THADOMAL SHAHANI TSEC ENGINEERING COLLEGE
Om Shete
TE C32
2103163

Assignment No : 1

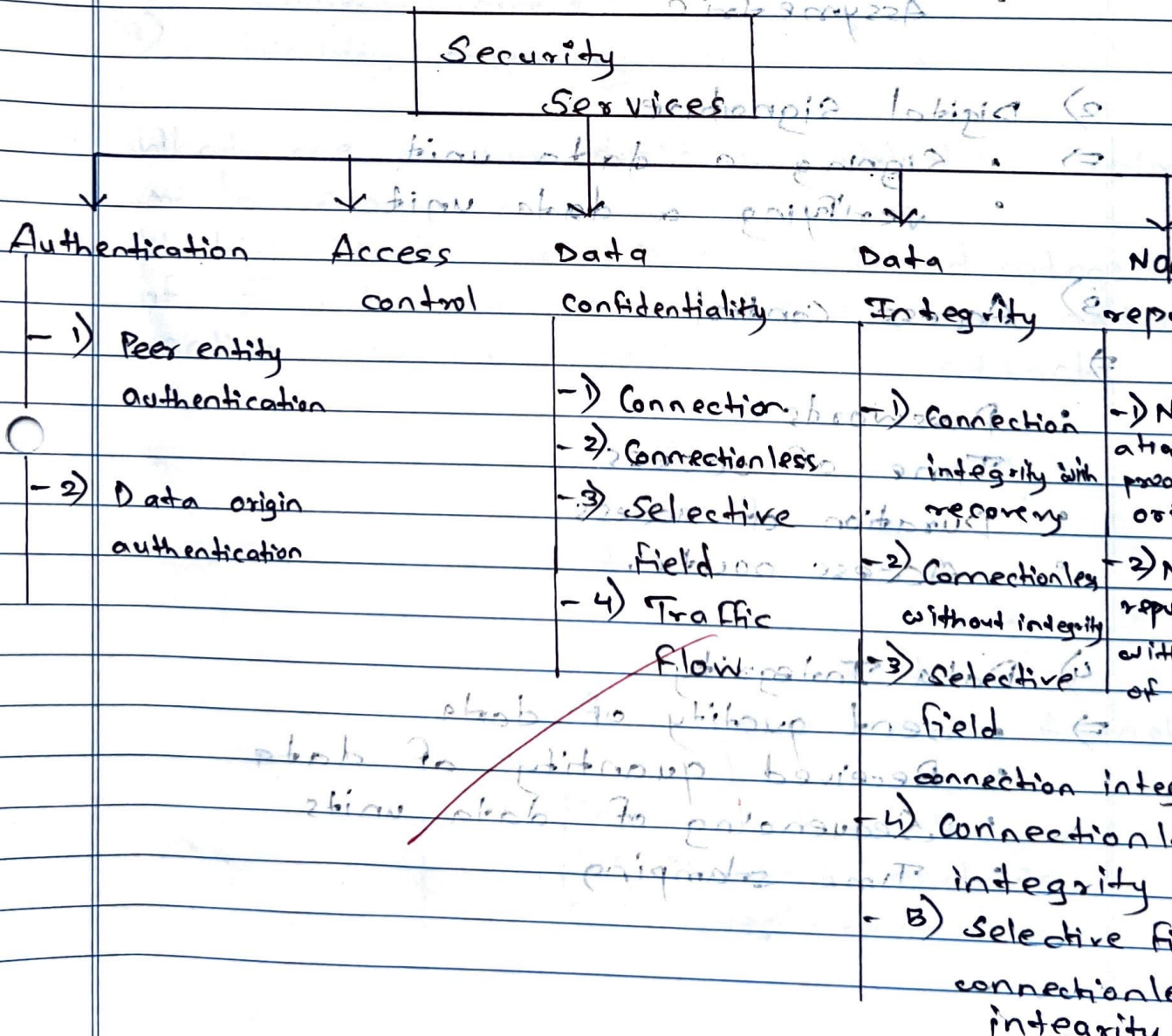
Q.1 Explain different services and mechanisms of security.

⇒

- **Security services**

⇒ Security services are safegaurd controls recommended to be placed at their various OSI layers.

- The various security services are listed as shown in below figure :-



THADOMAL SH
TSEC
ENGINEERING COLLEGE

Security Mechanism

⇒ Security mechanisms are various techniques recommended to provide security services at the various OSI layers.

- The various security mechanisms that can be applied are as following:

1) Encipherment

⇒
- Symmetric
- Assymetric

2) Digital Signature

⇒
- Signing a data unit
- verifying a data unit

3) Access Control

⇒
- Passwords
- Time of access
- Duration of access
- Access route

4) Data Integrity

⇒
- Sent quality of data
- Received quantity of data
- Sequencing of data units
- Time stamping

5) Authentication
⇒ i) Handshaking
ii) Cryptographic techniques
6) Traffic padding
7) Routing control
8) Notarization
9) Pervasive security
10) Security labels
11) Event detection
12) Security audit
13) Security recovery

Q.2 What are various types of attacks? Explain with example.

⇒ At high level, there are two broad categories of security attacks carried over the network- active attacks and passive attacks

Types of Attacks

- 1) Active Attacks
  - a) Replay Attack
  - b) DOS Attack
  - c) Fabrication Attack
- 2) Passive Attacks
  - a) Traffic Analysis
  - b) Eavesdropping

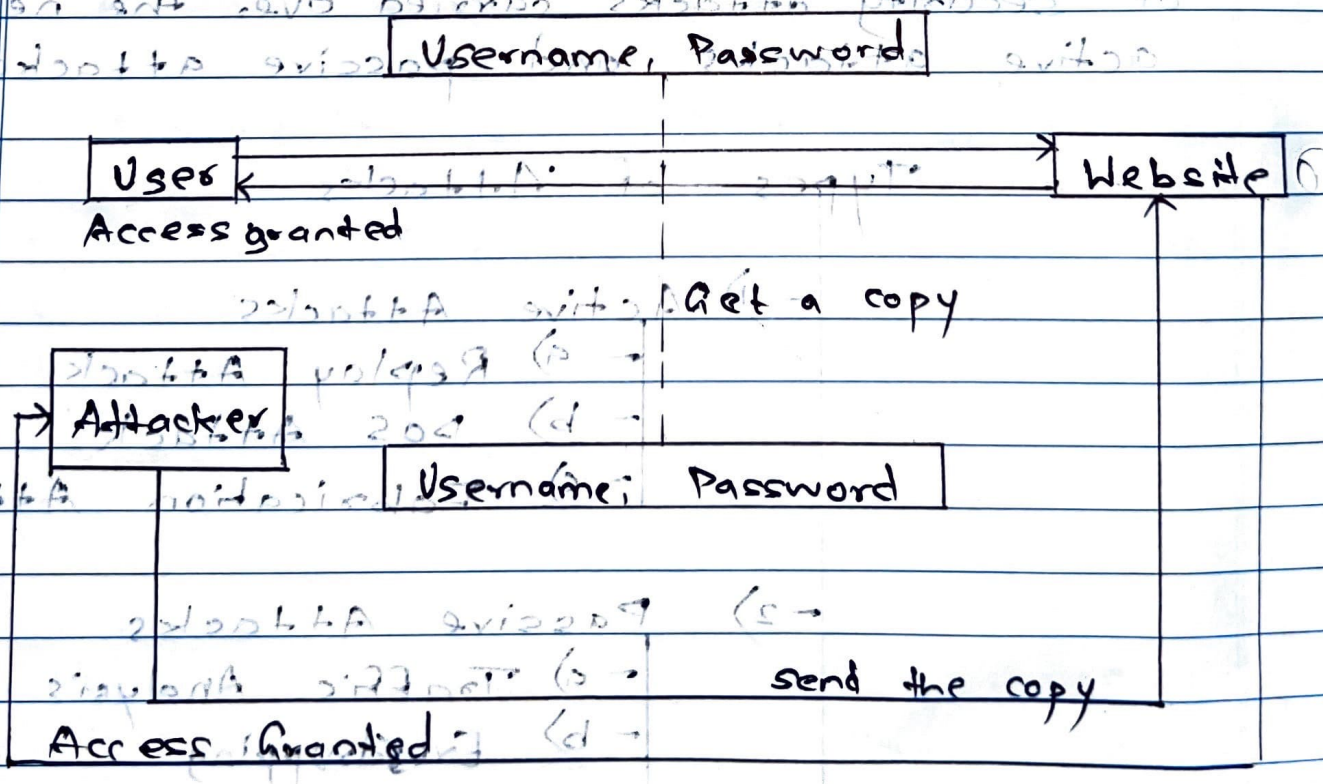
1) **Active Attacks**

⇒ An active attack is defined as an attack where the attacker actively participates in the communication or the attack mechanism and disrupts the system by sending several manipulated inputs.

a) **Replay Attack**

⇒ This is like a replaying a song. The attacker captures the real and specific communication packets, stores them with herself and then sends it at a later point in time as though she is sending the information for the first time like an authentic information.

For legal



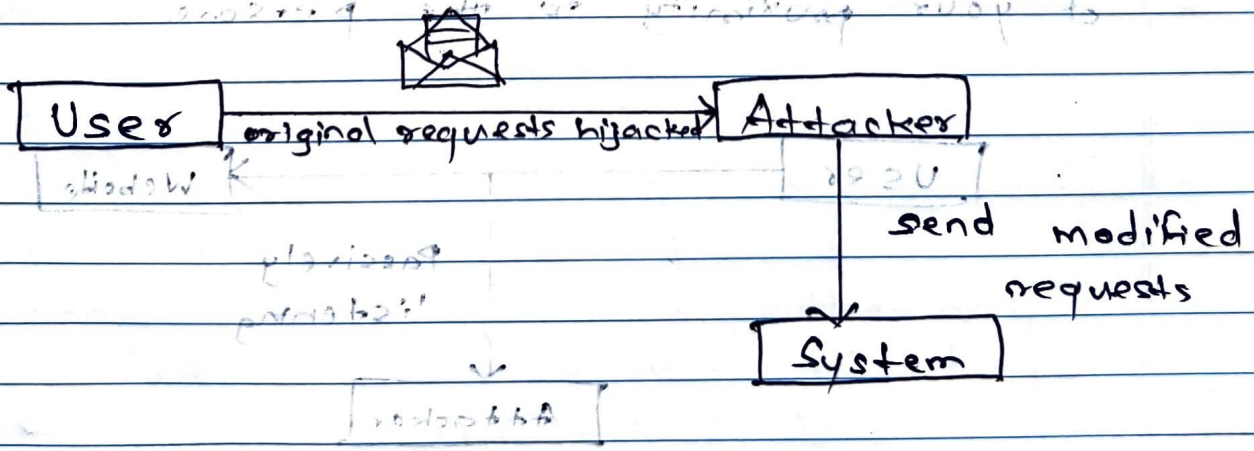
b) Denial of Service (DoS) Attack

⇒ DoS or its variation Distributed DoS refers to a category of attacks that can be aimed at various layers of network, operating system, application or other parts of information systems.

- For e.g., An application might be capable of processing a maximum of 100 requests per second. Attackers would typically send over ≥ 1000 requests per second such that the application fails to cope up with it and crashes.

c) Fabrication Attacks

⇒ Fabrication attack is again a broad category of active attacks where the attacker deliberately modifies messages, parameters, properties, etc. of information system components and try to alter the behaviour of the system often by passing security controls.



2) Passive Attacks

⇒ A passive attack is defined as an attack where the attacker does not alter the behaviour of the information system and silently performs her malicious activities.

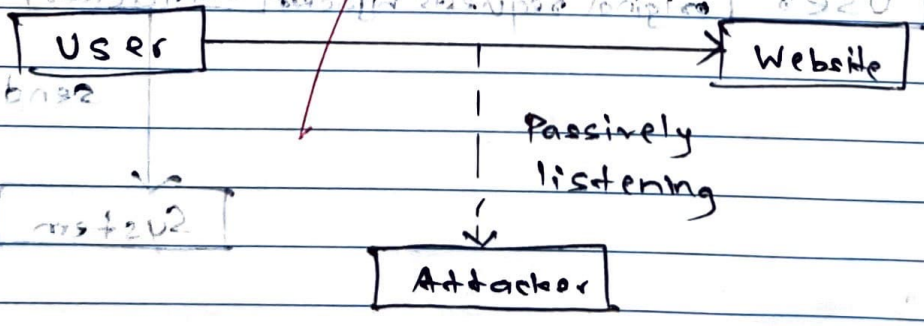
a) Traffic Analysis

⇒ In traffic analysis the network traffic and its pattern are watched out over a period of time to infer important information and guess possible activities.

- For e.g.,
Long communication: It can denote some emergency.

b) Eavesdropping

⇒ Eavesdropping is very similar to overhearing someone's telephonic conversation taking advantage of your proximity to the persons.



Q.3 List few latest viruses on net and explain.

⇒ Latest viruses on net

⇒
1) Malware
2) Ransomware
3) Trojans
4) AoBrut
5) Jokerro

1) Malware

⇒ Malware is a broad term that includes more than computer viruses.
- Worms, Trojans, adware and even ransomware may all be considered malware.
- This is any computer code intentionally created to do damage to computer systems, gain unauthorized access to computers, or to steal information.

2) Ransomware

⇒ Ransomware disables access to computer files by encrypting data.
- Demands for payment or other requests must be met before the offending software will be unlocked to reinstate access to servers or business files.

3) Trojans

⇒ Trojans typically require the receiptant to take some form of action, such as running a program or accessing a malicious website through a link passed by email.

- A common use of a Trojan attack is first to notify a computer user a virus has infected them.

4) CoBrut

⇒ CoBrut is a virus that is one of the most recent viruses to be unleashed by hackers. It is not terribly sophisticated in its technology but can wreak havoc just the same.

5) Jokeroo

⇒ Jokeroo is a serious piece of malware in the form of ransomware that is offered on underground hacking sites for proliferation by other cyberthieves.

- It can be distributed through social media sites, including Twitter and others.