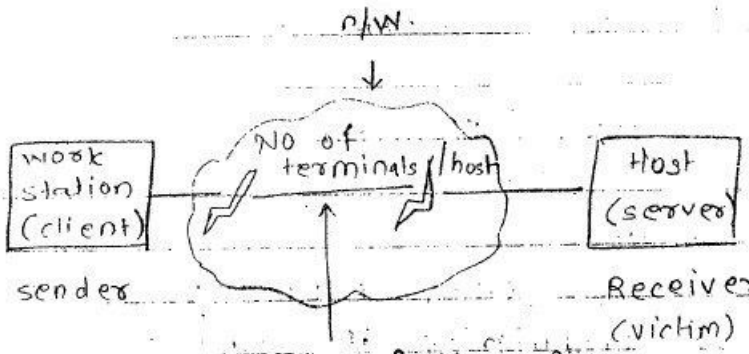
NETWORK SECURITY



Theory topics { Why Attack takes place
Who Attacks the n/w security

- challenge
- Fame
- money (Espionage)
- Ideology.

Why Attack takes place.

- Anonymity / Multiple points of attack
  Unknown path /
  Unknown parameter.

If Anonimity of victim is on WAN then its very difficult to identify the attacks.

Multiple points of Attacks : as multiple n/w coming in b/w sender & Receiver then it is possible that unknown attacker may attack.

unknown path :- the path in which packet moves is kno unknown.

unknown parameter :- only 1 gateway present
∴ connection to outside world is through gate way only but if there are many other way then it unknown perimeter.

WHO ATTACKS THE N/W SECURITY :-

1] CHALLENGE :-
Most of the attacks are for this reason.

2] FAME :-
Most of the attackers attack to the n/w to get the fame.

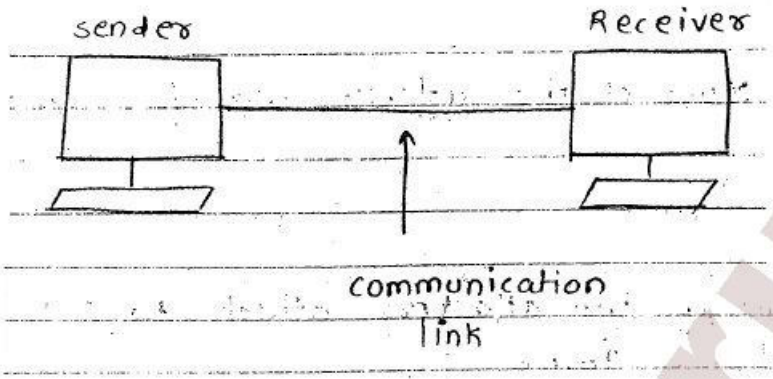
3] MONEY :-
Big organizations.

4] IDEOLOGY :-
Website - defacement

THREATS IN N/W :-

THREATS IN TRANSIT :-

WIRETAPPING :-



If attacker puts some efforts to listen the communication bet^n sender & receiver is called wiretapping.

WIRETAPPING

- Active wiretapping (Introduce its own data)
- Passive wiretapping.

ACTIVE WIRETAPPING :-

In active wiretapping attacker introduce its own data
∴ confidentiality & Integrity are lost.

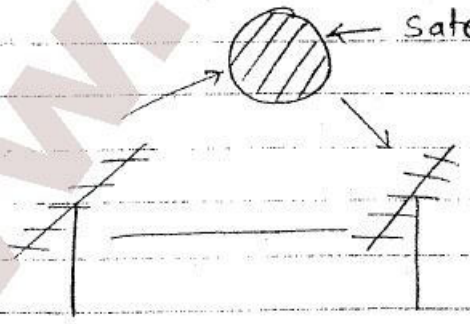
PASSIVE WIRETAPPING :-

In this attacker just listens the communication ∴ only confidentiality is lost.

communication have many options:-
- copper wire
- Fibre optic cable
- satellite
- Microwave
- wireless comm^n

COPPER WIRE	OPTICAL / FIBRE CABLE:
1] Inductance attack is possible (flux generated) is proportional to current in cable	1] Inductance attack is not possible.
2] Impedence attack is possible.	2] Impedence attack is not possible.
3] less possibility of noise in the enviornment.	3] less possibilities of noise.

SATELLITE / MICROWAVE:-



In satellite communication, satellite antenna is present bet^n sender & receiver.
In microwave direct communication is there bet^n sender & receiver.
- used in large area.

SATELLITE	MICROWAVE
1] open communication	1] open communication.
2] large multiplexing	2] less multiplexing.

WIRELESS COMMUNICATION:-

- It is available in smaller area for example a small building.
- No confidentiality
- Integrity nise.

EAVESDROPPING:-

Attacker doesn't put any effort to listen the communication is called as Eavesdropping.

THREATS IN N/W SECURITY:-

1] THREAT PRECURSORS (BACKGROUND)

a] PORT SCAN:-

If Attaker known all about n/w then its is called precursors.

No of ports = 2^{16} = 64 K I/O ports.
Only about 1024 ports are used.
Port 80 (HTTP) web
Port 23 Telnet
Port 25 SMTP (e-mail)

b] SOCIAL ENGINEERING:-

If attacker has some relationship in the n/w he can get the info about the n/w through this relationship.
- Exploits social attacks to find out o.s. & application program running in n/w.

c] RECONNAISSANCE:- (Collect Information)

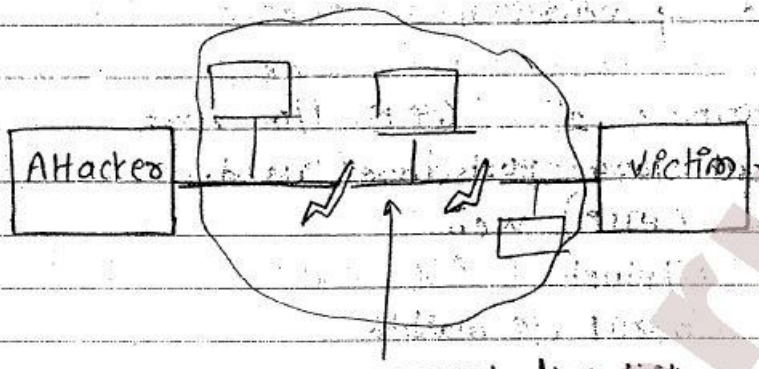
Dumpster diving.

d] COLLECT DOCUMENTATION.

e] CHAT ROOM.

3) DENIAL OF SERVICE (DOS) ATTACK :-

In denial of service attack, Availability is lost i.e. the ~~avail.~~ authorized user are denied from the resouces.



DOS takes place due to following :-

1) TRANSMISSION FAILURE :-
simply cut / break the communication link ie. wire.

2) CONNECTION FLOODING :-
It means exceed of bandwidth i.e. put so much data on link so that communication won't take place.

a) PING OF DEATH :- (Echo) :-

2 protocols :- TCP, ICMP (Internet control message protocol)

ICMP sends a ping packate to check whether Receiver is reachable i.e. address is valid or not. Then receiver replies then

target is reachable. Receiver sends echo packet as ack.

Receiver not only sends Ack but also sends ~~same~~ data. If some data is sent that means the channel is noiseless.

If A sends 1000 ping packets / sec then B has to respond with same rate but if not same then B will be busy in sending echo only but can't do its own working.

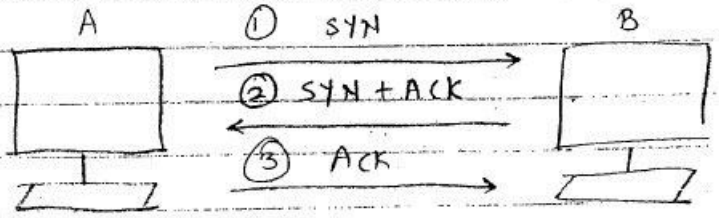
If B's capacity > A's capacity
∴ no chance of Attack.

b) SMURF ATTACK Double twist :-

In case of SMURF attack double twist attack along with ping packets.

A construct ping packet but not with its own address but address of B. This packet is sent to all host connected on the n/w. in broadcast mode. Then every host thinks ping packet is from B then all the hosts respond to B.

c) SYN ATTACK :-



A sends SYN signal to B to establish a connection If B is ready to communicate B will send SYN + ACK & If A gets this signal A will have to send Ack signal again. But these signal take time to reach the destination. It is called as pending communication. To avoid this B will have SYN-RECEIVE Buffer to store the signals. (Buffer overflow).

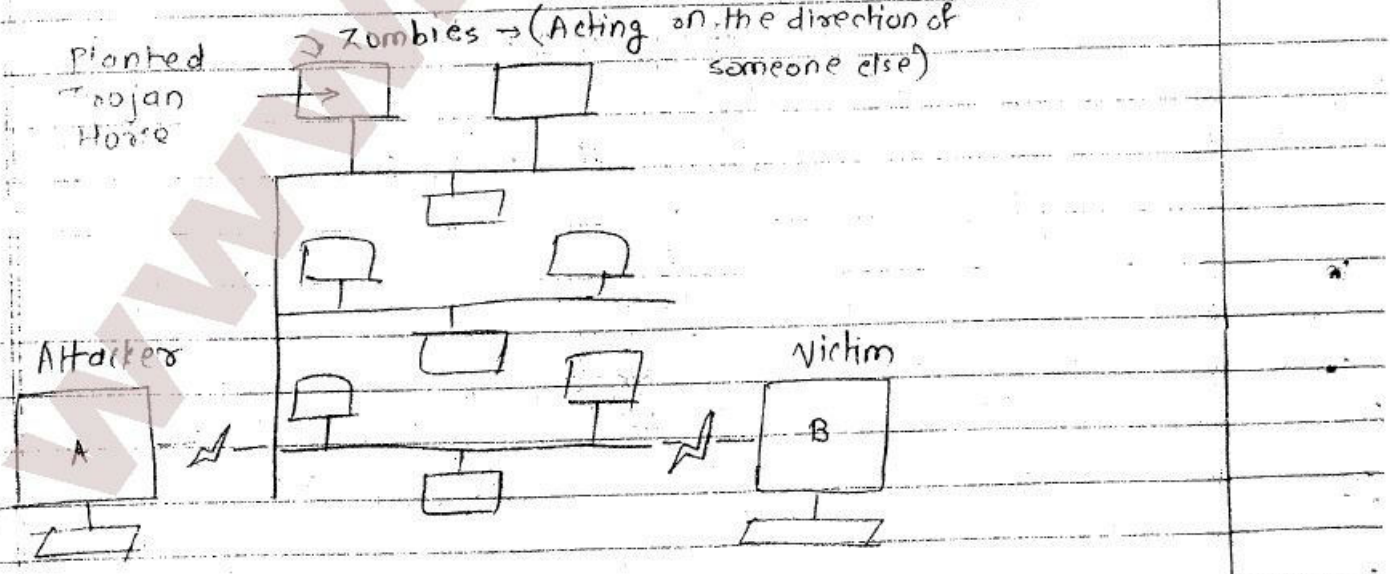
SYN Attack takes place with non existent address.

D] TRAFFIC REDIRECTION :-

Packets are routed by routed i.e. path is being decided by the router.

If router falsely claiming that it has best path. then all packets are routed through that pat i.e. Redirection of traffic.

E] DISTRIBUTED - DENIAL OF SERVICE :-



2 layer attack
[All above are 1 layer attack : Attacker is directly involved to attack victim]
2 layer attack doesn't directly involved to attack victim.
Attacker sends / plants virus to as many host as possible. The all attacked node or computers are called zombies.
All these ~~are inde~~ will independently attack to victim as soon as some event takes place, as they all were waiting for some event to occur.
The attack may be of different type depending upon type of virus planted on perticular host/node

4] IMPERSONATION :-

- (Authentication Related Attack)

a] Authentication failed by guess work :-
Unauthorized user gets somehow some info so that he has access to confidential data by claiming / proving itself authorized user.
[If person gets to know password by some guessing then has access to all info

b] Non existance authentication :-
No password

c] Circumvent Authentication :-

password $\xrightarrow{\text{stored in}}$ Buffer
↓
(Bufferoverflow)

protocol flaw :- To avoid above situation

d] Well-known Authentication :-

"community-string"
password given / allocate to a group not a single person.

5] SPOOFING :-

a) Masquerade (Mask)

Domain name confusion
eg:- If website exist say www.icici.org
create a new website as www.icicl.com
small variation to confuse customer.

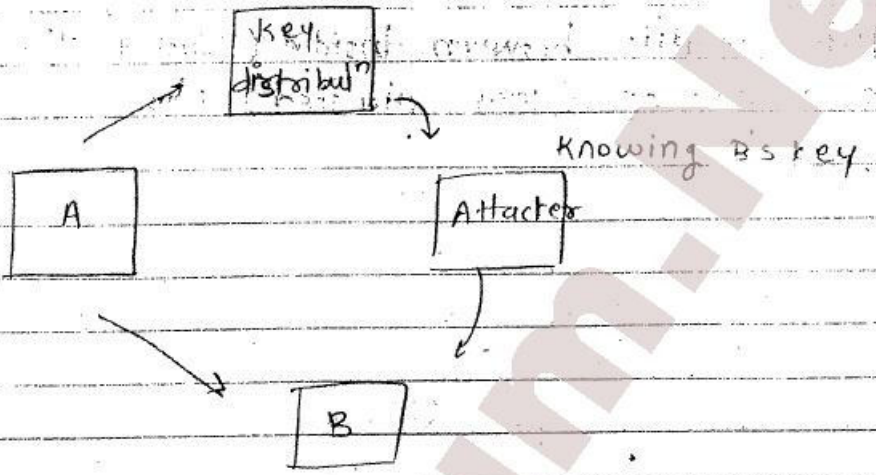
Government
↘
eg:- www.whitehouse.gov
www.whitehouse.com
↑
spoofing
(Masquerade.

b) session Hijacking :- (last minute Entry)

If A & B is having some communication about purchasing products & A & B are some proper rates At that time C comes in picture & destroys the communication link betn them & will take the advantage of those rates.

PAGE NO.
DATE

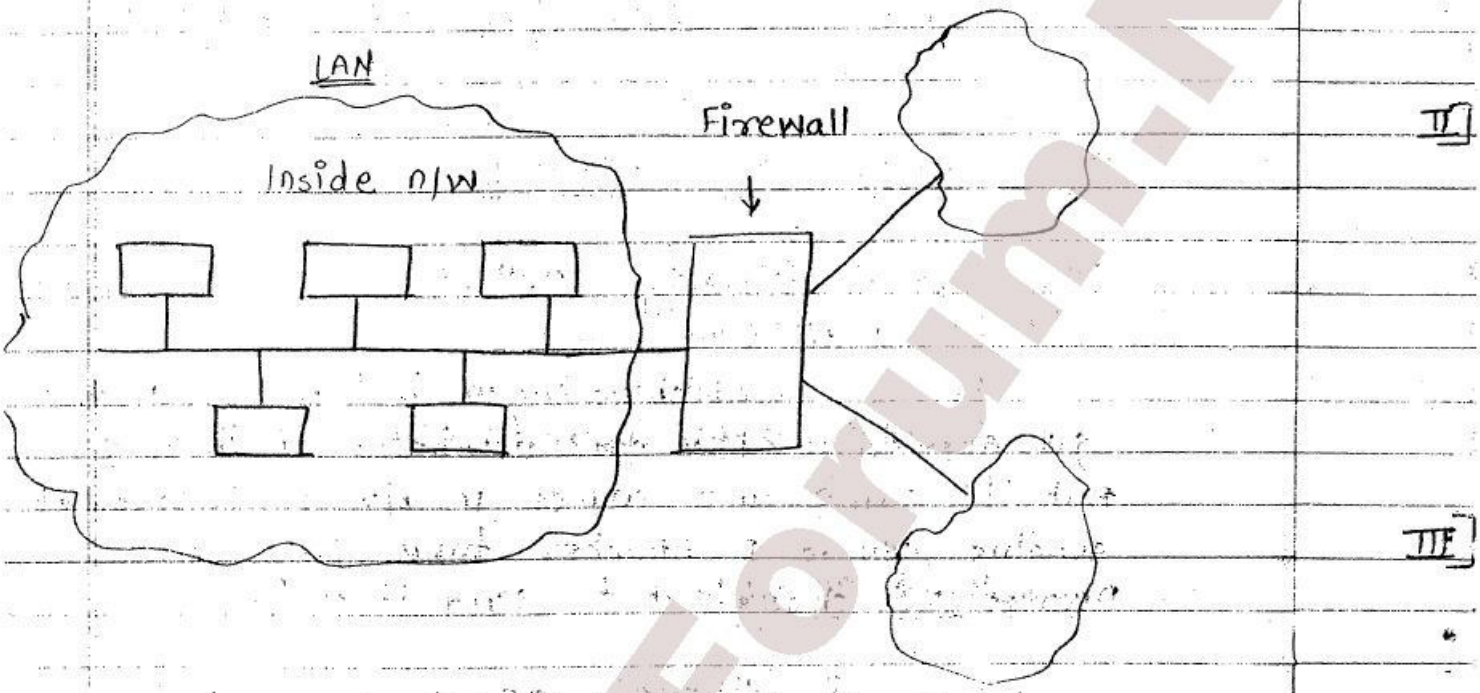
g) Man-in-the middle attack :-



Before establishing comm bet A & B. Both get key from key distribution Authority. But if some one comes in b/w & instead of sending key to B. Attacker takes this key Decrypt it / change it & send it to B.

FIREWALL :-

Filters traffic between Inside (Trusted) N/w and outside (~~Tous~~ Untrusted) N/w.



I] PACKET FILTERING FIREWALL / SCREENING FIREWALL :-

Whatever packets are coming from outside the ~~firewall~~ n/w, Firewall filters those packets & if they are permitted to go firewall sends them inside the n/w only on "ADDRESS" field of packet.

a) Default block :-
All the packets are defaultly blocked unless explicitely permitted.

b) Default ~~permitte~~ permitted
~~At~~ "All the packets are defaultly permitted unless explicitely permitted.

Default block is more secured than default permitted.
Packet filtering is not very much protected
Default permit is used for advent purpose.

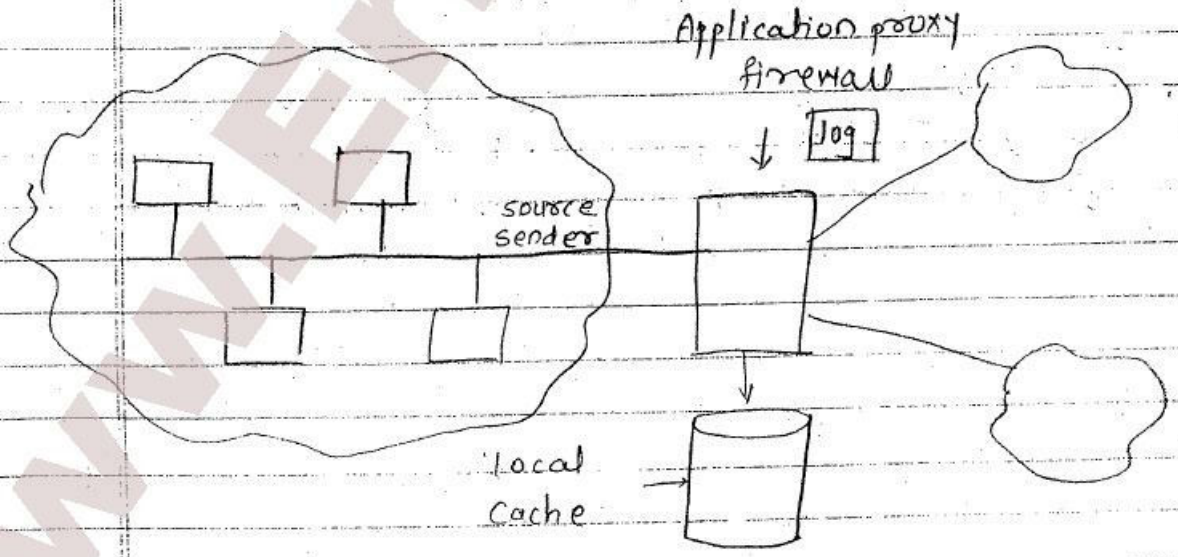
II] STATEFUL INSPECTION FIREWALL :-

This type of filtering method checks ~~eve~~ addre field for every packet.

state / context ⇒ ~~poo~~ port / scan type attack.

III] APPLICATION PROXY :-

This type of filtering method checks address as well as data field from packet.



If one on the web site is being accessed frequent the firewall maps it to the local cache to save the time.
Only Reading of data is passible.

IV] GUARD :-

- Very similar as Application proxy.
- Address or data can be reformatted.
- If the data being accessed frequently is in image format & is taking so much memory place. Guard converts it into the text format & stores them into local cache.
  i.e. converts high storage data → low storage data.

V] PERSONAL FIRWALL :-

Suppose a computer is not in n/w but want security then firewall can be installed on personal computer.

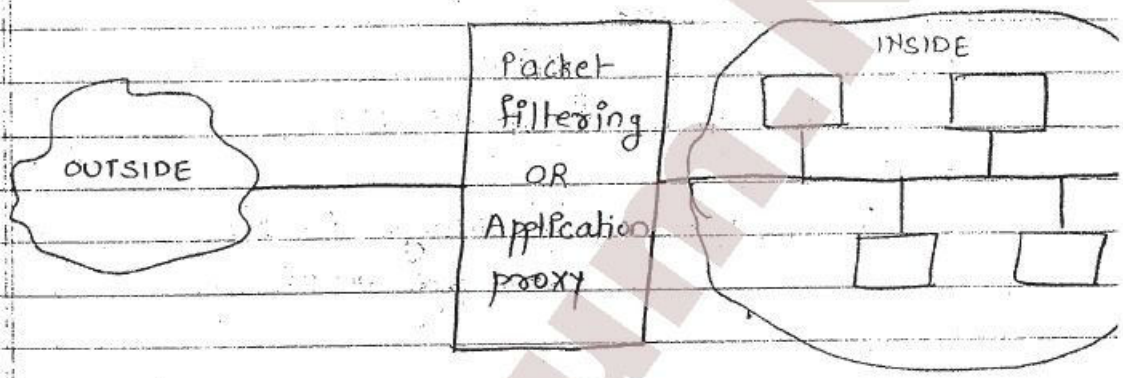
eg:-

VI] McAFFE FIREWALL :-

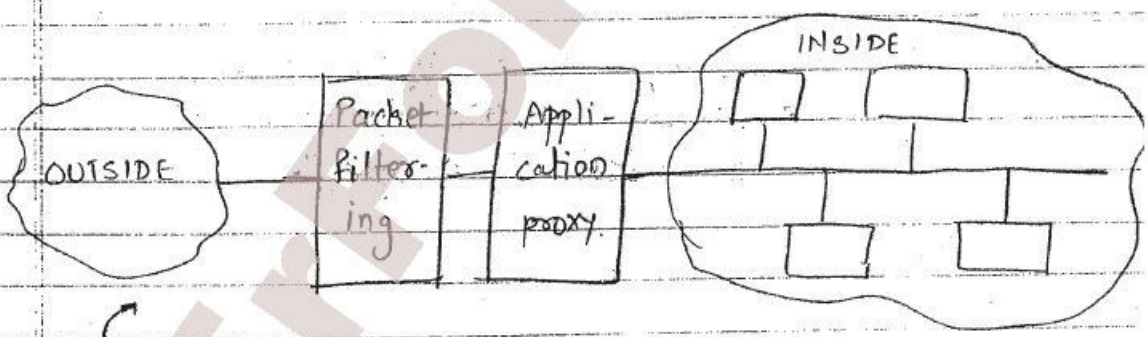
CONFIGURATION OF FIREWALL :-

(depth in defence)

BEFORE :-



AFTER :-

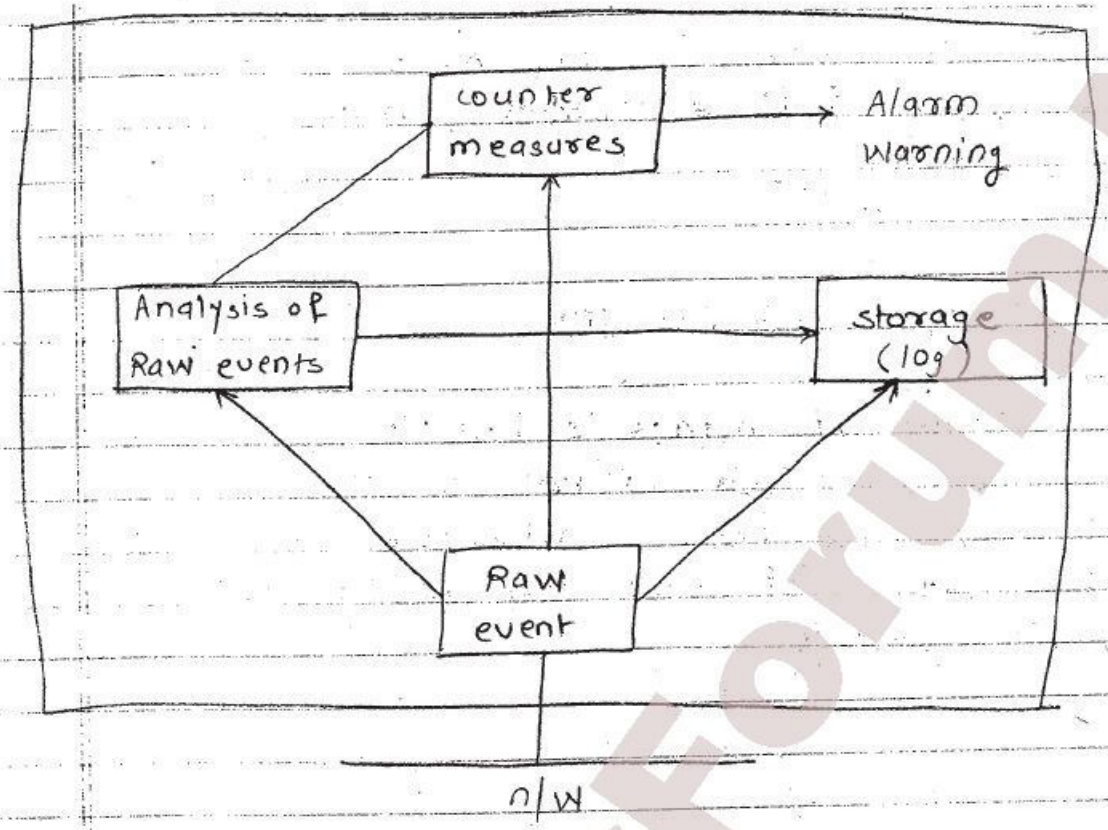


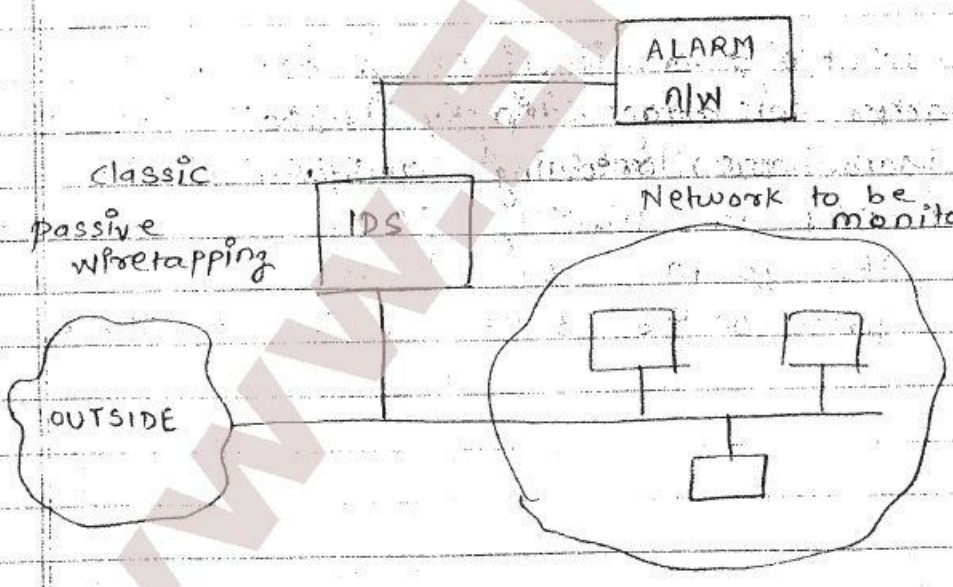
Firewall is ~~on~~ itself on a terminal

∴ A Hacker can attack directly firewall

∴ we can have following configuration.

INTRUSION DETECTION SYSTEM :- (IDS) :-





88

PAGE NO.
DATE

SIGNATURE BASED IDS (PATTERN MATCHING)

In this type of IDS, we know the pattern of attack. If it matches, attack is going to be happened.

HEURISTIC BASED IDS :-

Pattern of attack is not known but normal behaviour pattern is known.
Deviation from normal behaviour is attack.
New pattern of attack can be detected.
More powerful.

In stealth mode of operation IDS is connected to two different n/ws. First is n/w to be monitored & second is the Alarm n/w or warning n/w.
The warning or Alarm of the attack is never given on the same n/w to be monitored.

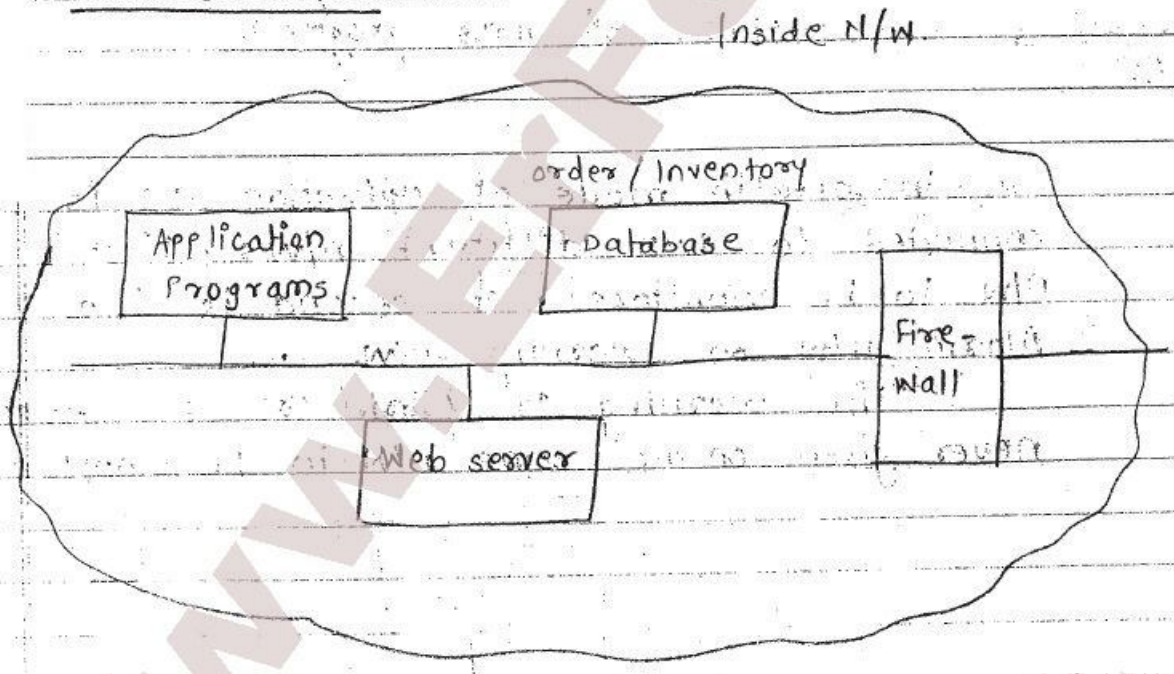
HONEYPOTS :-

- To attract the attacker.
- To study the behaviour of attacker, we will be keeping honeypots.

NETWORK SECURITY CONTROLS :-

a] DESIGN / ARCHITECTURAL CONTROL :-

- SEGMENTATION :-



LAN (Trusted n/w) :- Inside n/w

Before designing n/w first understand requirements of (org / company)

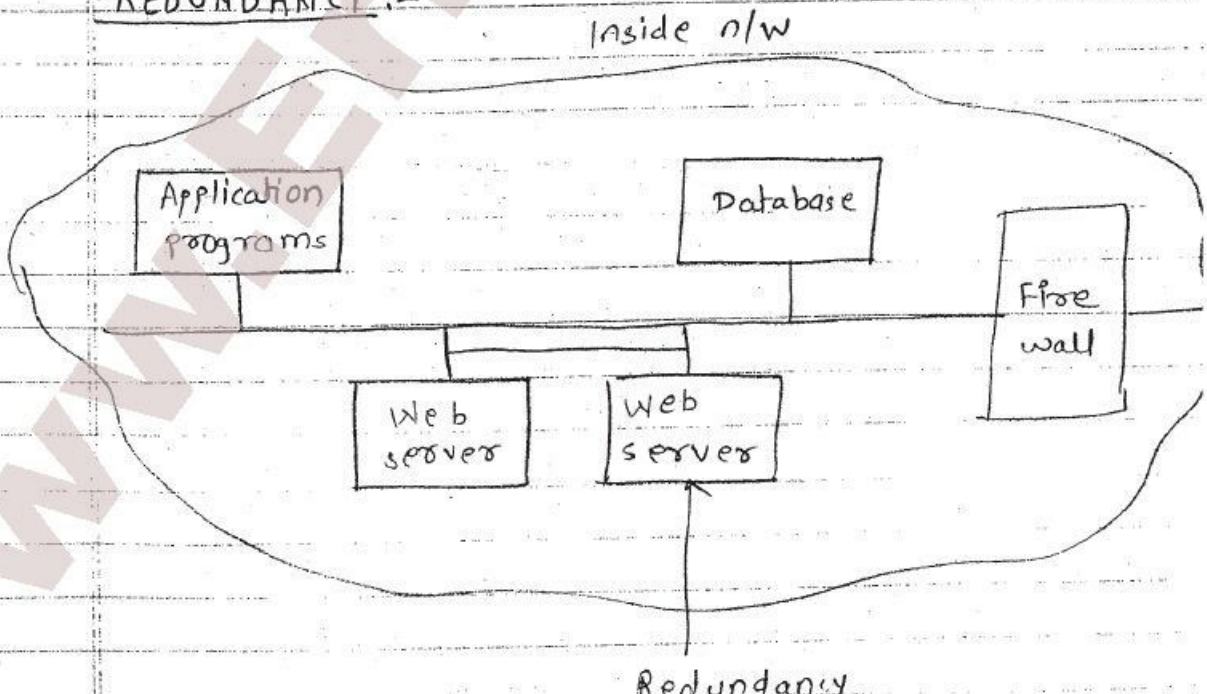
eg:- E-trading / E-commerce

Requirements for E-commerce :-

- Database management (Orders / Inventory stock
- Web services using web server
- Application programs
  eg :- Tally - for - financial operation
- security requirements (firewall)

Analysis is done during design. We will be having some terminal to do all requirement mentioned above. But segmentation says different terminal for each requirement ...
∴ e-segment each activity & a dedicated terminal for each operation. Benifit of this is that someone sends a virus to on termin of d/B, there won't be any application to support execution of virus program.

-REDUNDANCY :-



In Redundacy we will be having same copy of web server. If one of the web server becomes down then it is do not performing desire

work then other web server takes over, this is called, fail over mode.

- SINGLE POINT FAILURE :-

During design or final architectural design try to identify all the ~~identify~~ bottlenecks of system. Then remove such single points of failures or bottlenecks of system so system performance does not get affected.

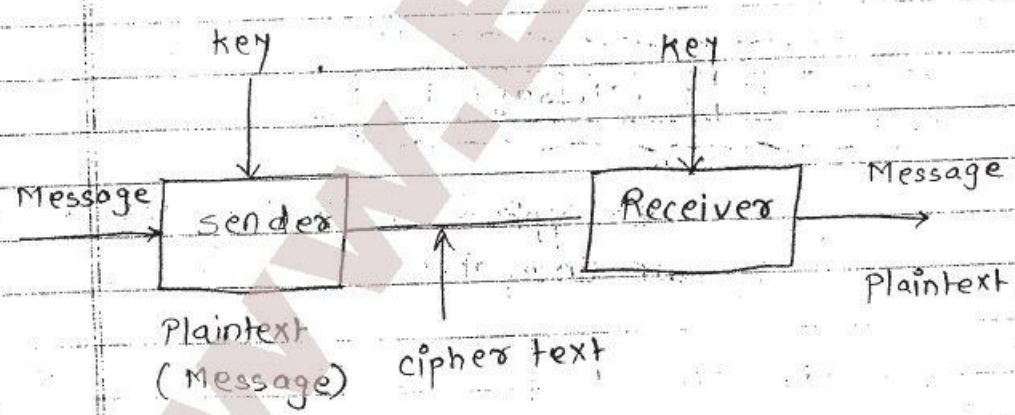
If th
is decry
here a
can att

b] CRYPTOGRAPHY IN N/W SECURITY :-

EQ

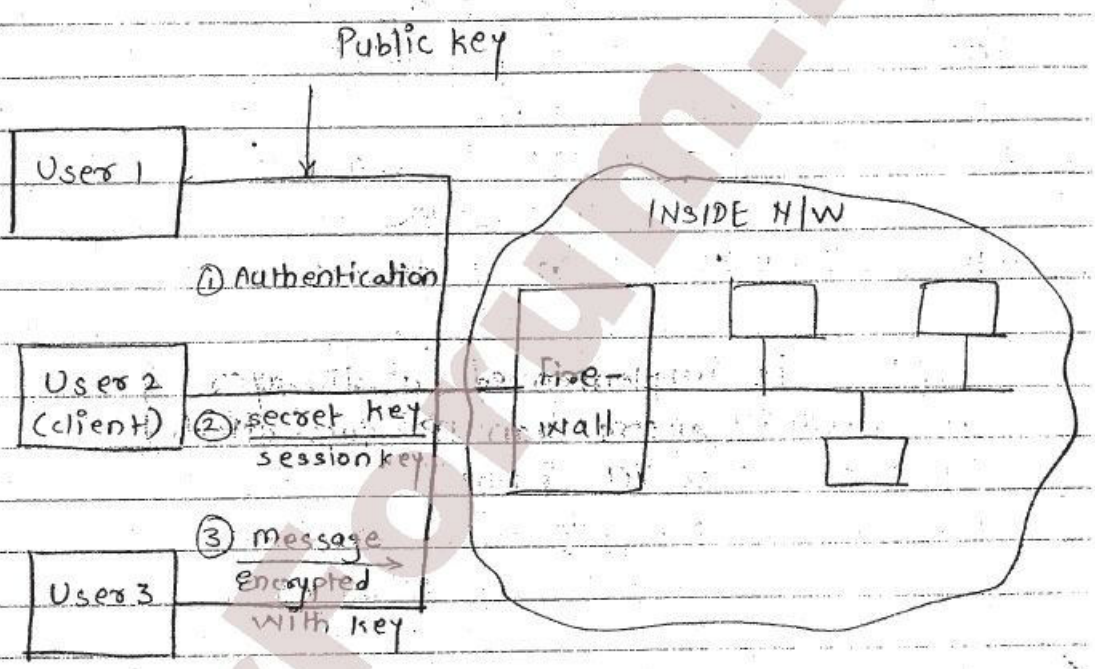
a] ENCRYPTION :-

LINK ENCRYPTION / END-TO-END ENCRYPTION :-



VIRTUAL PRIVATE NETWORK :- (VPN) :-

It is also known as Encrypted Tunnel.



1] Authentication done by Firewall
2] If authorized user, Firewal acknowledeges session key / secret key to user.
3] message encrypted with key is send by user to firewall.

Application of IPSec :- Secure Communicat^n across LAN across private and public WAN's & across ⓔ.
1) Secure branch office connectivity over e
2) Secure remote access over the Internet.
3) Establishing extranet & intranet connectivity with partners
4) Enhancing e-Commerce Security.

PAGE NO.
DATE

IPSec (IP SECURITY PROTOCOL SUITE)

TCP-IP PACKET :-

Physical Header	IP Header	TCP Header	Message	PHysical Trailor

IPSec PACKET :-

IPSec is implemented at IP layer & all above layers than IP gets affected by IPsec Like TCP & UDP

Physical Header	IP Header	Message + Header	Physical Trailer

ESP

ESP :- Encapsulated security payload

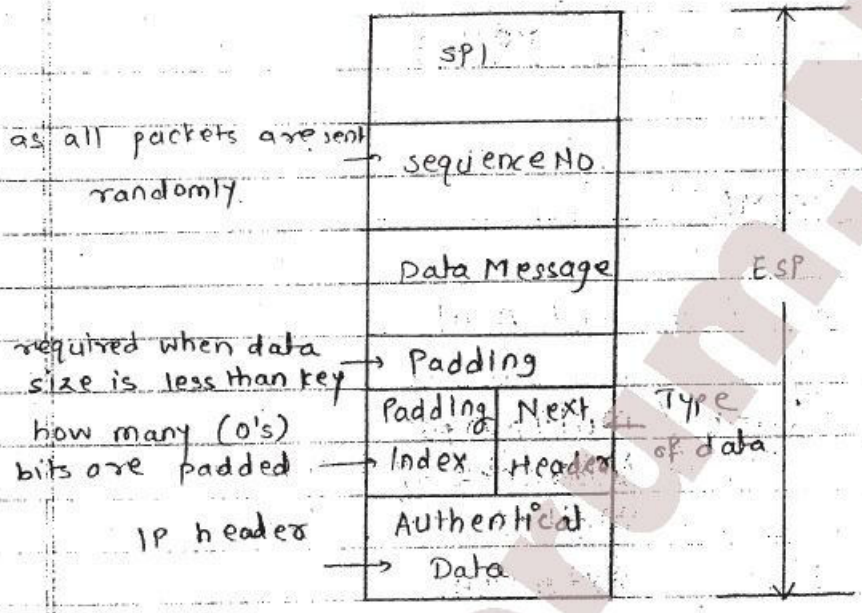
⇩

encrypted.

SECURITY ASSOCIATION :-

- size of key (is not specified in ESP, the use will decide)
- DES / AES / RSA algo (user can choose any algo)
- lifespan of association
- Initialization of vector

we can have Block & cipher / Bit ciper if block cipher with block of 64 bit size if data is less than 64 bit pad zeroes.



SSH (SECURE SHELL)

to communicate with unix shell ⇒ also implemented for windows 2000.

SSL

- secure socket layer
- implemented at transport layer.

Document defining IPSec

1) RFC: 2401 Overview Security architecture
RFC: 2402 description of a packet authentication extension to IPV4 & IPV6
RFC: 2406 description a packet encryption extension to IPV4 & IPV6.
RFC: 2408 Specification of Key management capabilities.

Extension header for authentication is AH
Extension header for encryption is ESP (Encapsulating Sec-payload)

SECURE E-MAIL :-

PGP (PRETTY GOOD PRIVACY) :-

PEM - S/MIME

PEM :- Privacy Enchanced Mail

S/MIME :- secure / multipurpose internet mail extension.

SECURITY REQUIREMENTS :-

CONFIDENTIALITY :-

Third party should not read message.

INTEGRITY :-

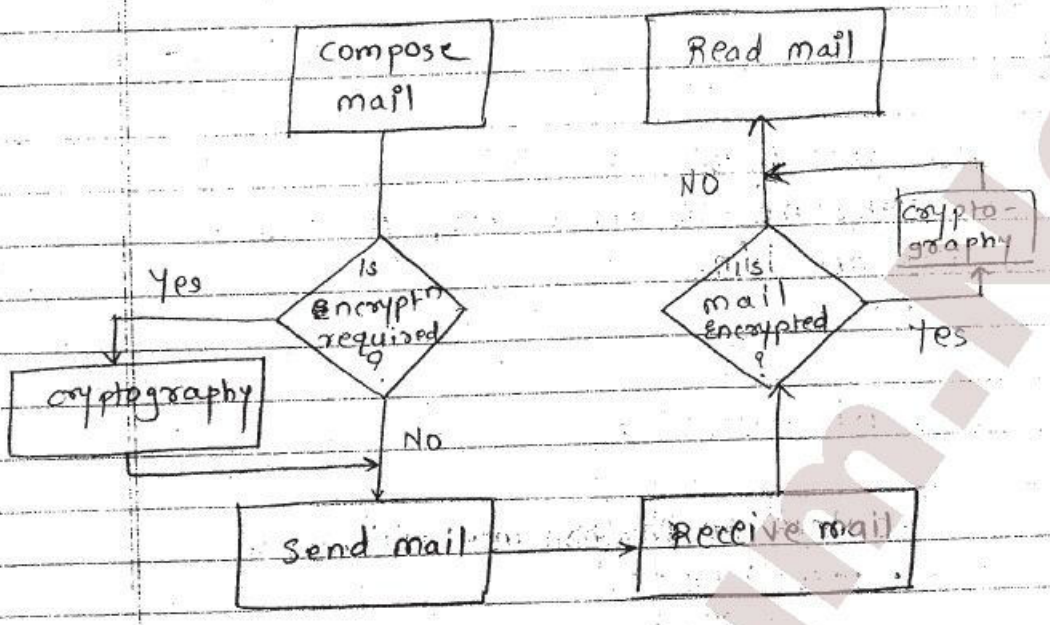
original message should be received without modification.

AUTHENTICATION :-

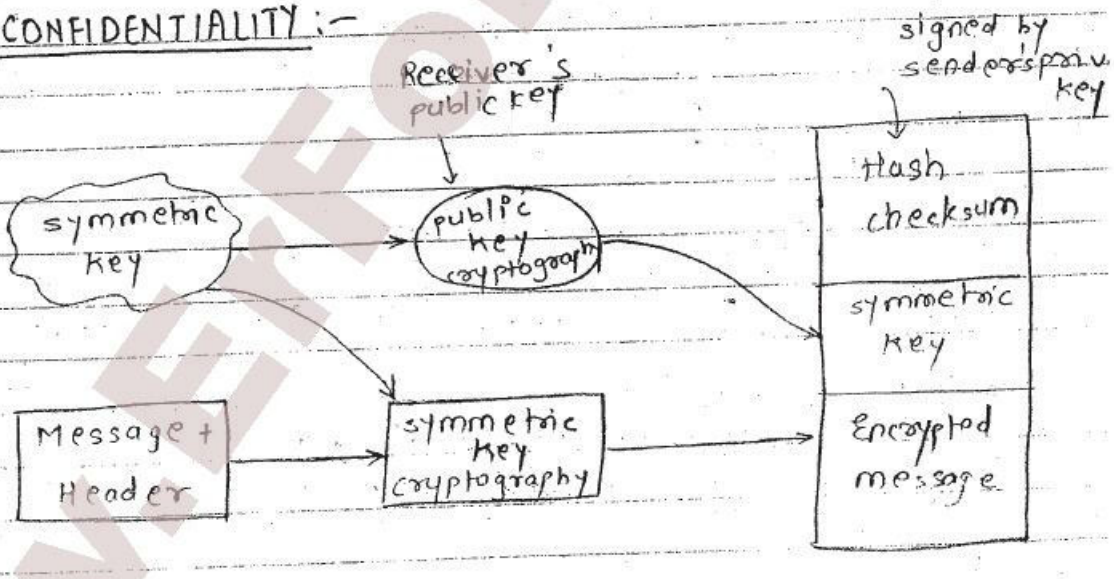
What is guarantee that mail is sent by actual sender only or some other person sends message with that same sender's name.

NON REPUDIATION :-

sender should not deny about ~~the~~ sending the mail.



CONFIDENTIALITY :-

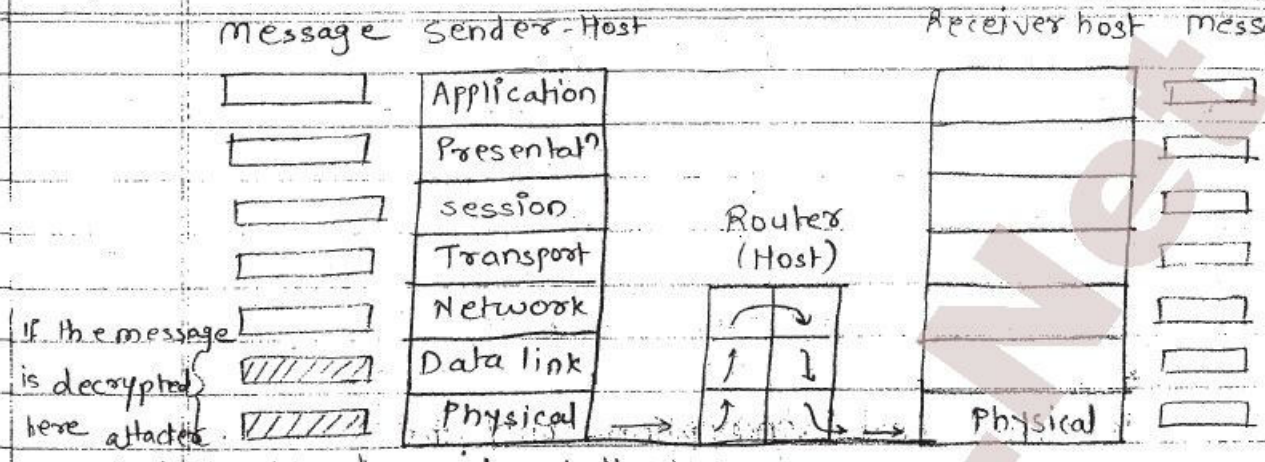


PGP :-

Ring of trust :-
If someone believe on you, you should also believe on him.

secure e-mail :-

- ACL on routers ⇒ Performance will be poor.
- Firewall (C defor)
- IDS



LINK ENCRYPTION :-

TWO ways :-

1] When message is being passed from sender host's physical layer to Receiver host's physical layer Encryption of message will be done.

2] When message is being composed ie when it goes to layer by layer it get encrypted.

If Encryption is on data link layer.

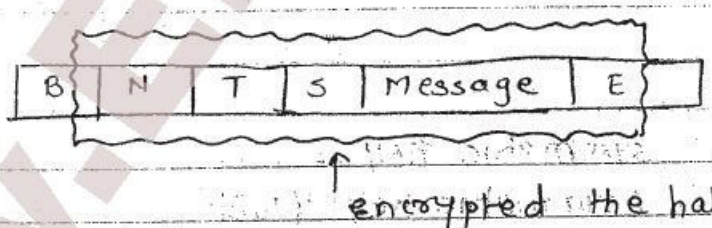


Fig :- Link Encryption.

LINK ENCRYPTION	END-TO-END ENCRYPTION
1] User is not aware	1] User is aware
2] Hardware Encryption	2] S/W & H/W encryption.
3] Useful only for dedicated communication link. Host / Router can see the message	3] Useful even for public Untrusted network.

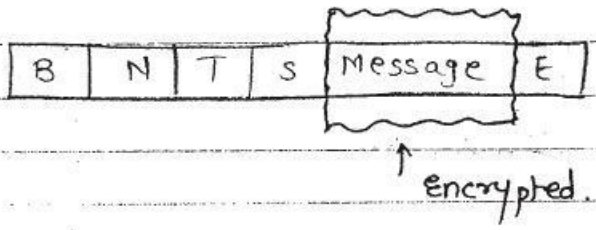


Fig:- End-to End encryption.

In end to end encryption only the message is encrypted, headers are not encrypted hence attacker can't attack & even if it he attacks he can't know the message since even at the receiver side message remains in encrypted format.

LINK ENCRYPTION	END TO END ENCRYPTION
4] No selective encryption	4] Encryption can be selective.
5] symmetric key	5] Public key.

KE = KD ⇒ symmetric key
KE ≠ KD ⇒ Asymmetric key (Public key)

In link encryption every router need to be trusted on 4 as header are also encrypted every router should first decrypt header to get destination address and data again decrypt it to send to next one. It is useful to use symmetric key.

Whereas in End-End only message is encrypted ∴ Asymmetric key (Public key)

PAGE NO.
DATE

RISK ANALYSIS :-

- RISC IMPACT :-

Because of any fault if any damage / loss occurs then the ~~los~~ cost to reconstruct it again, it is called as risc impact.

e.g. -] If 1lakh rupees required to construct d/B & if it damages the risc impact will be 1 lakh rupees (amount to recover d/B back).

2] Risk of power supply failure (vulnerability).

- LIKELIHOOD OF THE FAULT :-

probability of failure (0 - 1)
↑
problem)

- RISK EXPOSURE :-

(Risk impact x probability)

- RISK LEVERAGE :-

$$\text{Risk leverage} = \frac{(\text{Risk exposure Before control}) - (\text{Risk exposu after control})}{\text{cost of control}}$$

STEPS IN RISK ANALYSIS :-

1. IDENTIFY ASSETS :-

A Combine all the assets ie. H/W, S/W, data, & People & analysis them

	Confidentiality	Integrity	Availability
Hardware			stolen, non function
software	copy	modify	Delete
Data			
People			vacation, promotion
Documentation			

2] DETERMINE VULNERABILITY :-

3] EVALUATE LIKELIHOOD OF EVENT (0-1)

☞ Probability of vulnerability.

4] COMPACT ANNUAL LOSS :-

Due to every vulnerability.

5] SURVEY CONTROL :-

Risk leverage.

6] PROJECT ANNUAL SAVING :-

Database Risk exposure	100,000
Risk exposure after control	- 60,000
cost of control	+ 25,000
	65,000

saving :- Before control - after control

= 100,000 - 65,000

= 35,000

PHYSICAL CONTROL :-

(outside computing Enviornment)

NATURAL CALAMITIES :-

- Flood
- Fire
- Earthquake

MAN-MADE :-

- Theft
- vandalism

POWER SUPPLY :-

- UPs
- surge suppressor.