of this subsection, we look at possible approaches to proactive password checking.

2) **Explain in detail intrusion detection systems.**
(IDS: 2M, Diagram: 2M, IDS components: 2M, Types: 2M)

Ans.

An IDS (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. Intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways.



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:

1) Host-based IDS:

2) Network based IDS:

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

1. Logins at odd hours
2. Login authentication failure.
3. Adding new user account
4. Modification or access of critical systems files.
5. Modification or removal of binary files
6. Starting or stopping processes.
7. Privilege escalation
8. Use of certain program

2) Network based IDS looks for certain activities like:

1. Denial of service attacks.
2. Port scans or sweeps
3. Malicious contents in the data payload of packet(s)
4. Vulnerability of scanning
5. Trojans, Viruses or worms
6. Tunneling
7. Brute force attacks.

3) Explain need for firewall and explain one of the type of firewall with diagram.
(Explanation of need: 4M, Any one firewall explanation: 4M)

Ans.

A firewall works as a barrier, or a shield, between your PC and cyber space. When you are connected to the Internet, you are constantly sending and receiving information in small units called packets. The firewall filters these packets to see if they meet certain criteria set by a series of rules, and thereafter blocks or allows the data. This way, hackers cannot get inside and steal information such as bank account numbers and passwords from you.

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.

Types of Firewalls

1. Packet Filter
2. Circuit level Gateway

3. Application Gateway
4. Software
5. Hardware
6. Hybrid
7. Stateful multilayer Inspection Firewall

1.**Packet Filtering Firewall:** Packet Filtering Firewalls are normally deployed on the Routers which connect the Internal Network to Internet. Packet Filtering Firewalls can only be implemented on the Network Layer of OSI Model. Packet Filtering Firewalls work on

the Basis of Rules defines by Access Control Lists. They check all the Packets and screen them against the rules defined by the Network Administrator as per the ACLs. If in case, any packet does not meet the criteria then that packet is dropped and Logs are updated about this information. Administrators can create their ACLs on the basis Address, Protocols and Packet attributes.

Advantage:
The Biggest Advantage of Packet Filtering Firewalls is Cost and Lower Resource Usage and best suited for Smaller Networks.

Disadvantage:
Packet Filtering Firewalls can work only on the Network Layer and these Firewalls do not support Complex rule based models. And it’s also Vulnerable to Spoofing in some Cases.

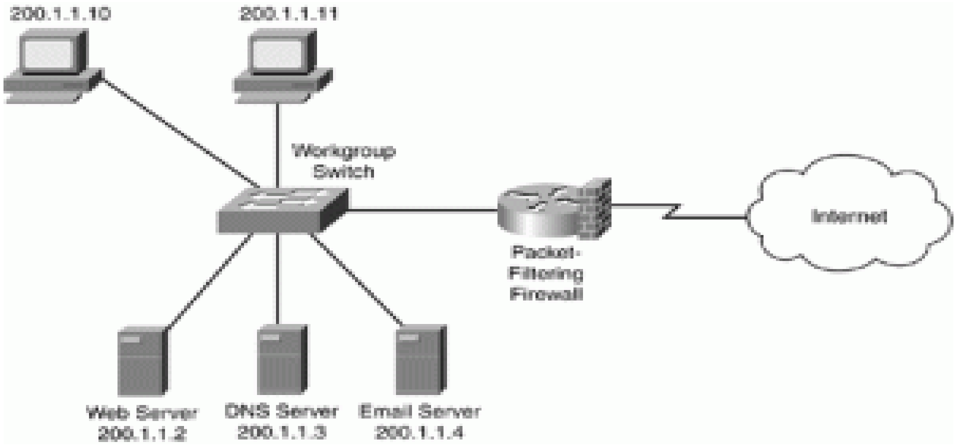


Fig: Packet Filtering Firewall

Q.6) Attempt any four of the following: 16

1) Enlist any four consequences when the system is accessed by non-employee.
(Any Four Consequences: 1M each)

Ans.

1. Unauthorized disclosure of information: disclosure of confidential, sensitive or embarrassing information can result in loss of credibility, reputation, market share, and competitive edge.
2. Disruption of computer services: be unable to access resources when they are needed can cause a loss of productivity. Disruption of services during critical processing time may be disastrous.
3. Loss of productivity: misuse of IT resources such as network bandwidth may cause slow response times, delaying legitimate computer activities that, in time-critical applications such as stock trading, can be very costly.
4. Use of a computer or its data for unapproved or possibly illegal activities: Someone gaining access to a bank computer and performing an unauthorized transfer
5. Financial loss: the losses can be directly from the theft of money or indirectly from the recovery of security incidents such as corruption of information or disruption of services.
6. Legal implications: security or privacy breaches can expose a company to lawsuits from investors, customers, or the public.
7. Blackmail: intruders can extort money from the company by threatening to exploit the security breach.

2) Explain rail fence transposition technique.
(Algorithm – 2M, Example- 2M)

Ans.

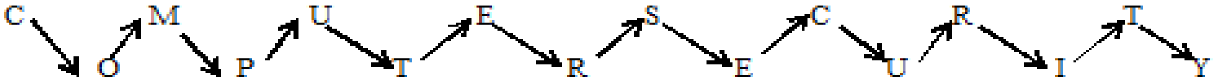
In Rail fence cipher, techniques are essentially Transposition Ciphers and generated by rearrangement of characters in the plaintext. The characters of the plain text string are arranged in the form of a rail-fence as follows.

Let the Plaintext be — COMPUTER SECURITY

Rail Fence Technique algorithm:

1. Write down the plain text message as a sequence of diagonals.
2. Read the plain text written in Step-1 as a sequence of rows.

Example: plain text = “COMPUTER SECURITY “is converted to cipher text with this help of Rail Fence Technique with dual slope.



Ciphertext: CMUESCRTOPTREUIY

3) Explain AH mode of IP security.
(Diagram: 1M, Explanation of Fields: 3M)

Ans.

Authentication Header (AH) provides authentication, integrity, and anti-replay for the entire packet (both the IP header and the data payload carried in the packet). It does not provide confidentiality, which means it does not encrypt the data. The data is readable, but protected from modification. AH uses the HMAC algorithms described earlier to sign the packet for integrity.For example, Alice on Computer A sends data to Bob on Computer B. The IP header, the AH header, and the data are protected with integrity. This means Alice can be certain it was really Bob who sent the data and that the data was unmodified.

Integrity and authentication are provided by the placement of the AH header between the IP header and the transport (layer 4) protocol header, which is shown as TCP/UDP in the Figure AH uses an IP protocol ID of 51 to identify itself in the IP header.

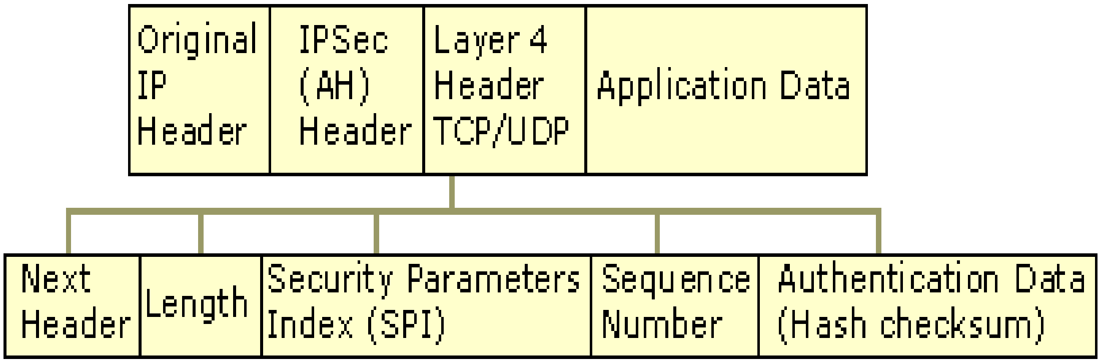


Figure: Authentication Header

AH can be used alone or in combination with the Encapsulating Security Payload (ESP) protocol.

The AH header contains the following fields:

1. Next Header: Identifies the next header that uses the IP protocol ID. For example, the value might be "6" to indicate TCP.
2. Length: Indicates the length of the AH header.
3. Security Parameters Index (SPI): Used in combination with the destination address and the security protocol (AH or ESP) to identify the correct security association for the communication. The receiver uses this value to determine with which security association this packet is identified.

4. Sequence Number Provides anti-replay protection for the SA. It is 32-bit, incrementally increasing number (starting from 1) that is never allowed to cycle and that indicates the packet number sent over the security association for the communication. The receiver checks this field to verify that a packet for a security association with this number has not been received already. If one has been received, the packet is rejected.
5. Authentication Data Contains the Integrity Check Value (ICV) that is used to verify the integrity of the message. The receiver calculates the hash value and checks it against this value (calculated by the sender) to verify integrity.

4) Explain IT Act 2000 and 2008.
(IT Act 2000: 2M, IT ACT 2008: 2M)

Ans.

Information Technology Act

The Government of India enacted The Information Technology Act with some major objectives which are as follows –

- To deliver lawful recognition for transactions through electronic data interchange (EDI) and other means of electronic communication, commonly referred to as **electronic commerce** or E-Commerce. The aim was to use replacements of paper-based methods of communication and storage of information.

- To facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000. The I. T. Act got the President’s assent on June 9, 2000 and it was made effective from October 17, 2000. By adopting this Cyber Legislation, India became the 12th nation in the world to adopt a Cyber Law regime.

Objectives of the IT Act 2000 are:

1. To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as “electronic commerce” in place of paper based methods of communication.
2. To give legal recognition to Digital signatures for authentication of any information or matter this requires authentication under any law.
3. To facilitate electronic filing of documents with Government departments
4. To facilitate electronic storage of data

5. To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions
6. To give legal recognition for keeping of books of accounts by banker's in electronic form.
7. To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

IT ACT 2008:

It is the information Technology Amendment Act, 2008 also known as ITA-2008

It is a considerable addition to the ITA-2000 and is administered by the Indian Computer Emergency Response Team (CERT-In) in year 2008.

Basically, the act was developed for IT industries, to control e-commerce, to provide e-governance facility and to stop cybercrime attacks.

The alterations are made to address some issues like the original bill failed to cover, to accommodate the development of IT and security of e-commerce transactions.

The modification includes.

1. Redefinition of terms like communication device which reflect the current use.
2. Validation of electronic signatures and contracts.
3. The owner of an IP address is responsible for content that are accessed or distributed through it.

Organizations are responsible for implementation of effective data security practices.

Following are the characteristics of IT ACT 2008:

1. This Act provides legal recognition for the transaction i.e. Electronic Data Interchange (EDI) and other electronic communications. Electronic commerce is the alternative to paper based methods of communication to store information.
2. This Act also gives facilities for electronic filling of information with the Government agencies and further to change the Indian Penal Code-Indian Evidence Act 1872, Bankers code Evidence Act 1891 and Reserve Bank of India Act, 1934 and for matter connected therewith or incidental thereto.
3. The General Assembly of the United Nations by resolution A/RES/51/162, dated 30 January 1997 has adopted the model law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.
4. This recommends that all States give favourable consideration to the above said model law when they enact or revise their laws, in terms of need for uniformity of the law applicable to alternative to paper based methods of communication and storage of information.
5. It is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

5) **Explain the function of entities used in SET.**
(Four Entities with function: 1M each)

Ans.

Secure Electronic Transaction (SET) is a security technology proposed by Visa and MasterCard to allow for more secure credit card transaction possibilities than what is currently available. SET has been waiting in the wings for full implementation and acceptance as a standard for quite some time. Although SET provides an effective way of transmitting credit card information, businesses and users do not see it as efficient because it requires more parties to coordinate their efforts, more software installation and configuration for each entity involved, and more effort and cost than the widely used SSL method.

SET is a cryptographic protocol and infrastructure developed to send encrypted credit card numbers over the Internet. The following entities would be involved with a SET transaction, which would require each of them to upgrade their software, and possibly their hardware:

The main entities in SET:

1. Cardholder
2. Merchant
3. Payment Gateway
4. Certificate Authority

The function of the entities is as given below.

- The Cardholder Application, also referred to as a digital wallet, is held by an online consumer and packages a digital signature and credit card information that ensures his or her identity and safeguards his or her financial information through a complex encryption system.
- The Merchant Server component is the verification product held by the merchant to process the online card payment.
- The Payment Gateway component is held by an acquiring bank or other trusted third party that accepts and processes the merchant's verification and the customer's payment information and filters them to their appropriate financial institutions.
- The Certificate Authority component, usually run by a financial institution, is the trusted agent that issues the digital certificates and is responsible for ensuring that all users of digital certificates are in fact secure and trustworthy customers.