30/8.

Class : 01

COURSE : NETWORK SECURITY (BSSE-512).

Textbook : Network security and cryptography.
Principles and Practice
By William Stallings.

Ref books :
* Computer Networks
By Andrew S Tennaubaum
* Network Security Cisco Press
By Yousuf Bhaiji
* TCP/IP Internetworking
By Jeff Doyell

Course Outline :
* Introduction
* Classical Encryption
* Symmetric Encryption Algo - DES
- AES

* Asymmetric Encryption Algo - RSA
* ~~Digital~~ message authentication - MD5
* Digital Signature
* IP Sec
* SSL
* PGP
* Firewall
* VLANs
* Attacks Mitigation Techniques
* Best Practices in Network Design
* Wireless N/W Security Issues ....

Data Communication:-

The error free transmission of data bits from one end to another is called data communication.

Computer Network: The interconnection of autonomous devices.

Topology: Physical arrangement / Structure of networks.

* LAN topology usually use hybrid topology.

~~technology~~

Internet: public network.

Intranet: private network.

Fishing attack: Somebody wants to access credential data.

Circuit switching: Oldest switching technology used for voice travel / analog transmission

Circuit switching has 3 steps. (dedicated path b/w source and end)

1) Circuit Establishment
2) Data transfer
3) Call disconnect / Circuit disconnect

* Data is transmitted in a single block in circuit switching.

* It is not suitable for data communication for eg 2000 bit ka data tha 1999 sahi chale gye but 1 bit ki waja se wapis 2000 bit bhejny parengy. That is why data communication

is not suitable in circuit switching.

* Packet switching: No need of call center. (The packet which has error only that will be re-transmitted). It is a digital base technology. (Packet switching is of two types.

1) Data-gram Packet switching (for digital)
2) Virtual Circuit packet switching. (for anal
   - call setup
   - data transfer
   - call disconnect

* OSI model is based on packet switching
* Presentation Layer has 3 main tasks:
  1) Compression / Decompression
  2) Encryption / Decryption
  3) Syntax conversion.
* Each layer adds a header to the data called PDU.
* Session layer:
  - Error recovery

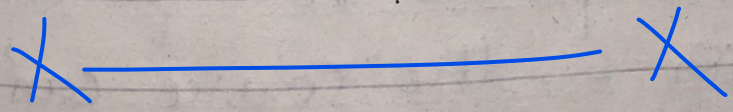
SSL protocol is used in Session layer.

Transport layer: TCP, UDP, IP, ICMP
↳ Internet control Message Protocol.

* IP is a totally unreliable protocol. TCP, ICMP provides reliability to IP.
* Data link Link Layer:
  ↳ Flow control
  ↳ Synchronization
  ↳ Data control

✗ Top 5 layer in OSI - Protocol dependent layers.

✓ Physical layer is related with hardware MAC address.



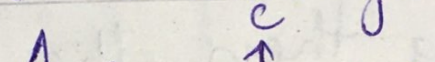
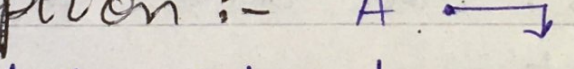
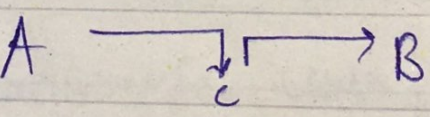
Class : 02

7/9 NETWORK SECURITY.

* Computer Security: The protection afforded to an automated info system in order to attain the appropriate objectives by preserving the integrity, confidentiality and availability of any info systems assests.
* System Requirements:
* Secrecy / Confidentiality
* Integrity → Only authorized people have the right to access administrative data / manipulate data.
* Availability → Any data / service / resource should be a variable with any specific or authorize person.
* Authenticity → Authentic user, data dono ki hoti hai. Data ko authenticate karna k wahin wo manipulate toe nahi hua.
* Non-Repudiation → the source can't deny. If your system as such that the

source can't deny the existence of data.

* We create an access policy to work with all these requirements.
* If the first three stated requirements are fulfilling then the system is secured.
* Policy: Anything whose technical solution is available in the market then we can include it in our policy.
* External Attacks: that does not exist in our network.
* Internal Attacks: (intrusion detection) that exists in our network. Difficult to detect.
* (firewall will not block internal attacks).
* Phishing Attack: → Attack on credential data. → (Replicate any website that user enters).

* Scripting virus: (file.exe)
* Keyloader virus: (keyboard hack)
* Threats/Attack: It is any kind of danger which could affect the security that may lead to potential loss or damage.
* Interception:  A se data deliver hua B ko but beech mien ksi intruder ne ap k data ko intercept ki'a hai. Here confidentiality is violated.
* Interruption :-  (A se B tak data transfer horaha tha but beech mien interrupt hogaya. Here availability is violated.)
* Modification:  (During the transfer of data from A to B, C modified the data or phr B ko bhej dia. Here integrity is violated.

* Fabrication: A • ⟶ C ⟶ • B

Kisi ne apki jagah data transfer kardia B ko.

Here authenticity is violated.

* Passive Attacks: (Interception)

Passive attacks mien attacker ka target ye hai k wo 2 parties k darmiyan jo communication horahi hai us ko access karle.

- To break the confidentiality of data.
- Easy to generate but detection is difficult.

* Active Attacks:

Attacker tries to access communication data.

i) To access confidential data

ii) Manipulate the data.

- Difficult to generate than passive attack but easy to detect.

→ Interruption → Modification → fabrication

We prefer to take preventive measures rather than to detect the attacks.