COMPUTER SECURITY THREATS

- Computer Security Concepts,
- Threats,
- Attacks,
- Assets,
- Intruders

COMPUTER SECURITY

Computer security means protect our computing system

MAIN ASPECTS ARE:

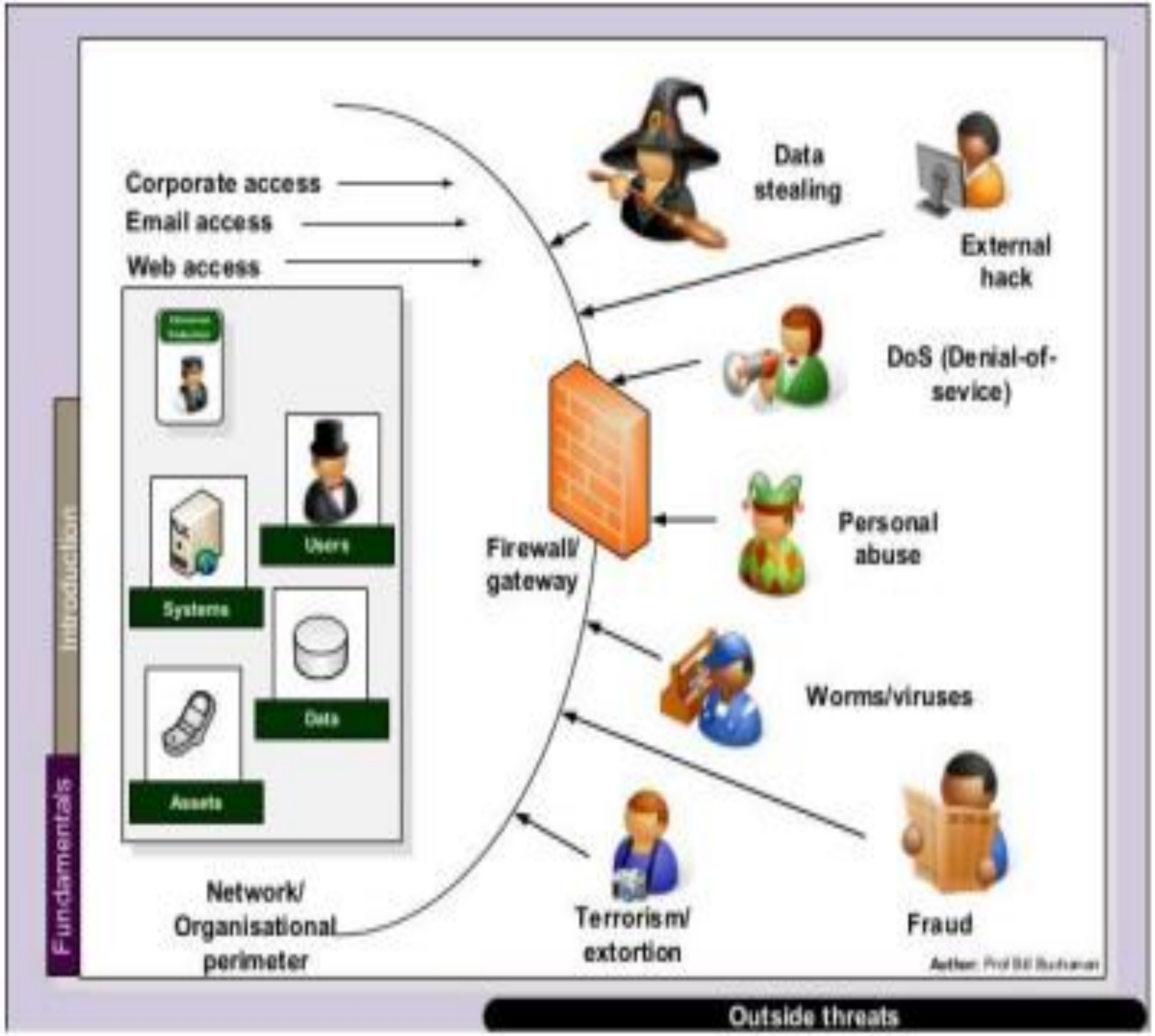
- Prevention:- Prevent your assets from being damaged
- Detection :- Detect when assets has been damage
- Reaction:- Recover your assets

- Computer Security: - Ensuring the data stored in a computer cannot be read or compromised by an individual's without authorization.

- Most computer security measures involve data encryption and passwords.

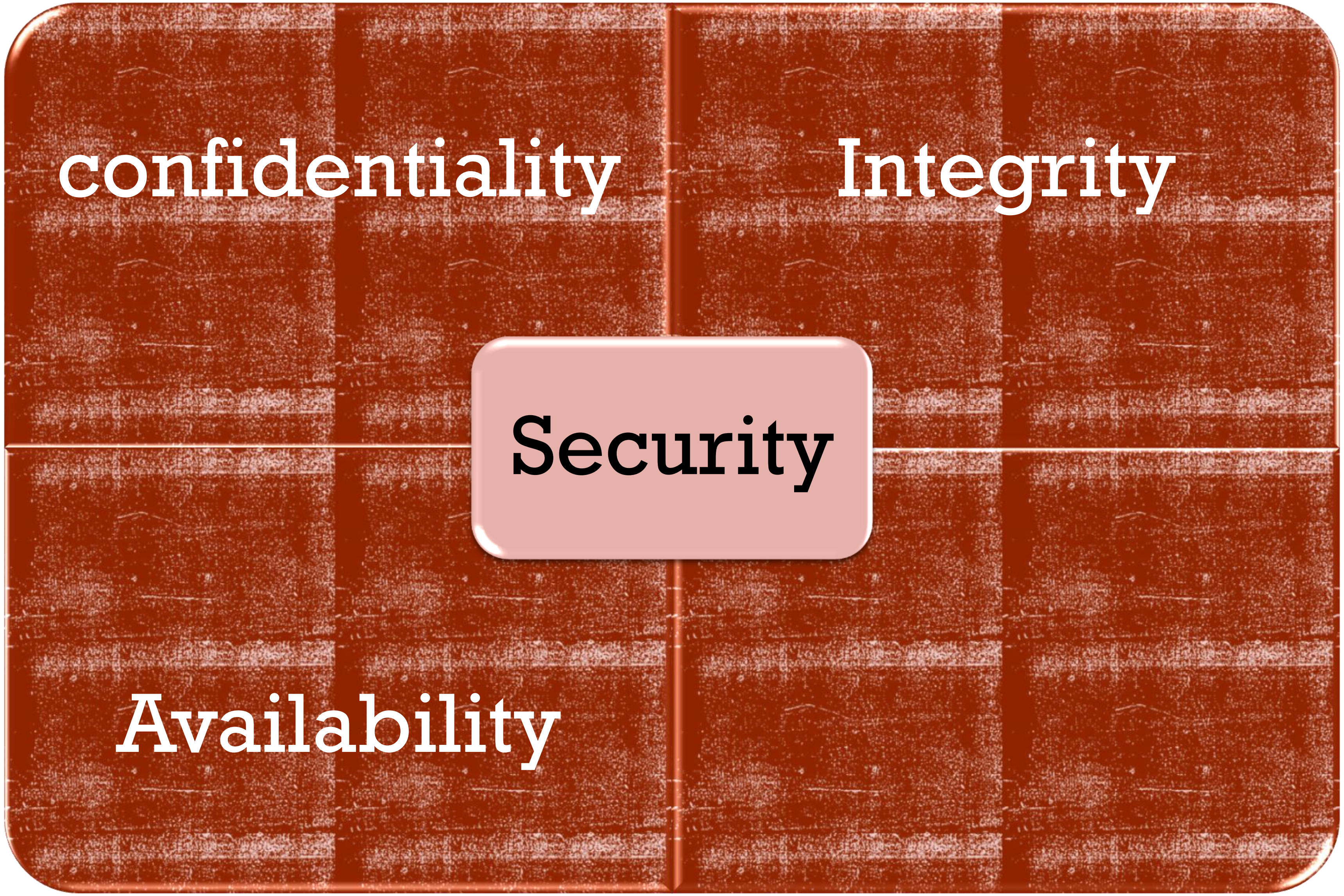
COMPUTER SECURITY

- The purpose of computer security is to device ways to prevent the weaknesses from being.



THREE GOALS IN COMPUTING SECURITY

Three goals of computer security are 1. Confidentiality 2. Integrity 3. Availability



confidentiality

Integrity

Security

Availability

WHY IS COMPUTER SECURITY IMPORTANT?

- Computer security is important, primarily to keep your information protected. It's also important for your computer's overall health, helping to prevent viruses and malware and allowing programs to run more smoothly. Security is needed due to following reason.
- **1.Privacy**:- It defines the right of individuals to hold information about themselves in secret, free from the knowledge of others
- 2. **Accuracy**: - Most of damages of data is caused by errors and omissions. An organization always needs accurate data for transaction processing, providing better service and making
- 3. **Threats** by dishonest employ
- 4. **Computer** Crimes:- When computer resources can be misused for unauthorized or illegal function
- 5. **Threats for fire and Natural Disasters:-** fire and natural disasters like floods, storms, lightening etc

THREATS

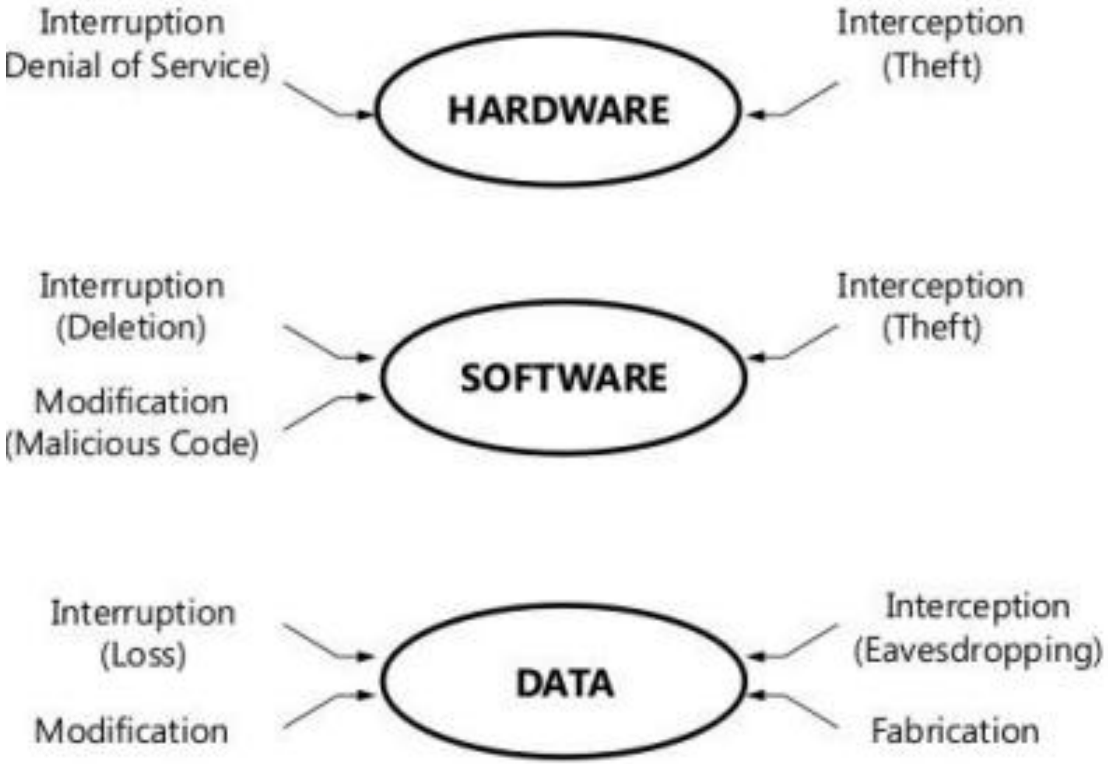
- A threat to a computing system is a set of circumstances that has the potential to cause loss or harm.
- A threat can be an **object or person or other entity** that represents a constant danger to an asset.
- There are many threats to a computer system, including **human-initiated and computer- initiated ones.**
- A threat is blocked by control of vulnerability (Weakness of the system).

WE CAN VIEW ANY THREAT AS BEING ONE OF FOUR

- •An interception means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system.

- In an interruption is an asset of the system becomes lost, unavailable, or unusable.
- If an unauthorized party not only accesses but tampers with an asset, is called as a modification.
- An unauthorized party might create a fabrication of counterfeit objects on a computing system.
- The intruder may insert spurious transactions to a network communication system or add records to an existing database.

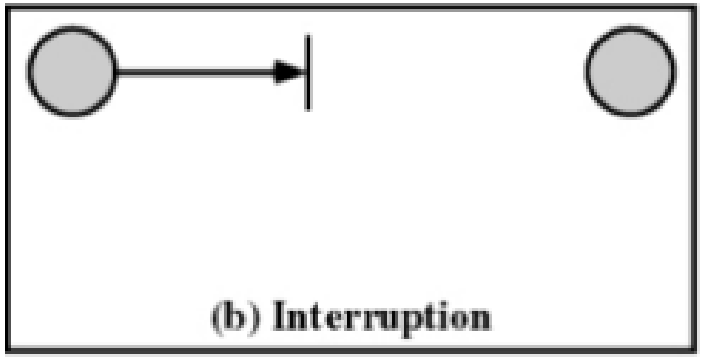
How Threats Affect Computer Systems



KINDS OF THREATS

INTERRUPTION -

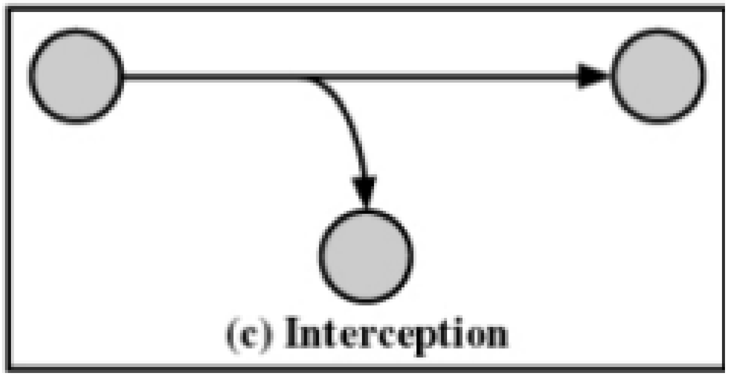
- An asset of the system is destroyed of becomes unavailable or unusable
- – Attack on availability
- - Destruction of hardware
- – Cutting of a communication line
- – Disabling the file management system



(b) Interruption

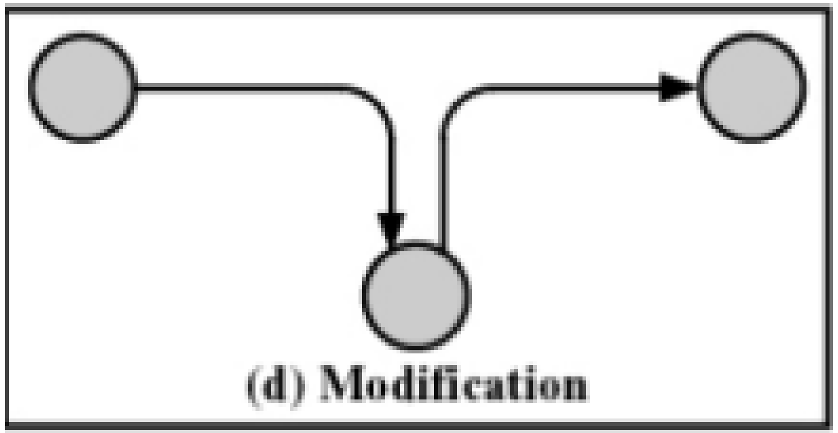
INTERCEPTION

- -An unauthorized party gains access to an asset
- – Attack on confidentiality
- – Wiretapping to capture data in a network
- – Illicit copying of files or programs



- There is a middleman or process or machine trying to intercept

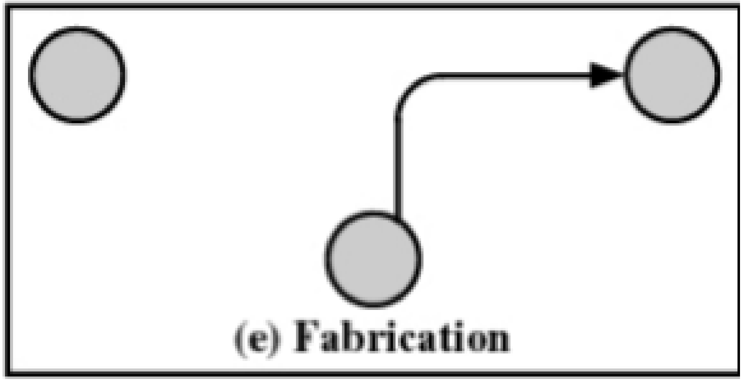
MODIFICATION



- An unauthorized party not only gains access but tampers with an asset
- – Attack on integrity
- – Changing values in a data file
- – Altering a program so that it performs differently
- – Modifying the content of messages being transmitted in a network

- Here middleman changes the data and send to the receiver

FABRICATION


(e) Fabrication

- --An unauthorized party inserts counterfeit objects into the system
- – Attack on authenticity
- – Insertion of spurious messages in a network
- – Addition of records to a file

- Here sender not sends data to the receiver. Middleman fabricate the data

ATTACKS

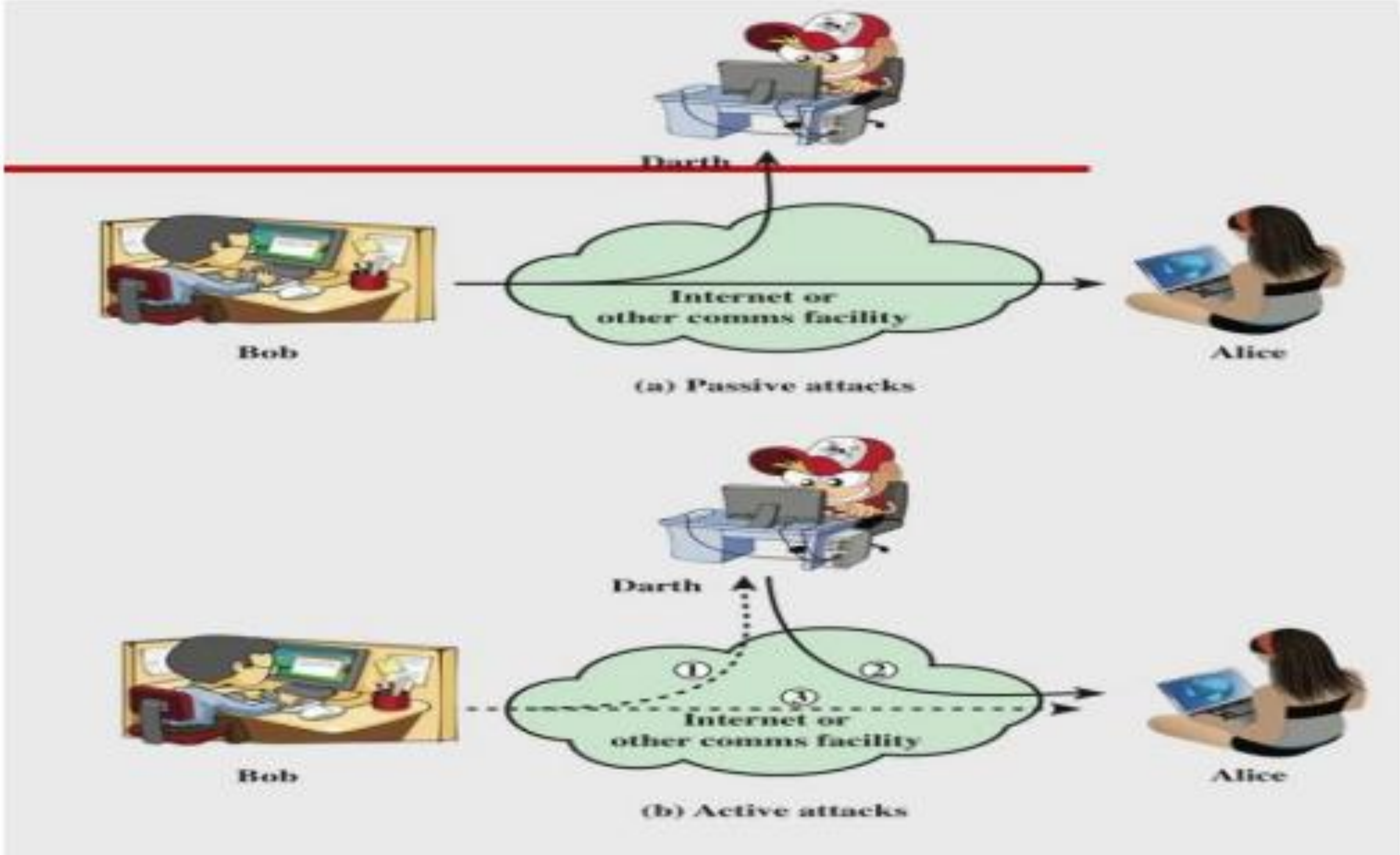
Attack is the process of gaining the access of data by unauthorized user.

It is an Act or attack that exploit vulnerability(Weakness of the system)

WHAT DOES ATTACK MEAN?

- An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations.

- Two types of attacks are.
- 1. Passive attack:-data just accessed by third party, no modification, does not affect system resources
- 2. Active attack:- data will be modified



(a) Passive attacks

(b) Active attacks

Figure 1.1 Security Attacks

PASSIVE ATTACKS:

- -Release of message contents for a telephone conversion, an electronic mail message, and a transferred file are subject to these threats
- – Traffic analysis:- By analyzing the traffic flow between sender and receiver third party access the data

ACTIVE ATTACKS

- Masquerade takes place when one entity pretends to be a different entity
- – Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
- – Modification of messages means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect
- – Denial of service prevents or inhibits the normal use or management of communications facilities
- • Disable network or overload it with messages

INTRUDERS

- Intruders are the attackers who attempt to breach the security of a network. They attack the network in order to get unauthorized access.
- Intruders are of three types, namely, **masquerader, misfeasor and clandestine user**
- **Masquerader:** are outsiders and hence they don't have direct access to the system, their aim is to attack unethically to steal data/ information.

- **Misfeasor :**The category of individuals that are authorized to use the system, but misuse the granted access and privilege.
- **clandestine :**The category of individuals those have supervision/administrative control over the system and misuse the authoritative power