Name :- Akash Santosh katkar
GT / Roll No. :- 5895/35
Signature :- Akash.

INS Assignment 3

Q.1. Explain PGP services in detail.

→ i) It was developed by phil Zimmerman

ii) PGP is open-source.

iii) Although PGP can be used for protecting data in long-term storage, it is used primarily for email security.

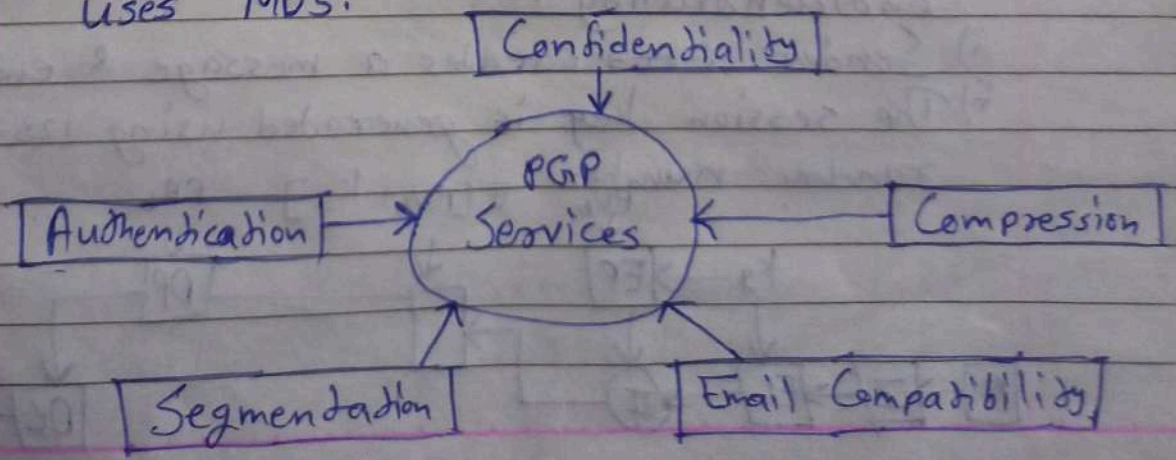
iv) PGP is a complete email security package that provides privacy, authentication, digital signatures & compression all in an easy to use form.

v) The complete package, including all the source code, is distributed free of charge via the internet.

vi) Due to its quality, zero price & easy availability on UNIX, LINUX, Windows & MacOS platforms, it is widely used today.

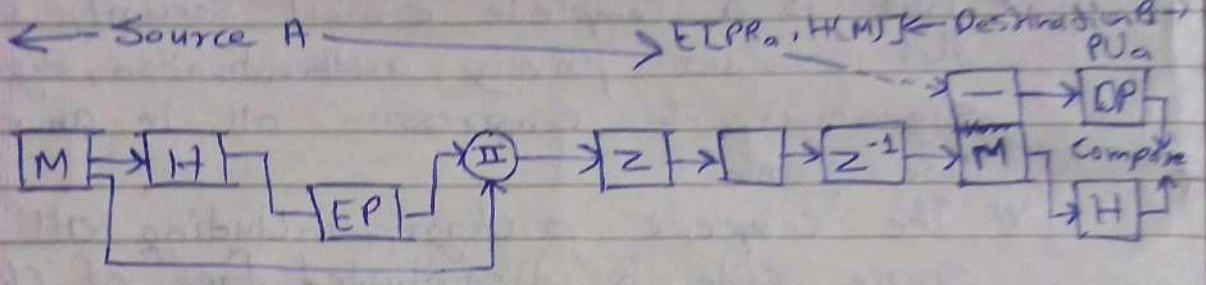
vii) PGP encrypts data by using a block-cipher called IDEA (International Data Encryption Algorithm), which uses 128-bit keys, IDEA is similar to DES & AES.

viii) Key management uses RSA & data integrity uses MD5.



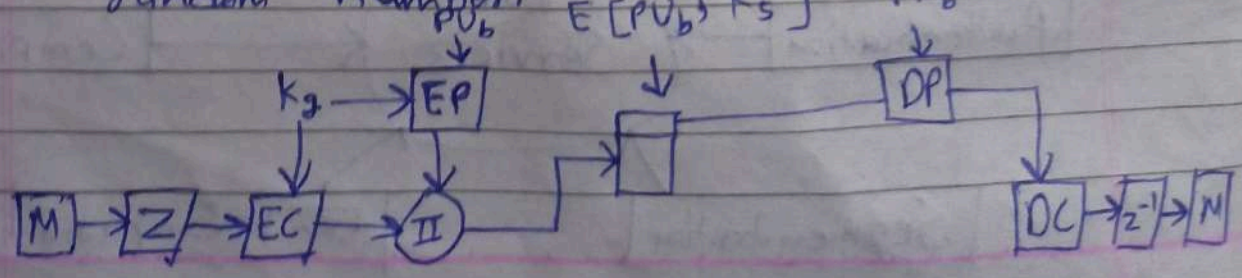
Name :- Akash Santosh kakkar
GI/Roll No. :- 5895/35
Signature :- Akash.

- Authentication:
  i) The sender writes the message.
  ii) The digital signature of the message is produced.



iii) 160-bit of message hash produced by SHA-1.
iv) RSA signs the hash with the help of senders private key.
v) Hash is attached to the message.
vi) Sender's public key along with RSA is used to decrypt hash code & recover it by the receiver.
vii) Using this hash received messages are verified by receiver & comparison with decrypted code.

- Confidentiality:
  i) Sender ~~cred~~ creates a message & encrypts it.
  ii) The session key is generated using 128-bit random number.



iii) Session key encrypts messages using IDEA / CAST-128 / Triple-DES.
iv) RSA encrypts session key using recipient's public key.
v) Encrypted session key is attached to message.
vi) Decryption & recovery of session key takes place using RSA with private key to receiver.
vii) Decryption of message takes place by session key.

- Compression :
i) Compression of message are done by PGP for reducing the space for e-mail storage & transmission.
ii) Message compression by PGP takes place before encryption & after signing.
iii) Thus, for verification purpose uncompressed message & signature are stored.
iv) Compressed encryption improves security.
v) for compression, ZIP algorithm is used whereas for decompression UNZIP algorithm is used.
vi) After compression, encryption of message takes place to increase cryptographic security.

- E-mail Compatibility :
i) PGP encrypts the block of transmitted message. Some system uses ASCII text, PGP converts it into raw 8-bit binary stream.

to a stream of printable ASCII characters. This schems is called radix-64 conversion.

ii) After receiving, the incoming data is converted into binary by radix-64. Them the encrypted message is recovered by using session key & then decompressed.

iii) Since encryption, even when it is limited to the signature results in arbitrary binary strings & since many e-mail systems only permit the use of ASCII characters, we have to be able to represent binary data with ASCII strings.

iv) PGP uses radix-64 encoding for this purpose.

v) Radix-64 encoding, also known as Base-64 ~~and~~ encoding. It first segments the binary stream of bytes into 6-bit words.

vi) The $2^6 = 64$ different possible 6-bit words are represented by printable characters as follows.
a) The first 26 are mapped to the uppercase letters A through Z.
b) The next 26 to the lowercase a through z.
c) The next 10 to the digits 0 through 9.
d) And the last two to the character + & /.
e) This causes each triple of adjoining bytes to be mapped into four ASCII characters.

- Segmentation :
i) The length of Email is ~~usa~~ usually restricted to 50,000 octals.
ii) Longer messages are broken-up into smaller

segments & mailed separately.
iii) PGP provides subdivision of messages & reassembly at the receiving end.

Q.2. Write a short note on S/MIME.
→ i) S/MIME (Secure/Multipurpose Internet Mail Extension) is security enriched of MIME Internet email format standard.
ii) It is not restricted to mail.
iii) It can be used with any transport mechanism which transport MIME data.
iv) S/MIME is basically developed as the industry standard for organizational & commercial use, whereas PGP will be used for personal email security.

- S/MIME provides following Cryptography security services.
i) Authentication
ii) Message integrity using digital signing.
iii) Non-repudiation of origin.
iv) Privacy & data security using encryption.

- MIME header

Name :- Akash Sandosh kadkar
GI / Roll No.:- 5895 / 35
Signature :- Akash.

E-mail header	
MIME-VERSION: 1.1 Content-type: type/subtype content-transfer-encoding: encoding type content-id: message-id content-description: textual explaination of non texual contents Email body	MIME Header

- Benefits

i) Privacy :- The message is read by only indended receipient.

ii) Authentication :- Receiver of message knows that the message indeed arived from the apparent sender.

iii) Integrity :- Recipient knows the message was not altered while transmitting.

Q.3. Explain IPSec modes of operation

→ i) IPSec is the capability that can be added to present versions of internet protocol (IPv4 & IPv6) by means of additional headers for secure communication aerossl LAN, WAN & Internet.

ii) IPSec is a set of protocols & mechanism

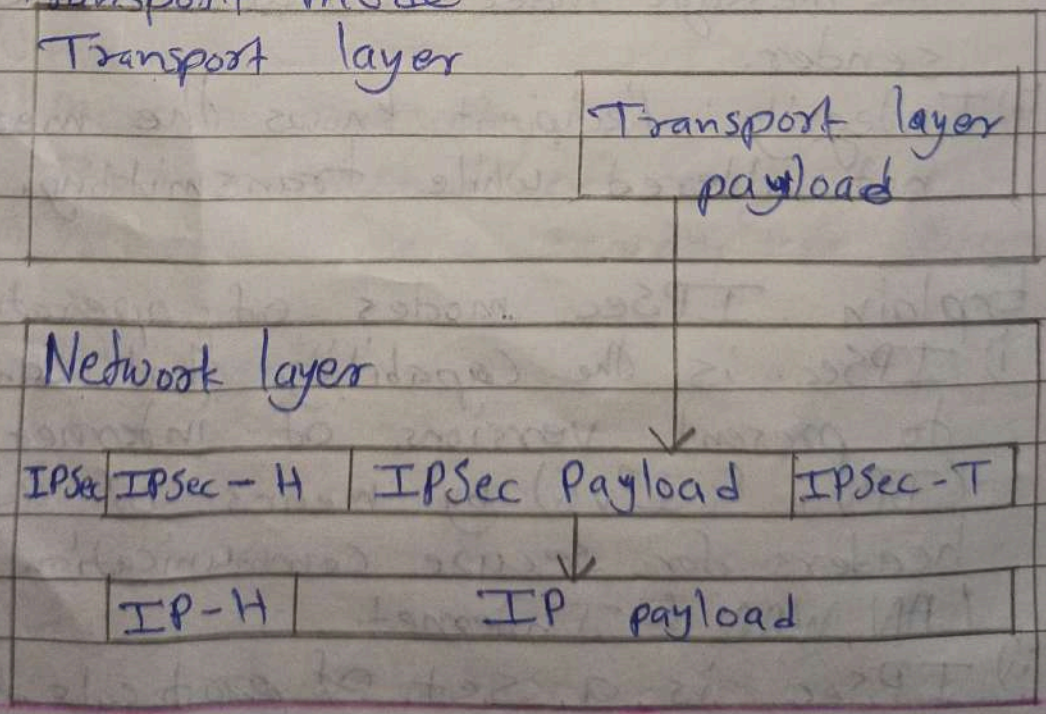
that provide confidentiality, authentication, message integrity & detection of IP layer

iii) The device (firewall or gateway) on which the IPSec mechanism resides is called as security gateway.

iv) A internet protocol general purpose mechanism is ensuring the authenticity & privacy of data i.e. passed over the internetwork. Therefore, security mechanism were needed to secure the data on the internet. That's why a set of protocols were designed to solve the security issues & these protocols are called as IP Security (IPSec).

v) IPSec has two modes of Operation.
- Transport mode
- Tunnel mode

- Transport mode



Name :- Akash Santosh kadkar
GI / Roll No.:- 5695 / 35
Signature :- Akash.

i) In Transport mode, IPSec protects what is delivered from the transport layer to the network layer. Therefore, protecting the payloads that is to be encapsulated within the network layer.

ii) Transport mode does not protect the IP header. It protects only the packet from the transport layer.

iii) In this mode, the IPSec header (& Trailer) are added to the information coming from transport layer. IP header is added later.

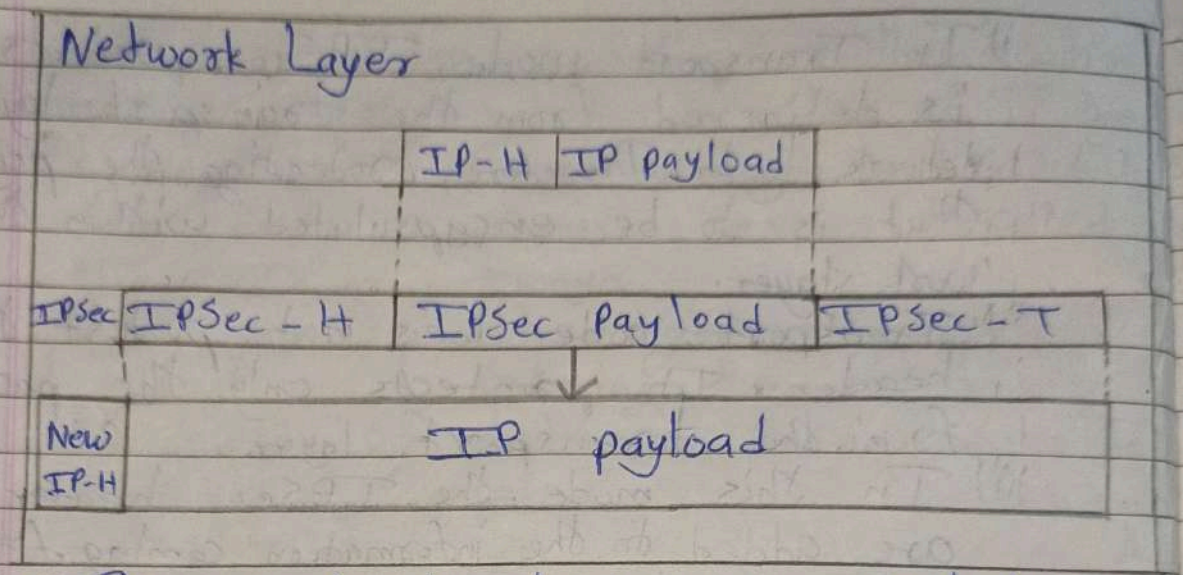
iv) Transport mode is normally used when we need host to host (end-to-end) protection of data.

v) The sending host machine uses IPSec for authentication or encryption of the payload which is delivered by the transport layer.

vi) The receiver host machine uses IPSec to verify authentication & / or decryption of IP packets & forward it to the transport layer.

- Tunnel mode

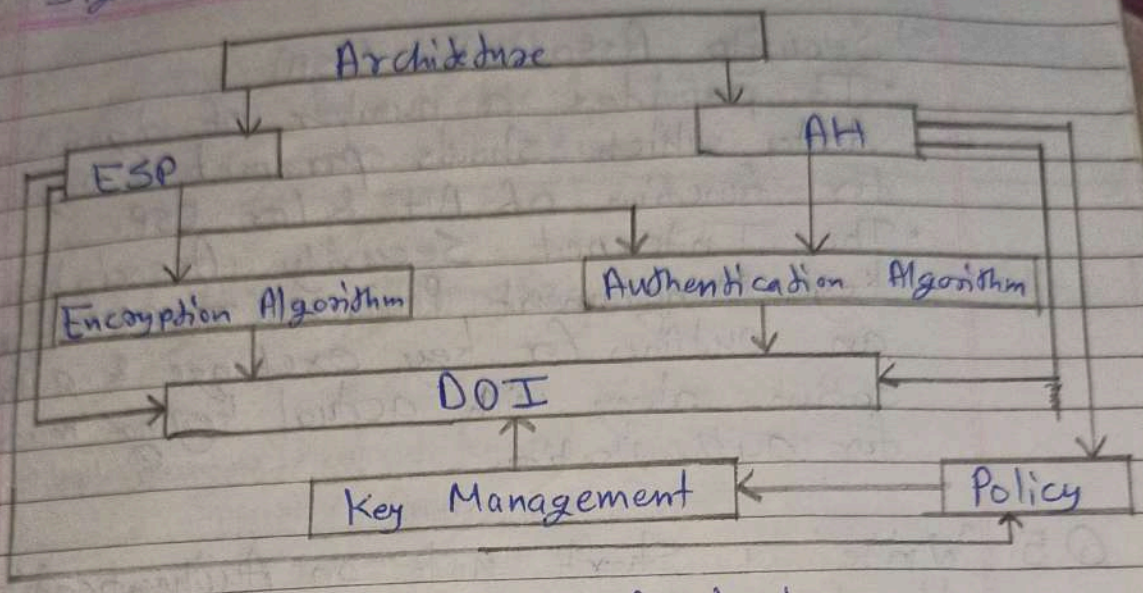
i) In Tunnel mode, IPSec protects the entire IP packet. It takes an IP packet, including the header, applies IP security method to the entire packet & then adds a new IP header shown in figure.



ii) This mode is basically used between two routes between a router & a host, between a host & router.
iii) Between sender & receiver the whole original packet is protected from invasion
iv) It seems like the entire packet transmits through an imaginary tunnel.

Q.4. Explain IPsec Architecture with the help of diagram.

→ i) It includes various components of IPSec, their interaction & Operation modes.
ii) It contains various protocols like EGP (Encapsulating Security Protocol), ISAK MP / Oakley (Internet Security Association & key Management Protocol), AH (Authentication Header), IKE (Internet key Exchange) & works like as shown in figure



iii) IPSec is an open standard.
iv) It is a part of IPV4 Suite.
v) IPSec is a suite of protocols interact with each other to provide the complete security in wireless enviornment.
vi) IPSec framework needs the host to provide data integrity using ESP or AH & IKE & providing confidentiality using ESP.
vii) It supports the following protocols for various operation performing.

1) Authentication Header (AH)
- It provides data source authendication & connectionless data integrity for IP datagram & it also assists in protection against reply attacks.

2) Encapsulating Security Payload (ESP)
- It offers data source authentication, confidentiality, limited traffic flow & connectionless integrity.

Name :- Akash Santosh badkar
GI / Roll No. :- A 5895 / 35
Signature :- Akash.

Page No. 11
Date

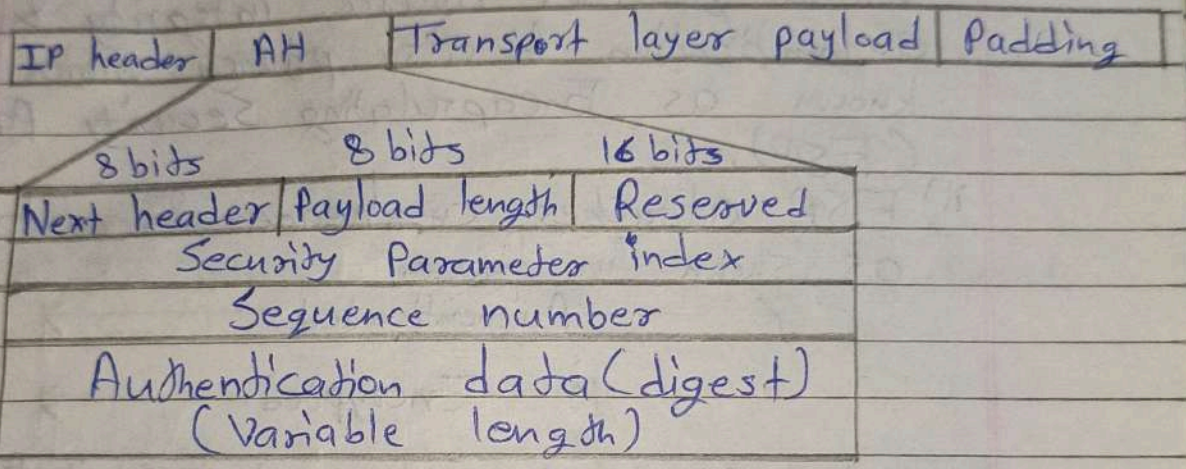
3) Security Association (SA)
- It provides a number of algorithm & data which shows parameters required for function of AH & / or ESP.
- The Internet Security Association & Key Manggement Protocol (ISAKMP) gives an outline for key exchange & authentication along with actual keying material for authentication.

Q.5. Write a short note on Authentication Header protocol.

→ i) It provides support for data integrity & authentication of IP packets.
ii) Data integrity service ensure that data inside IP packets is not altered during the transit.
iii) Authentication Service enables end user to authenticate the user at the outer end & decides to accepts or reject packets accordingly.
iv) AH is based on the other end & decides to accept or reject packet accordingly.
v) AH is based on the MAC protocol i.e. two communication parties must share a secret key.
vi) AH header format is shown in figure.

Name :- Akash Santosh Kadlam
GI / Roll No.:- 8095135
Signature :- Akash.

Data used in calculation of authentication data (except those fields in IP header changing during transmission)

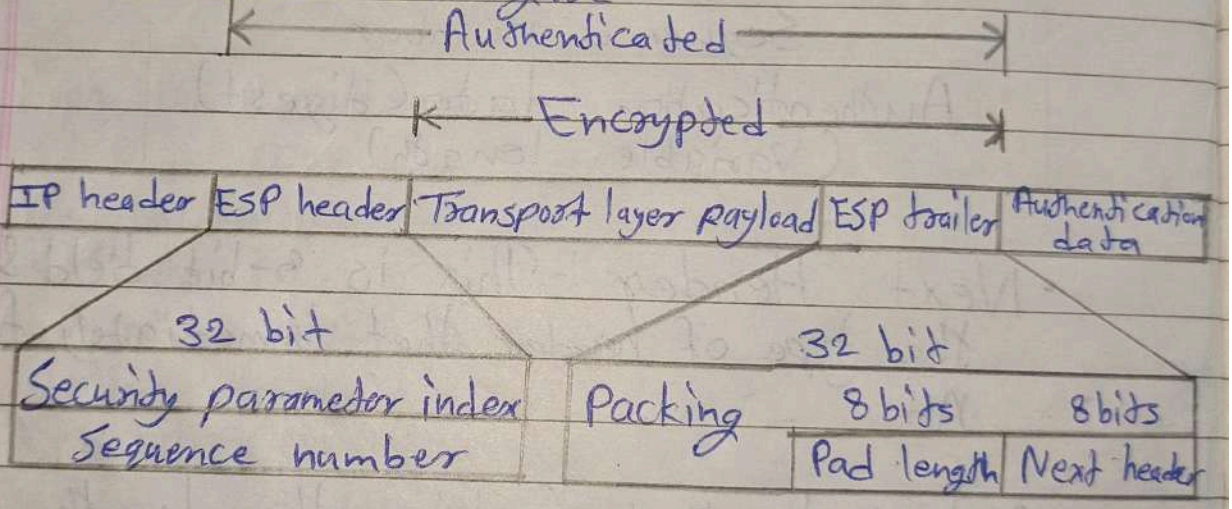


- Next Header :- This is 8-bit field & identifies the type of header that immediately follows the AH.
- Payload length :- Contains the length of AH
- Reserved :- Reserved for future use.
- SPI :- Used in combination with the SA & DA as well as the IPSec protocol used (AH or ESP) to uniquely identify the security association for the traffic to which a datagram belongs.
- Sequence number :- To prevent replay attack.

Q.6. Write a short note on Encapsulating Security Payload.

→ i) Because of the drawbacks of AH, IPSec describes an alternative protocol which provides source integrity & authentication & also privacy which is known as Encapsulating Security Payload (ESP).

ii) ESP attaches a header & a trailer as shown in figure.



iii) While including an ESP header & trailer in IP datagram in IP header the value of protocol is 50.

iv) A next header field within the ESP trailer contains the protocol's field original value which describes the payload type being accomplished by IP datagram like UDP or TCP.

v) Description of the header & trailer field are as follows.

• Security Parameter Index (SPI) :-

a) It is 32-bit field used in combination with the source & the destination address.
b) It identifies as security association.

- Sequence number :-
a) This 32-bit field is used to prevent replay attack.

- Pad ~~ding~~ length :-
a) Indicates the number of pad bytes immediately preceding this field.

- Padding :-
a) It contains the padding bits.

- Next header :-
a) It determines the type of encapsulated data in the payload.

- Authentication data
a) It is variable length field contains the authentication data called as the integrity check value for the datagram.

Q.7. Explain SSL Protocol Structure (SSL Architecture) with the help of diagram.

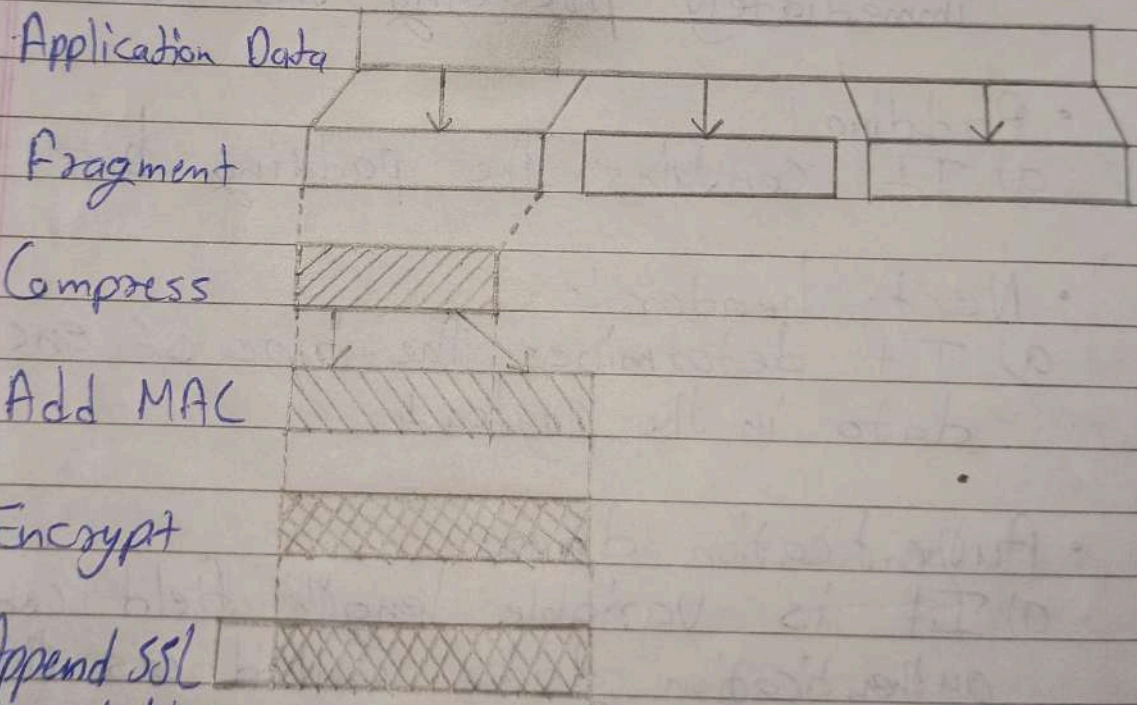
→

Name :- Akash Santosh kadkar
GI IRoll No :- 5895135
Signature :- Akash.

SSL handshake Protocol	SSL cipher Change protocol	SSL alert protocol	Application Protocol (e.g. HTTP)
SSL Record Protocol			
TCP			
IP			

SSL Protocol Architecture

1) SSL Record Protocol :
- It is used to send messages.
- Each message is divided into fragment

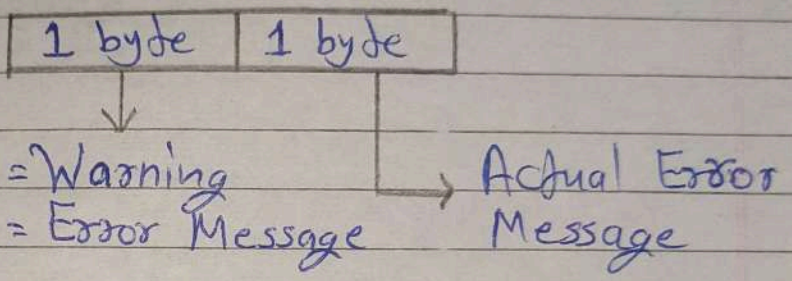


- Fragments are then individually compressed.
- Message Authentication code (MAC) is then appended to these compressed fragments
- It is them encrypted.

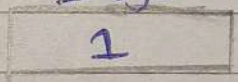
Name :- Akash Santosh Kadkar
GI / Roll No. :- 5895/35
Signature :- Akash.

- A header is then attached to these encrypted fragments called the SSL record header.

2) SSL Alert Protocol.
- It is used to send error Messages.



3) SSL Change cipher specification:



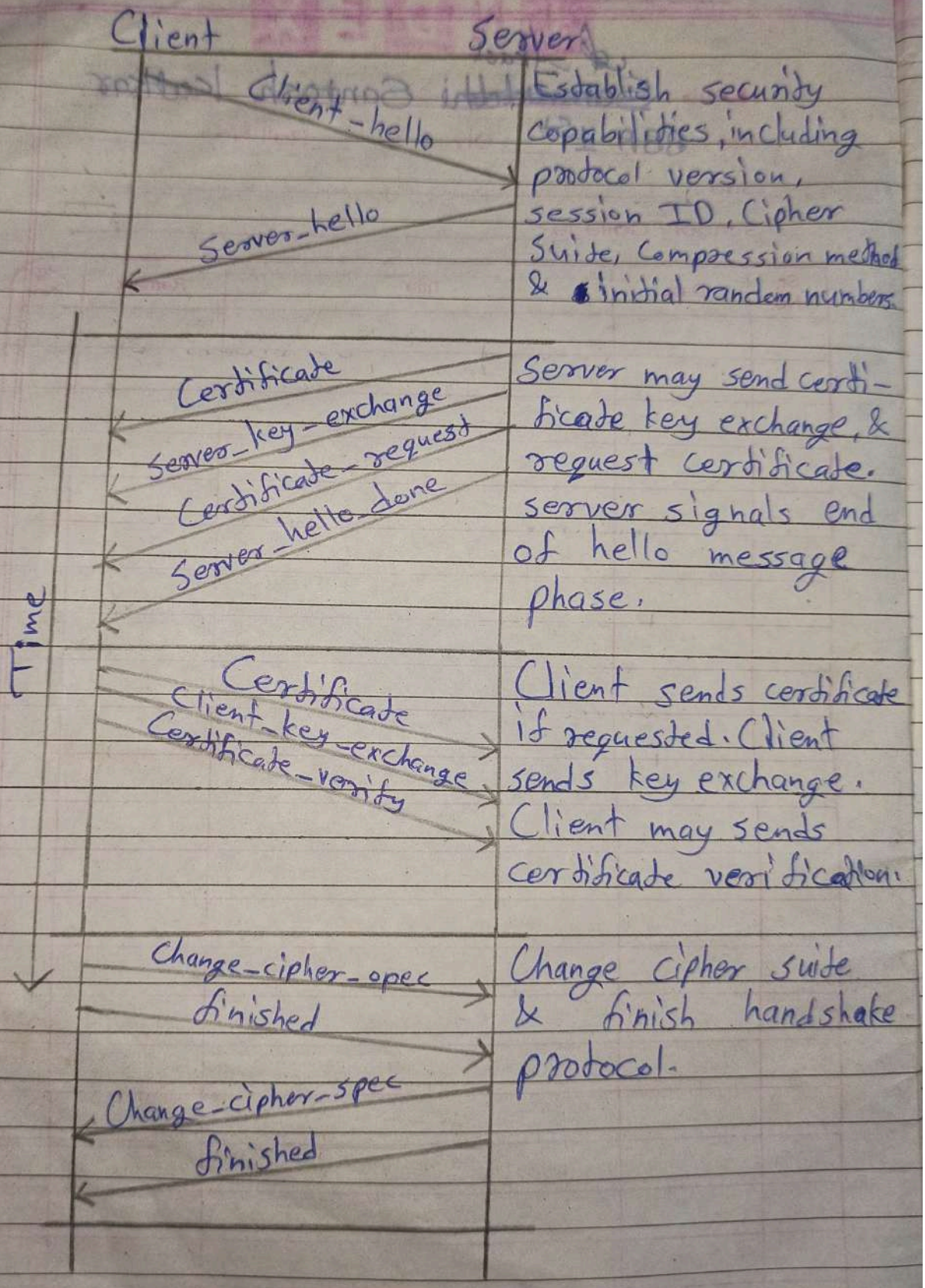
When client sends messages to server, server stores it temporarily.

- When storage Cipher specification is 1 the data is moved from temporary storage to permanent storage.

4) SSL Handuri Handshaking Protocol:
- Handshaking is used to set connection between two parties.

Name :- Akash Santosh katkar
GI / Roll No. :- 5895 / 35
Signature :- Akash.

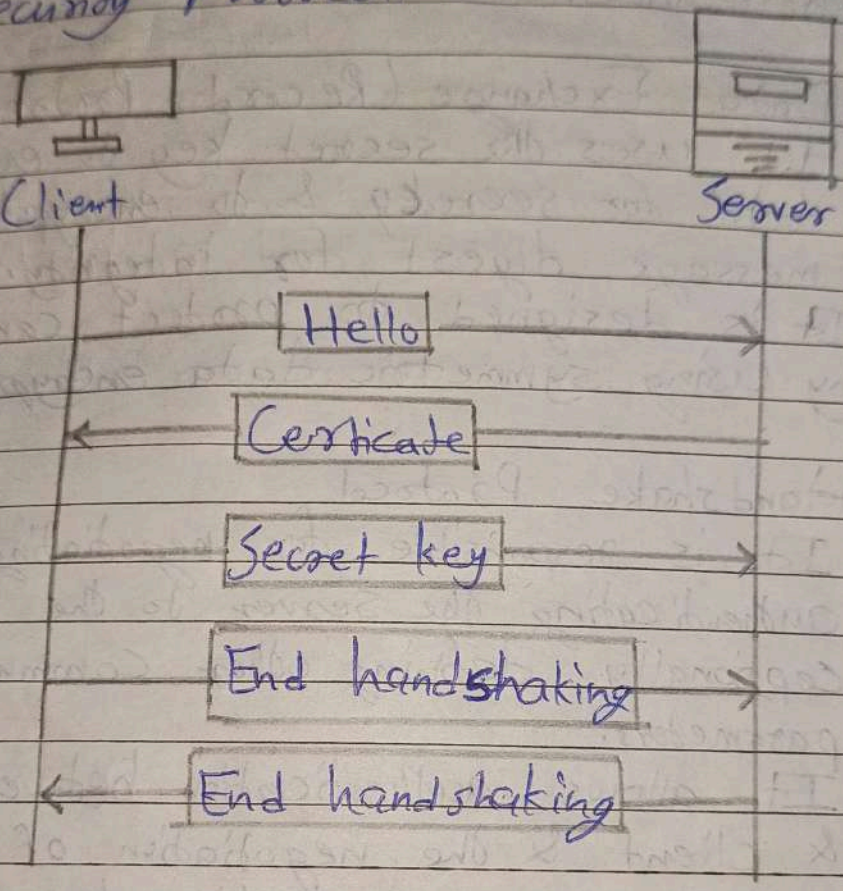
17



Name :- Akash Santosh kadkar
GI/Roll No.:- 5895/135
Signature :- Akash.

Q8. Write a short note on Transport layer Security Protocol.

→



i) TLS is a feature of mail servers designed to secure the transmission of electronic mail from one server to another using encryption technology.

ii) TLS can reduce the risk of eavesdropping, tampering & message forgery mail communication

iii) TLS based on SSL 3.0 protocol.

iv) TLS was designed to private & security at the transport layer.

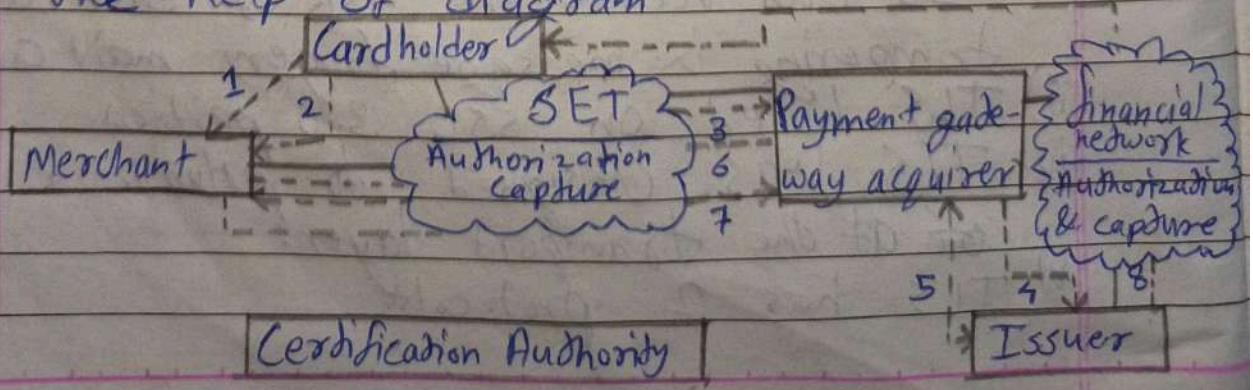
v) TLS has 2 protocols.

a) Data Exchange (Record) Protocol
b) Handshake Protocol

a) Data Exchange (Record) Protocol
- It uses the secret key to encrypt the data for secrecy & to encrypt the message digest for integrity.
- It is designed to protect confidentiality by using symmetric data encryption.

b) Handshake Protocol
- It is responsible for negotiating security, authenticating the server to the browser & optionally defining other communication parameters.
- It allows authentication between the server & client & the negotiation of an encryption algorithm & cryptographic keys before the application protocol transmits or receive any data.

Q.9. Explain architecture of SET protocol with the help of diagram



Name :- Akash Santosh Kadbar
GI / Roll No. :- 5895135
Signature :- Akash.

20

- Step 1 :- Consumer browser the merchant's website & initiates to purchase.
- Step 2 :- He sends payment & encrypted financial information along with his digital certificate to the merchant.
- Step 3 :- Merchant's website transfers the payment information to the acquirer (i.e. a payment card processing center or Merchant's Bank) while a CA certifies that digital certificate belongs to the card holder.
- Step 4 :- Acquirer checks with issuer (Consumer's bank) for payment authorization.
- Step 5 :- Issuer authorizes the payment.
- Step 6 :- Merchant receiver this approval.
- Step 7 :- Merchant completes the order by capturing the transaction & thus, consumer's credit card is changed.
- Step 8 : Issuer sends credit / debit card bill to consumer (card holder)

At last, Merchant ships the goods to consumer.

Q.10. Explain Intruder & its classes in detail
→ i) Same user who interrupts the privacy or resources of other users without ~~perpess~~ permission.
ii) ~~Inst~~ Intruders can be authentic user of a network or can be from outside the network.
iii) Three classes of intruders are
1) Masquerader
2) Misfeasor
3) Clandetine user.

1) Masquerades :- (Impersonation) (Outsider)
An individual who is not authorized to use the computer & who penetrates a systems access controls to exploit legitimate user's account.

2) Misfeasor :- (Insider)
An individual who is not authorized to use the computer & who penetrates a systems access controls to exploit legitimate user's account.

3) Clandestine User :- (Both insider & Outsider)
An individual who seized supervisory control of the system & uses this control to envade auditing & access controls or to suppress audit collection.

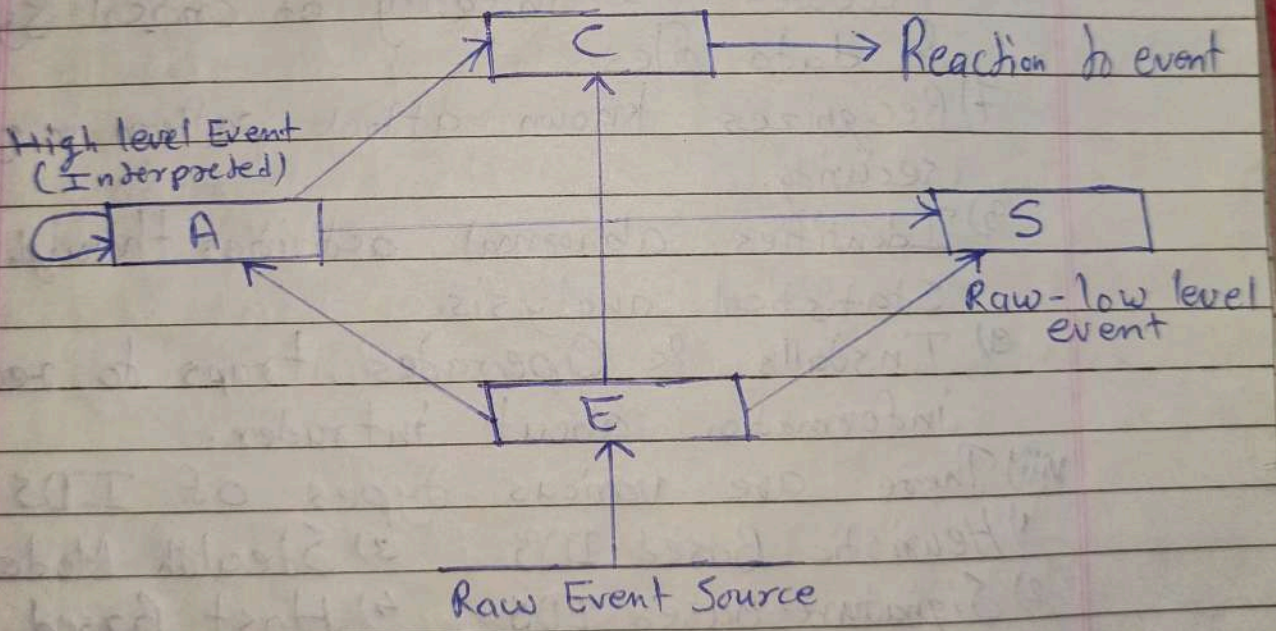
Name :- Akash Santosh kadam
GI / Roll No. :- 5895 135
Signature :- Akash.

Q.11. Explain ~~Instrue~~ Intrusion Detection System with the help of diagram.

→ i) It is a device that monitors activity to identify malicious or suspicious events.

ii) An IDS is a sensor (like a smoke detector) that raises an alarm if specific things occur.

iii) Four basic elements of an IDS are :-
1) Events (E) 2) Analysis (A)
3) Counter Measure (C) 4) Storage (S)



iv) IDS receives raw inputs from sensors, when an event occurs.

v) If it is a simple low level event then IDS simply stores inputs & takes same control measures.

vi) In case of high-level events, they can first

analyzed & then counter measures are taken & details are stored.

vii) An IDS performs various functions
1) Monitors user & system activities.
2) Audits System Configuration for valnerability & misconfiguration.
3) Correct System Configuration Errors.
4) Manages Audit Traits.
5) Highlights user voilation of policy on normal activity.
6) Accesses the integrity of critical system & data files.
7) Recognizes known attack pattern in system security.
8) Identifies abnormal activities through Statistical analysis.
9) Installs & Operates traps to record information about intruder.

viii) There are various types of IDS :-
1) Heuristic Based IDS
2) Signature-Based IDS
3) Stealth Mode IDS
4) Host Based IDS.

Q. 12. Explain Heuristic based IDS in detail.

→ i) Heuristic based IDS is also known as anamoly based IDS.
ii) It looks for behaviour that is not normal or out of ordinary.
iii) It builds a model of acceptable behavior & flag exception to that model.

iv) In future administrator can ~~work~~ mark a flagged behaviour (earlier exception) as acceptable, so new IDS will treat that previously exceptional behaviors as acceptable.

v) It has no database of signature, unlike signature based IDS.

vi) It is an intelligent system which does some calculation or analysis on its own to decide which behavior is acceptable & which is exceptional.

vii) Inference engine of an IDS performs continuous analysis of the system & raises an alarm if something out of ordinary happen.

viii) In heuristic IDS, all activities are classified into 3 categories :
a) Good
b) Suspicious
c) Unknown.

ix) With time & further analysis some actions may move from one category to other depending on IDS's learning, whether, certain actions are acceptable or not.

x) Advantage :-
- It can detect new attack or new viruses.

xi) Disadvantage :-
- It may give wrong prediction.

Name :- Akash Santosh Kathar
GI /Roll No.:- 5895 / 35
Signature :- Akash.

Q.13. Explain Signature based IDS in detail.

→ i) Signature for known attack types are stored in a database.

ii) Each & every incoming packet is checked with this database to check whether it is a match to any signature stored in database.

iii) If signature for an attack or a particular virus is not present in database, it would go undetected.

iv) This is similar to the way most antivirus software detects malware.

v) The common strategy for IDS in detecting intrusion is to memorize signature of known attacks. The ~~indent~~ inherent weakness in relying on signature is that the signature pattern must be known first.

vi) New attacks are often unrecognizable by popular IDS.

vii) Advantage :-
- It can be used to detect viruses & other attacks very effectively if database is upto date with signature of all latest & possible attacks.

viii) Disadvantage
- It can't detect any new virus or attack whose signature is not present in database.

Name:- Akash Santosh Kadkar
GI | Roll No.:- 5095/35
Signature:- Akash.

Q.15. Explain Virus & any 5 types of Viruses.

→ 1) A small piece of software attached to programs is known as virus.

2) It spreads from one machine to another by leaving its infection on route.

3) Some virus effects are mild which can be ignored while others can damage software, data, files & hardware.

4) Virus needs human intervention to get spread.

5) It cannot infect the system unless we execute or open the file or program containing it

- Types of viruses

i) File infector virus.

a) A file-infecting virus is one of the most common types of virus.

b) Typically, it infects files with .exe or .com extensions.

c) When the infected file is accessed or executed, it may be partially or completely overwritten by the virus.

d) A file infecting virus can also spread across the system & over the network to infect other systems.

ii) E-mail Virus

a) An email virus is a virus that is sent with or attached to email communications.

While different types of email viruses work different ways.

b) Email viruses run the gamut - from creating popups to crashing systems or stealing personal data.

c) Email viruses also vary in how they are presented.

iii) Boot Sector Virus.

a) A boot sector virus is a computer virus that infects a storage device's master boot record (MBR).

b) It is not mandatory that a boot sector virus successfully boot the victim's PC to infect it.

c) As a result, even non-bootable media can trigger the spread of boot sector viruses.

d) These viruses copy their infected code either to the floppy disk's boot sector or to the hard disk's partition table.

iv) Macro Virus

a) The macro virus is initially embedded in one document or a few documents, but it can spread to other documents within the same computer, as well reaching out to other computers through shared documents.

b) Unfortunately, not all macro viruses can be detected by anti-virus software, although there are some good products available that can be used to detect them.

v) Stealth Virus

a) A stealth virus is a hidden computer virus that attacks operating systems process & averts typical anti-virus or anti-malware scans.

b) Stealth viruses hide in files, partitions & boot sectors & are adept at deliberately avoiding detection.

Q.15. Explain Life Cycle of Virus.

→ There are various phases in file cycle of virus.

1) Dormant phase

- In this phase virus is inactive.
- The virus gets activated by executing the events.
- All viruses may not have this phase.

2) Propagation phase.

- Virus replicates itself & attaches itself to same program.
- The replica may have slight changes as virus changes their forms to avoid detection.

- Every virus infected program contains copy of the virus which enters itself into a propagation phase.

3) Triggering phase
- Virus performs the function it is intended for
- Many system events causes the triggering phase such as counting how many times virus replicates itself.

4) Exception phase
- Virus executes its function which can be harmless like just a message on the screen or damaging like deletion of information or program.

Q.16. Explain Counter measure of viruses in detail.
→ i) There are various counter measures to overcome the risk of attacking virus.
1) Antivirus
a) Rather than detecting & removing viruses, it is always better to prevent it.
b) Do not allow virus to enter into the system & also block it to make modification in the systems file.
c) Dedection :- Try to locate the virus by the type of its infection.

d) Identification :- Once detected, find out that specific virus which has infected the program
e) Removal :- Once identified, try to remove almost all virus traces from infected areas so that it cannot spread anymore.
f) A good antivirus should be installed & updated regularly.

2) Generic decryption
a) GD facilitates the antivirus program to speedily scan & easily detect most complicated polymorphic viruses.

3) Digital immune system
a) IBM developed Digital Immune System for virus protection.
b) The main aim behind this growing threats of internet based virus spreads.
c) When a new virus enters in network digital immune system automatically detect it, analyse it, capture it, protect against it, deletes it & also spreads information about it to other systems running IBM Digital Immune System so that it can easily be detected before its execution.

4) Behaviour blocking Software.

a) Behaviour blocking software along with as observes behaviour of a program in real time for harmful actions.
b) Then this software blocks potentially harmful actions before it harms to system.
c) Observed behaviour includes.
I) Attempts to perform operation which are unrecoverable or formatting of disk drives.
III) Modifying the contents or logic of the executable files.
IV) Alterations in coucial system settings.
V) Interruption in network communication.

5) Updating Vaccine Software like antivirus
a) Antivirus ~~vaccine~~ software ~~like antivirus~~ should be installed & updated periodically to protect against viruses.

6) Scanning of Email attachment files.
a) While downloadding email attachment files we should:
- Be very cautious with email attachments of unidentified sources.
- Not to be mislead by apperance of attachment files.
- Be ~~cautious~~ cautious of doubtful files attached to emails even though you received them from

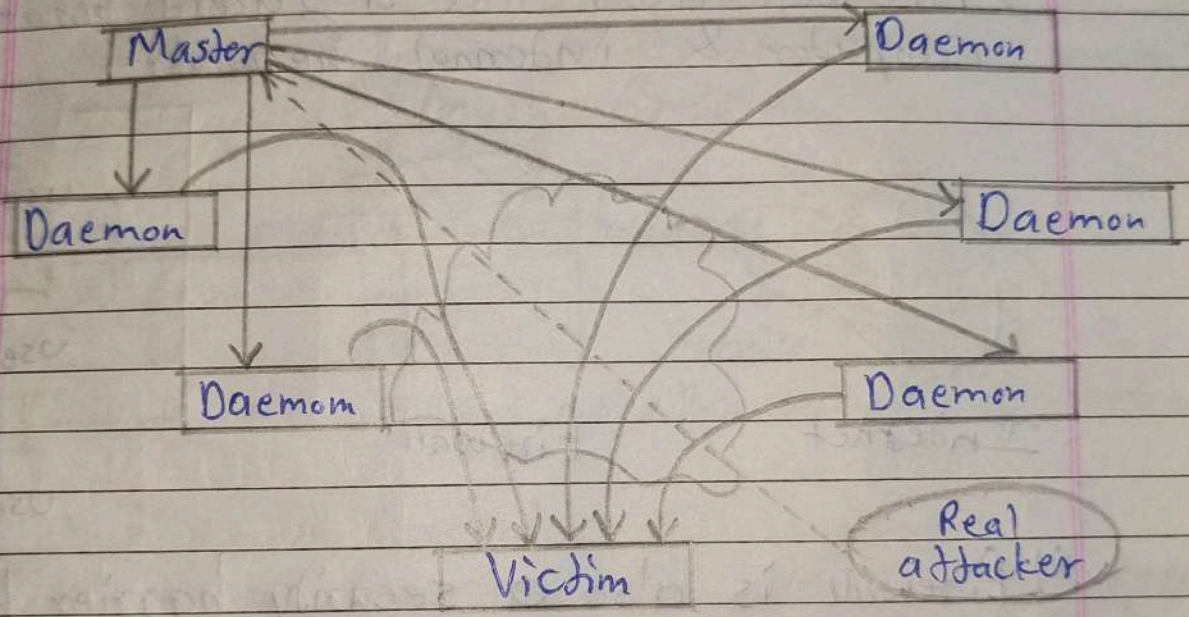
Name :- Akash Santosh kadkar
GI / Roll No. :- 5895 / 35
Signature :- Akash.

Page No. 32
Date

known resources.

Q.17. ~~Email~~ Explain Distributed DoS in detail.

→ i) It uses multiple computers within network or even outside the network to launch a synchronized DoS attack for target machine.



ii) Using client server technology, attacker increases its effect by exploding resources of innocent assistant computers.

iii) Basically master program of DDOS is installed on one computer using a stolen account.

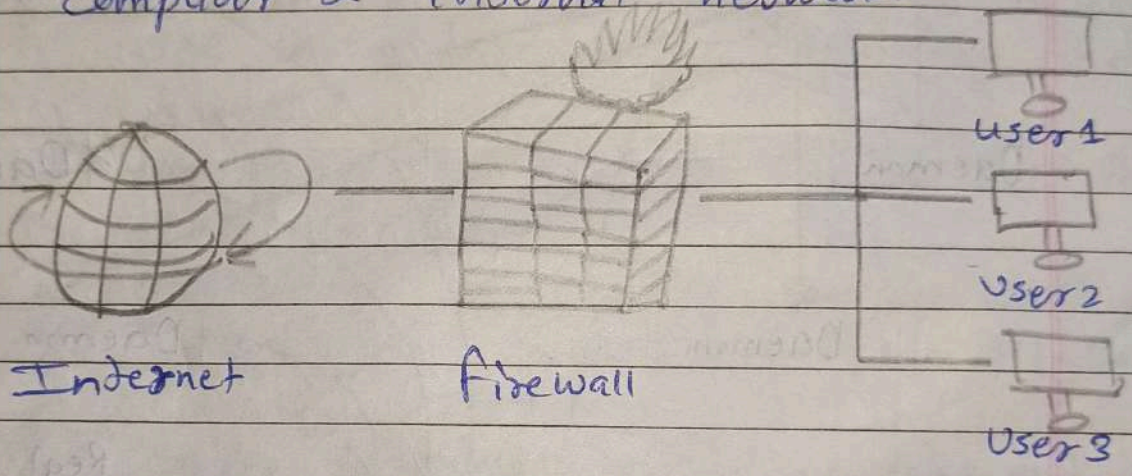
iv) This master program then is prescribed time communicates with multiple agent program on the network.

v) Agent when receive these commands initiates thousands of agents.

vi) DDoS attacks make systems inaccessible by flooding network with useless traffic so that authenticated users never gets access to these resources.

Q.18. Explain firewall & its design principles.

→ i) Fire wall acts like a guard between your computer & internal network.



ii) Firewall is also a security barrier between two networks that screens traffic coming in & out of the gate of one network, to accept or reject connections & services according to a set of rules.

iii) Firewalls are present at boundary of Internet & internal network (Ex: LAN)

- Firewall design principles

1) Aims:

a) Establish a mangged ~~disk~~ link.

b) Protect the local network from internet attacks.
c) Provide a single block point.

2) Design goals.
a) All traffic from local network to internet must pass through firewall.
b) Only authorized traffic will be permitted to pass through firewall.

3) Four general techniques
a) Service control :-
Control internet services types that can be accessed whether inbound or outbound.

b) Direction Control :-
Controls the route through which a specific service requests are allowed to move.

c) User Control :-
Determines the service access that which user is allowed to access it.

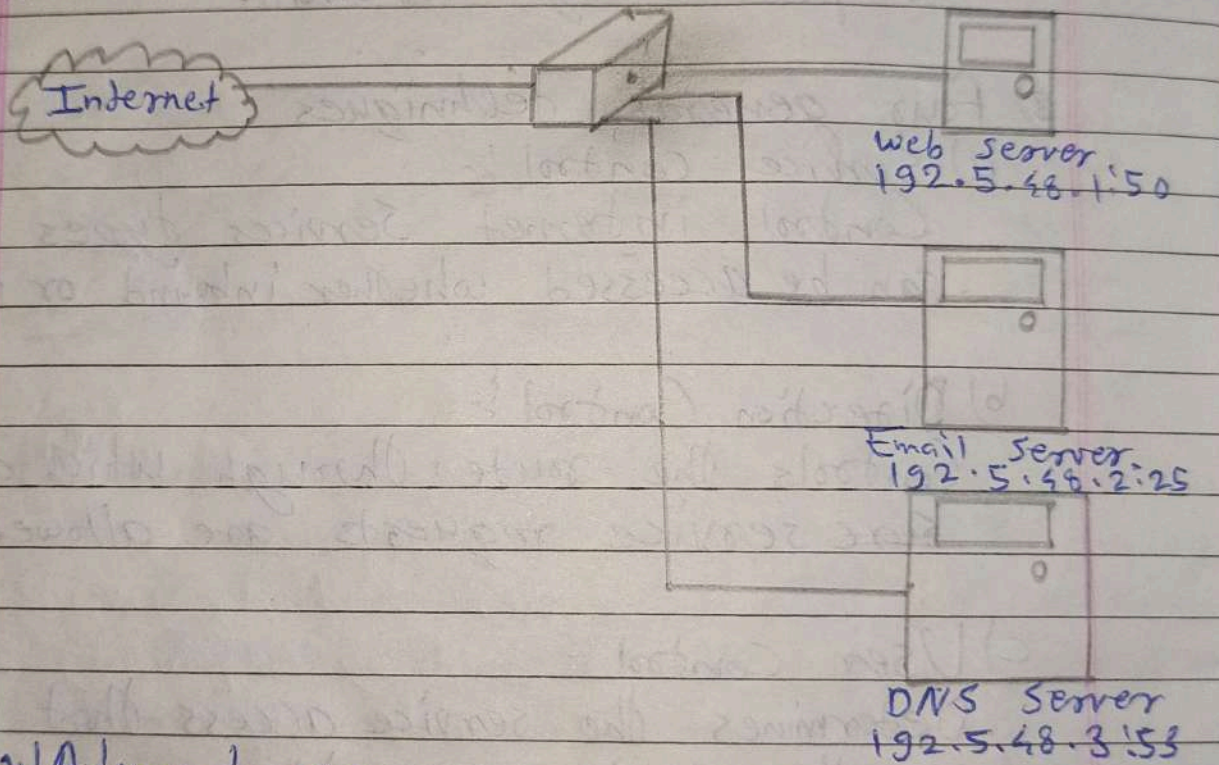
d) Behaviour Control :-
Control the way specific services are used.

Q.19. Explain Packet filtering Gateway Firewall.
→ i) It is the simplest & in some situations the most effective firewall.

ii) It controls access on basis of packet address (address of source & destination) or specific traffic protocol.

iii) In other words, it only checks the IP addresses in the packets (source & destination).

iv) It does not look into the contents i.e. internal data of the packet.



v) Advantages
- Ease of working
- Transparency in working forwards users
- faster

vi) Disadvantages :-
- Difficult in framing packet filter rules.
- Absence of authentication.

Name :- Akash Santosh kadkar
GI / Roll No. :- 5895 / 35
Signature :- Akash.

Q.20. Explain Statefull inspection Firewall.

→ i) This firewall maintains information from one packet to another in input stream.

ii) It accumulates a number of packets together & then checks them together.

iii) An attacker may split & distribute virus into multipacked. The virus is divided into small pieces that cannot be recognized or detected by virus scanner.

iv) This firewall accumulates these packets & then checks them to thwart such an attack.

v) Advantages :-

- Client server model not used.
- Complex & difficult packet screening management.