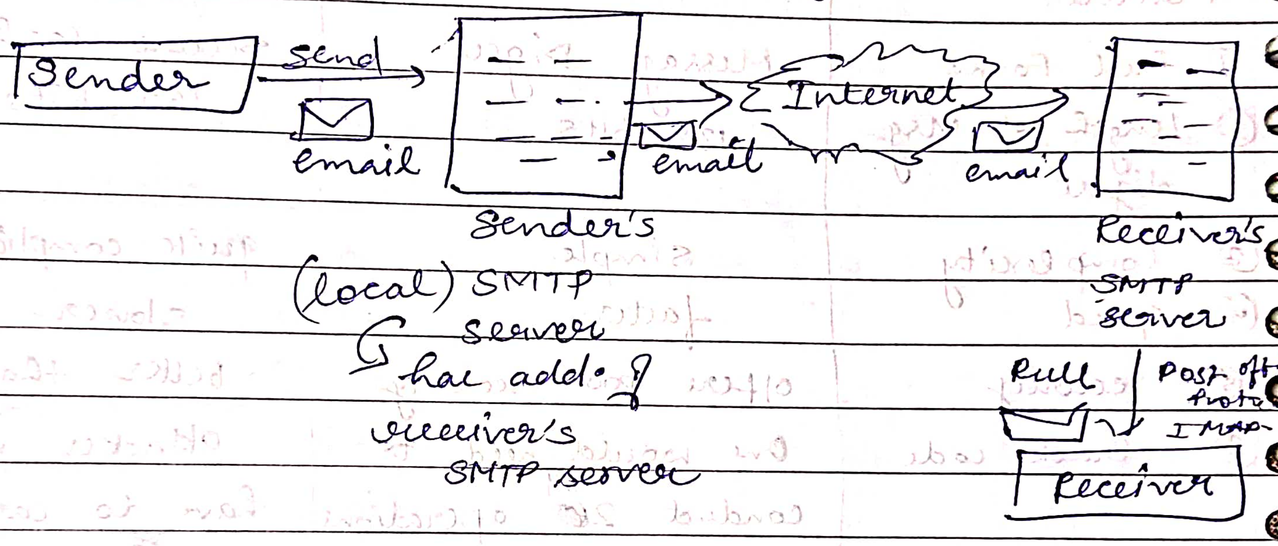
4|03|24

Email Security.

Two components
→ Header
→ Content (Body)

Email Communication

SMTP used for email comm.
- runs on application layer of TCP/IP.



Email Security

PEM | PGP | S/MIME

Pretty good privacy

1) Pretty good Privacy

(I) Digital sign. MD encrypt with sender pvt key
(II) Compression → I/P msg. & digital sig. ⇒ compressed → due to faster encry. ↳ Lampbell - Ziv - Compression tech.
(III) Encryption → IDEA algo. ↓ CT
(IV) Enveloping → sym. key encry. w/ receiver public key
(V) Base 64 encoding

PT → what is ur name
my name is XYZ
what 2 ur 1
name 1
ur 2
my 1.2 XYZ
Pointer is also used,

IP message
↓
24bit | 24bit | ...
↓
6 | 6 | 6 | 6
↓
decimal value → compare with table
↓
A → ascii value → [ ]

UNIT-3

IP Security

Application Layer → Second higher level sec (SSL, PGP, MIME, SHTTP PEM, etc)
↑
Transport Layer
↑
Internet Layer → First higher level security
↑ IP Security
Data link Layer ↓
↑ Two protocols
Physical Layer → AH (authentication header)
→ ESP (Encapsulating security payload)

IP Sec Packet

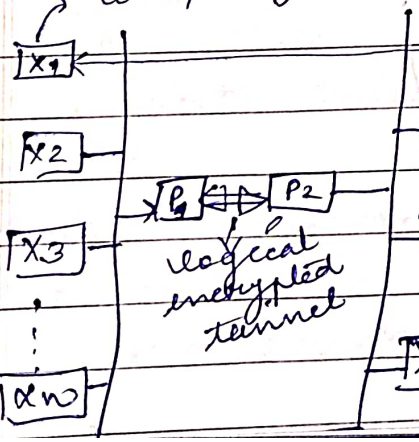
| AH | Payload |

- authentication
- Integrity
- Anti-Replay Attack services
- Confidentiality
- Encryption of msg

AH & ESP Modes of operation

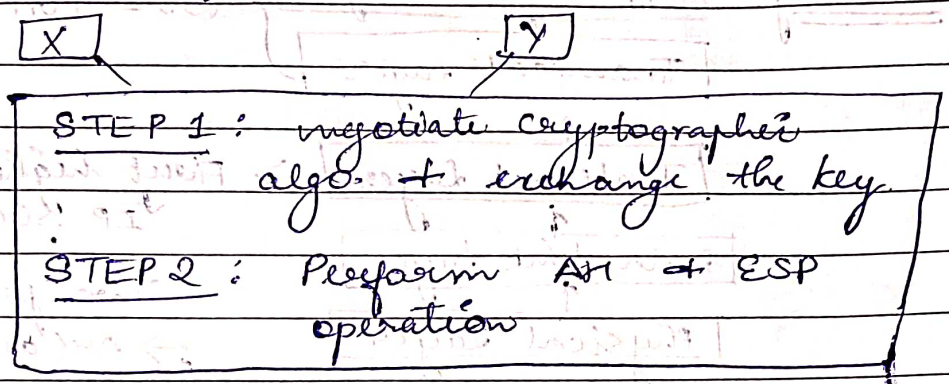
↓
Tunnel mode
- Logical encrypted tunnel is established b/w communicating parties
- X will send the data to its proxy at sender's side

↓
Transport mode
- Source add & Dest add are not encrypted



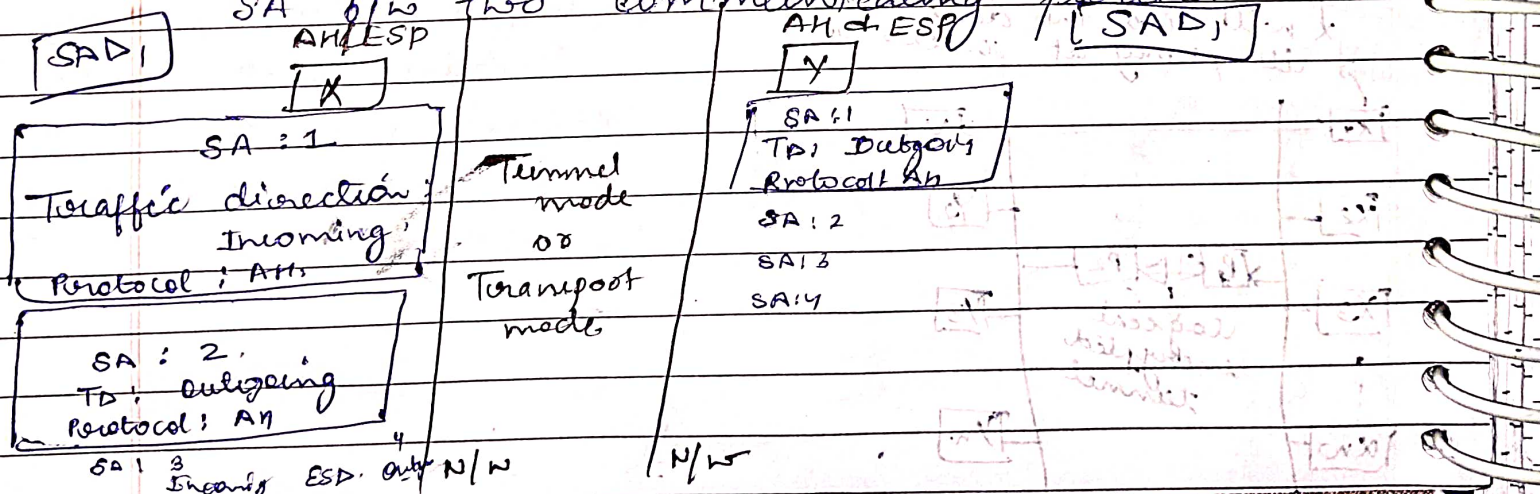
Internet Key Exchange protocol.

Main purpose
- to negotiate the cryptographic algo. it used for encry. the data.
- Exchange of Keys.



- **Security Association**
  → o/p of Internet Key Exchange protocol is SA

It is agreement b/w two communicating parties regarding IPP security protocol version in use, cryptographic algo, exchange of cryptographic keys & the lifetime of keys.
- main purpose of IKEP is to establish SA b/w two communicating parties.

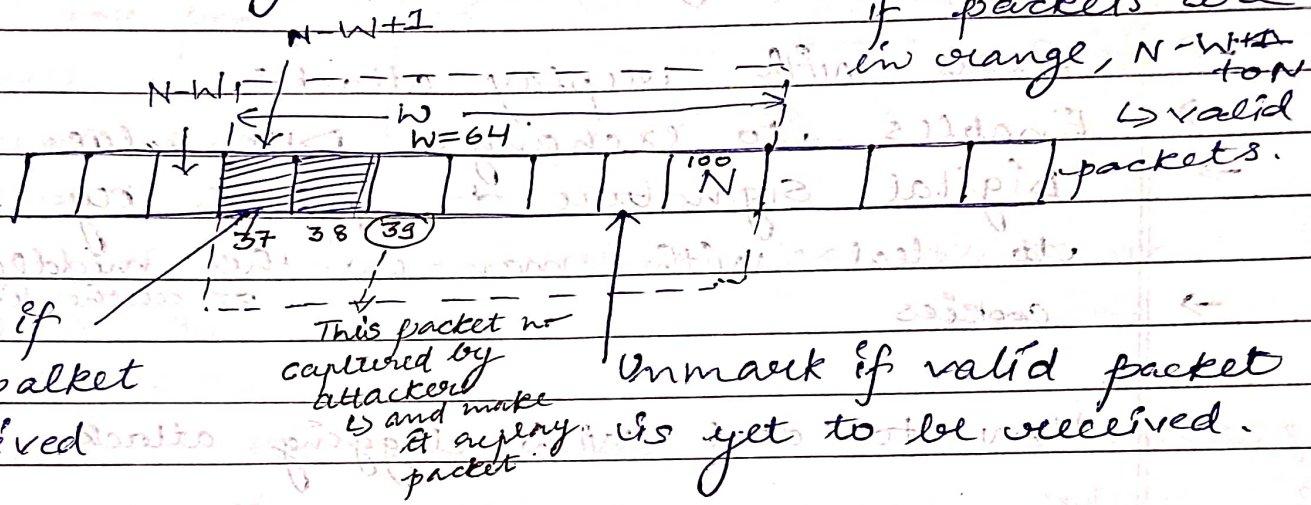


Sparge → Security Association Database.

PAGE No
DATE : / /201

Dealing with Replay Attacks (AH)

- AH maintains a field known as Sequence no.
- Initially seq. no, N = 0 ; if packet arrives N = N+
- If packet size large, $2^{32} - 1$ to 0, never circle back.
- Receiver maintains a window, sliding window and this window move one by one as we are receiving packets.



CASE I : If range of packets seq no are b/w N-W+1 to N, then receive this packet & treat as valid packet.

CASE II : If packets seq no. less than N-W+1 then, it is replay packet & discard it.

Case III : If packets seq no is greater than N, then shift the boundary with highest value of packet seq. no.

- Bursty packets.
- In case of congestion, even valid packets are treated as invalid

• various features of clogging attack

PAGE No
DATE : / /201

Oakley Key Determination Protocol.

Refined version of Deffie Hellmen Key Exchange Protocol

• Clogging or Congestion attack
↳ Attacker sends too many DHK value & host is busy in calculating these DHK value.

→ Deals with replay attacks.
→ Enables to exchange DHK values
→ Digital signature & public key encryption to deal with man-in-the-middle attack or authentication.
→ cookies

How to deal with clogging attack

CASE-I

[X] ⟶ [Y]

[X]	[Y]
DHK value, cookie, other info → encrypted with pvt key	DHK value, cookie, other info → Decrypt with public key of X

CASE III

Y will prepare its own DHK values, cookie & acknowledgement → Encrypted by pvt key of Y

CASE-III

[X] → encrypt by public key of Y and send msg

if DHK values, cookies are matched

Firewall

Specialized router which protects the corporate n/w by standing b/w the n/w and outside world.

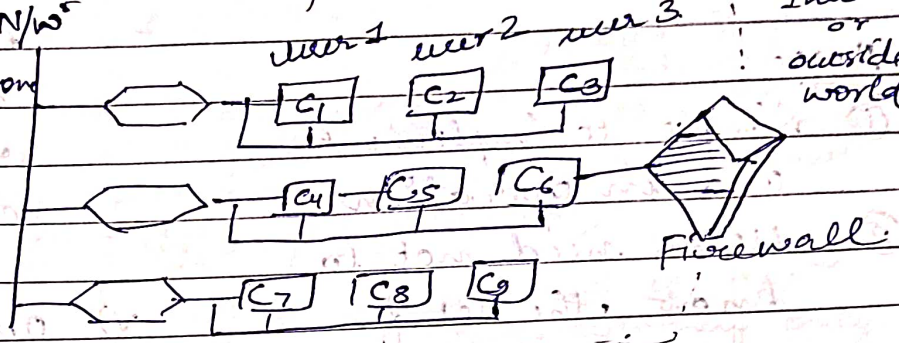
Features

→ All incoming & outgoing traffic must pass from firewall.

→ Firewall decides whether incoming or outgoing traffic should go inside or outside the n/w

→ Security policy.

→ Firewall should be strong enough so as to render the attacks on it is useless.

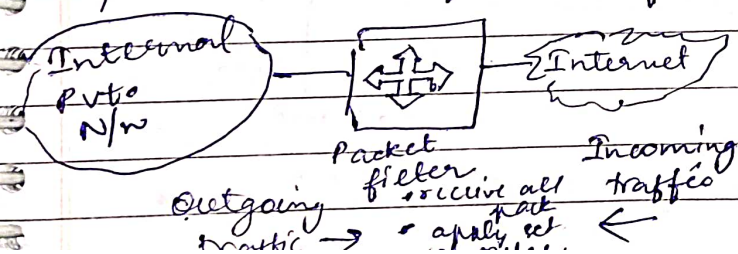


Types of Firewalls

↓

Packet Filter (Screen Router)

- Set of rules, every pack must pass through pack filter
- It will check whether pack is satisfied set of rules.



↓

Application gateway

→ proxy server

I) Users request the app^n gateway by HTTP/TELNET using TCP/IP applications.

II) App^n gateway ask user to supply user id, password domain remote host etc.

default rule says either accept all packets or discard

ADV.

① Simple to implement and in operation

② Users need not to know the set of rules.

③ Packet filter operation is very fast.

DIS Adv.

① Setting no. of rules correctly is difficult

② Lack of support for authentication.

③ Attacks may be possible (IP add. spoofing attack. To overcome we go for dynamic packet filter.

Another gateway
↳ circuit gateway
change IP address ← ↳ perform some additional op.
{ user - with changed IP add comm with user

III) User supply all these details.

IV) Appln gateway on behalf of user establish a new connection with remote host & communicate with it.

V) Operations are not visible to users

ADV.

→ More secure.

→

Disad

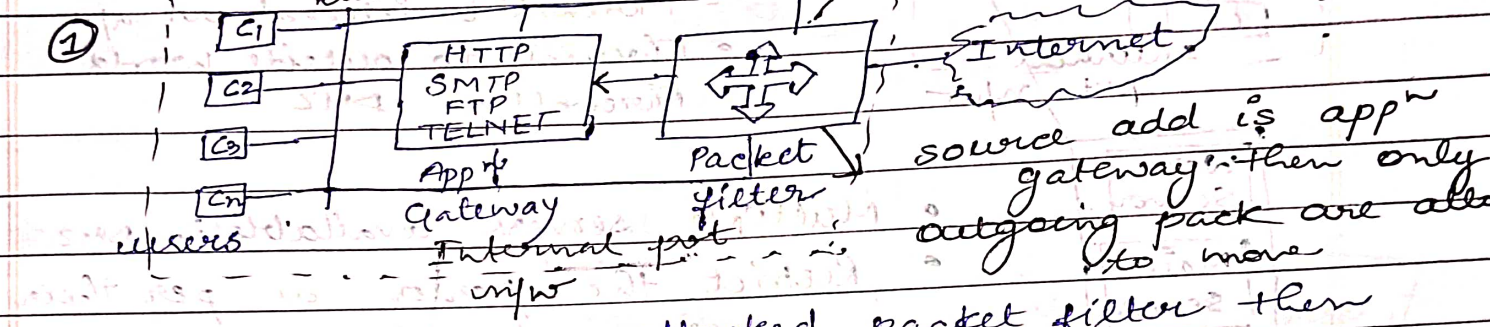
→ More connection

Firewall Configuration / DMZ → Implementing both packet filter + app. gateway

① Screened Host firewall with single home bastion

② Screened host firewall with dual homed bastion

③ Screened Subnet Firewall



- if attacker somehow attacked packet filter then whole n/w exposed to attacker.

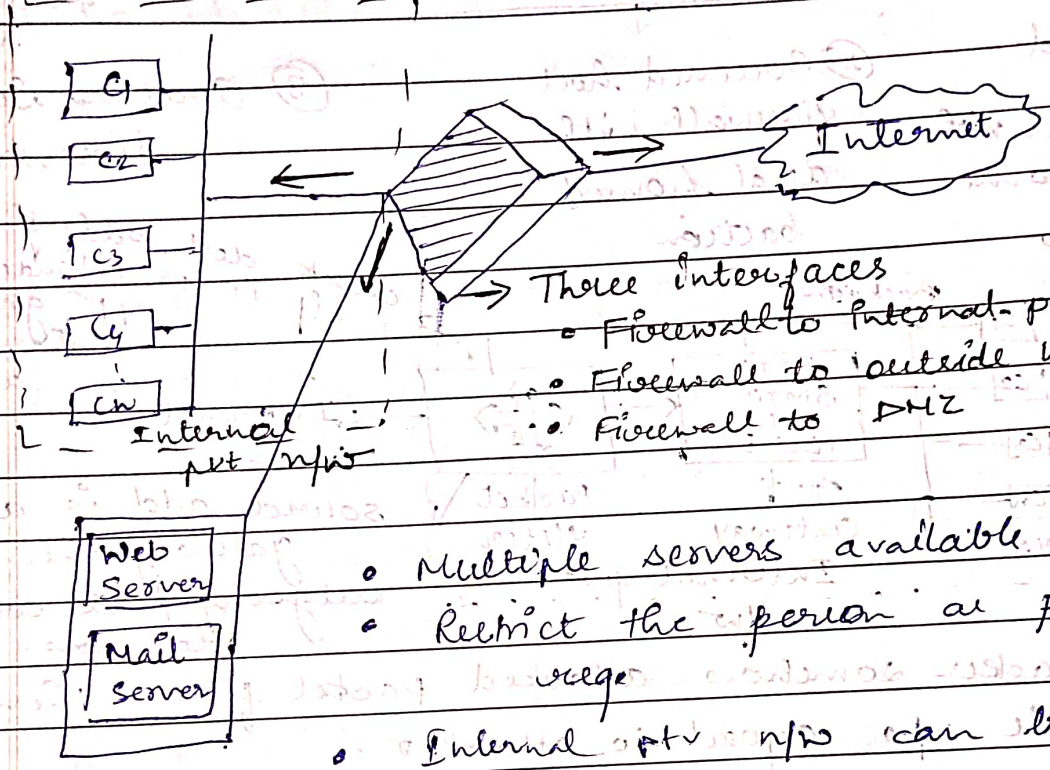
② C1 C2 C3 C4 — HTTP SMTP FTP TELNET — Internet

- Attacker has to attack on app^n gateway also, to get access of whole n/w

③ C1 C2 C3 Cn — Backbone — App^n gateway — Internet — Internet pvt. n/w

- highest level of security.

Demilitarize Zone (DMZ) n/w



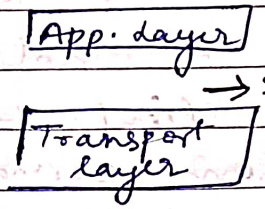
- Multiple servers available in DMZ
- Restrict the person as per their usage
- Internal pvt n/w can be safe

Firewall limitations

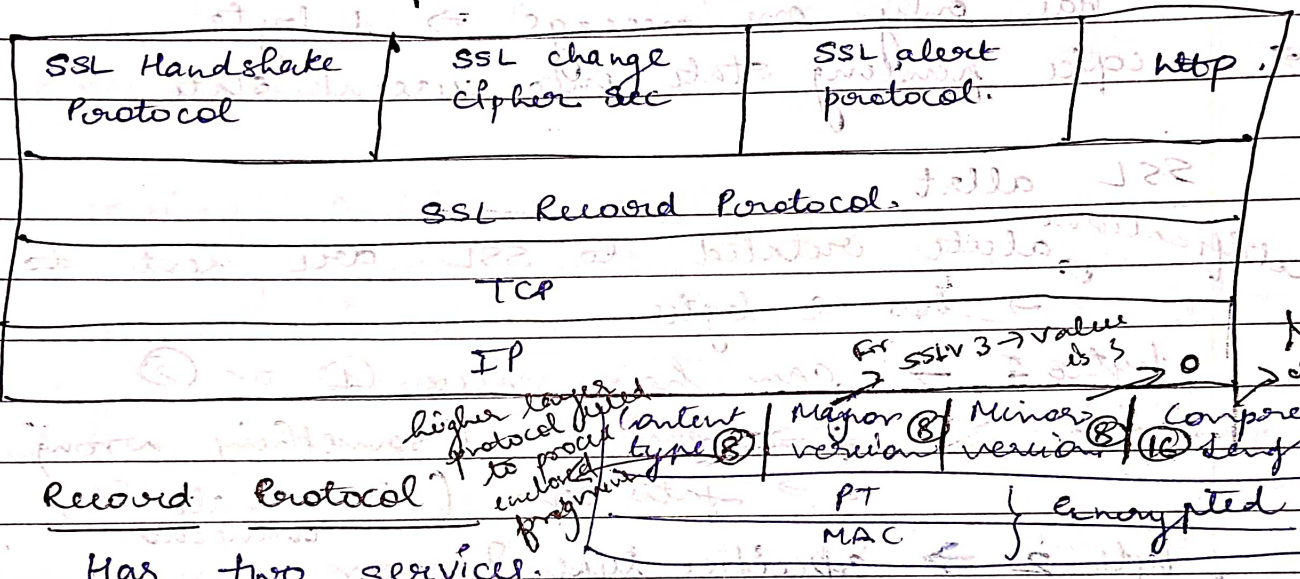
1) Insiders intentions
2) Direct Internet traffic
3) Virus Attacks.

Secure Socket Layer (SSL)

→ Used to provide security for communication b/w 2 users
  → ensures Integrity, authentication + confidentiality
→ lies b/w application layer + transport layer of TCP/IP



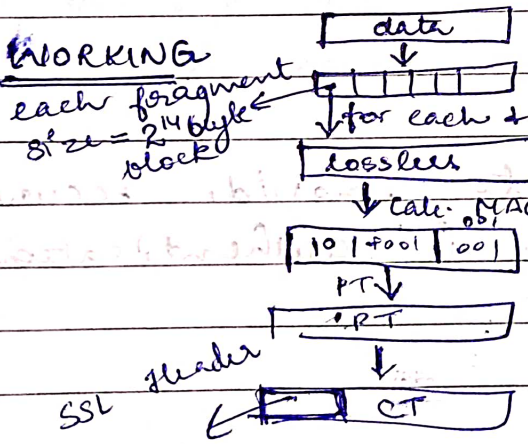
Protocol Stack of SSL.



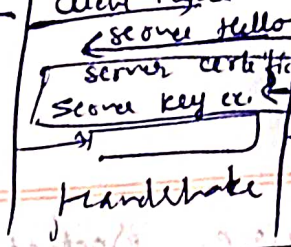
SSL Record Protocol

Has two services:
→ confidentiality (by encryption)
→ Message Integrity (by MAC) Msg authentical code

WORKING



SSL version
session id
Cipher suite
compression method



SSL Handshake Protocol

- Ensure Authentication
- Key exchange b/w client + server

WORKING

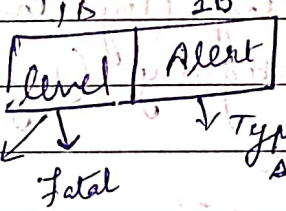
① Client will establish connection with server
② After that server will send a key to the client (key exchange) to check whether client is authorized person or not → server certificate
③ Key exchang from client to server → client certificate
④ Handshake done from server → client current status of crypto algo through cipher change spec

SSL Change cipher spec

Has only one message ⇒ 1 byte
⇒ copies pending state into current state

SSL alert

notification of alerts related to SSL are sent to client.
→ has 2 bytes
byte 1 → can have value ① or ②
1 → warning (something wrong is happ)
2 → fatal error (terminate it connection)
byte 2 ⇒ specifies type of error



KOMAL GUPTA

Q What is hash func? How to provide security using hash func? What is authentication req. in hash func

Qu. Explain DS

Qu. What is SSL

Qu. What is firewall & functioning of firewall

UNIT - IV

CYBERSECURITY

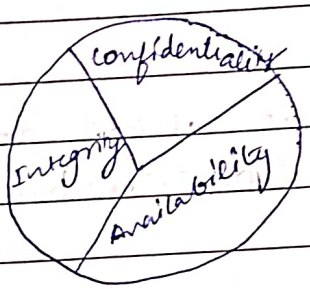
- name for safeguards to avoid or reduce disruption from attacks on data, computer sys. or mobile devices.
- It is process or technique used to protect the sensitive data / information, s/w from cyber attackers / hackers.
- Improving Online Security
  - → Move away from unsupported s/w
  - → Always download and install latest s/w.
  - → Always use strong passwords.
  - → Don't click on unknown attachments or link.
  - → Backup your data
  - → Make your staff cyber aware.
  - → Manage Security mechanism with your suppliers.
  - → Always use latest or updated antivirus s/w.
  - → Delete spam emails.

Need of CyberSecurity [To overcome Threats

1) Ransome
2) Botnets Attacks → Distributed DOS
   → Spreading spam mails
   → stealing confidential info.
3) Social Engineering Attacks
4) Phishing

Key concepts of cyber Security or Basics

CIA rule



Cyber crime

Illegal usage of communicating devices to commit or facilitate illegal act.

Individual or team who using their skills performs illegal act is cyber criminal

cyber space
↳ Internet is component of cyberspace

Three layers
→ Physical
→ Logical
→ Social

Components
→ geographical
→ Physical N/W
→ Logical N/W
→ Cyber persona
→ persona

vectors 3D.
Complex

Cyber crime

- Cyber crime against individual
- cyber crime against property
- [against society] → cyber crime against government

process of securing data and inf. within cyber space → cyber security.

Various types

- → Phishing / scams — Internet fraud
- → Cyber bullying → sharing harmful content — Social Media fraud
- → Cyber stalking — Online recruitment
- → S/w piracy — Ransomware attack
- → cyber extortion — Identity theft

websites, military org.

→ Web hijacking
→ Pornography / child pornography
→ Salami Attacks
→ Virus Attacks
→ DOS Attacks
→ Email Bombing
→ Internet time theft
→ Theft of information electronically
→ Forgary
→ Physically damage the comp. sys.
→ Sale of illegal articles
→ Online gambling (Hawala)
→ Email spoofing
→ Cyber defamation
→ Data Diddling
→ Theft of comp. System
→ Cyber terrorism

How to prevent cybercrime

7 TIPS

1) Use up-to-date security s/w s.a. Antivirus & Firewall.

2) Implement security setting in your browsers.

3) Use proper authentication i.e. set password as strong as possible.

→ Do not send or share your sensitive inf. online or on social media.

→ Educate yourself and your collegues about cyber crime.

→ Educate your children about risk of internet & keep watching their activities.

→ Always be ready to complain in police wherever you become victim.

Ways of getting your password or cracked

→ Brute force attack
→ Phising
→ Credential stuffing
→ Password Spraying
→ Malware Installations – keyloggers.
→ Shoulder surfing.

Preventions
→ Strongest password.
→ Use password manager (tool) which saves all your passwords like Dashlan / LastPass.
→ Use account locks. (limits)
→ Change passwords periodically.
→ Do not use your personal inf.
→ Don't share your password

Management Mantra

18%

Security Management Policies

- Authentication
- Authorization
- Identification
- Access Control
- Accounting.

⇒ Threats & Challenges

⇒ Solution