OSI Security Architecture

Erukala
Suresh
Babu

Digitally signed by
Erukala Suresh Babu
DN: cn=Erukala Suresh
Babu, o=NITW, ou=CSE,
email=esbabu@nitw.ac.
in, c=IN
Date: 2019.08.27
06:40:29 +05'30'

Dr. E. Suresh Babu

Assistant Professor

Department of CSE

National Institute of Technology, Warangal

Course : Cryptography and Network Security

Outline

- OSI Security Architecture: Introduction
- Security Goals
- Security Attacks
  - ✓ Taxonomy of Attacks

OSI Security Architecture: Introduction

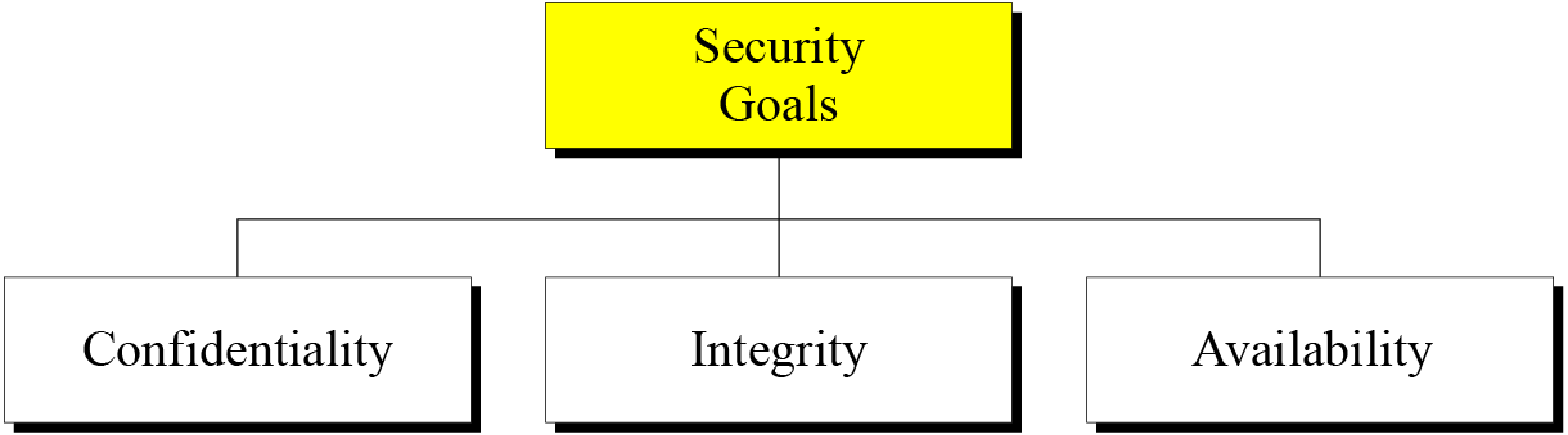
- The Open Systems Interconnection (OSI) security architecture provides a systematic framework for defining
  - ✓ **Security Attacks,**
  - ✓ **Security Mechanisms,**
  - ✓ **Security Services**

- Open Systems Interconnection (OSI) security architecture provides a useful, if abstract, overview of concepts

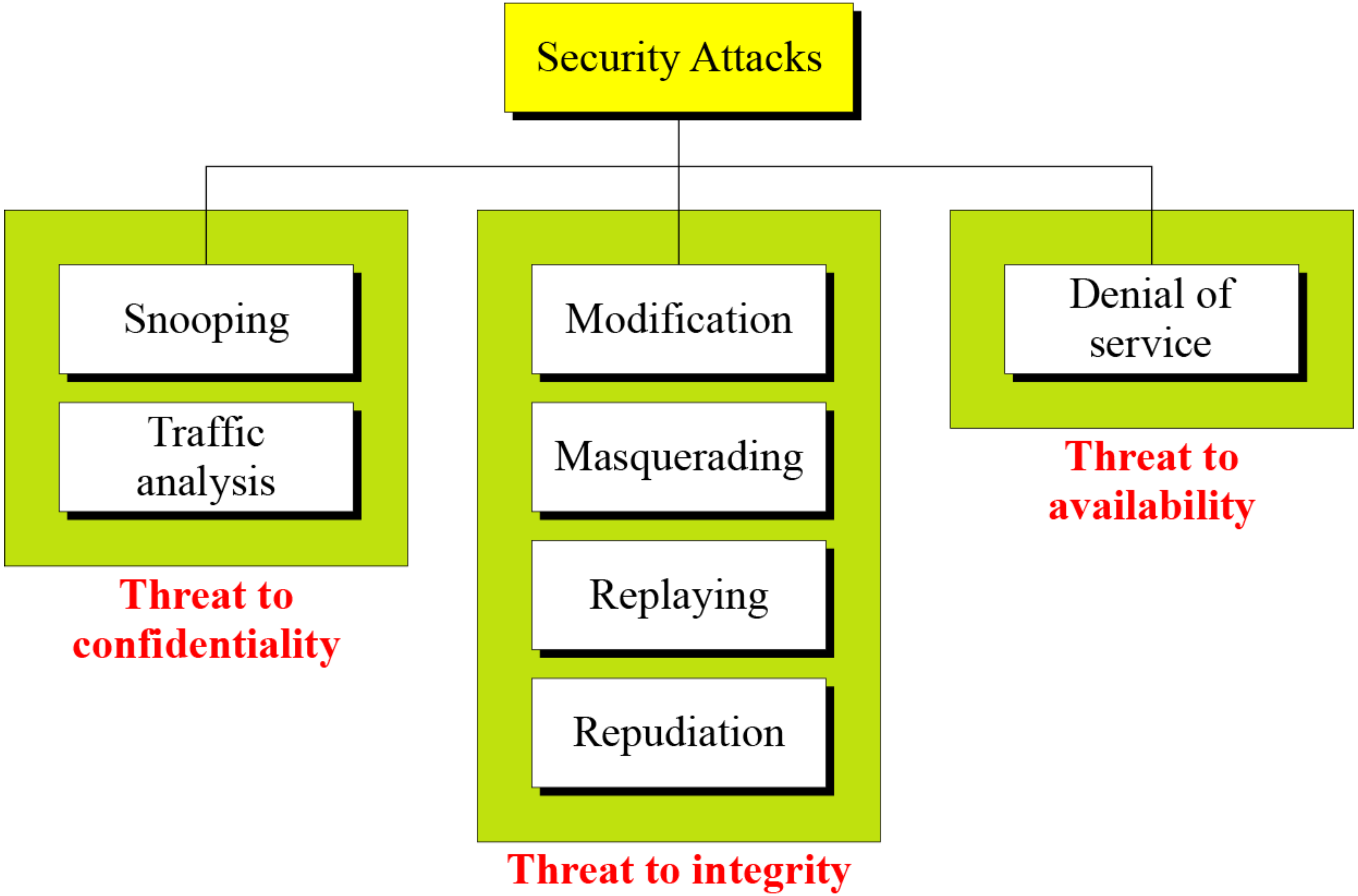
Network/Information Security..

- Network/Information security is all about
  - ✓ How to prevent attacks, or failing that,
  - ✓ How to detect attacks on Network/information-based systems

Taxonomy of Security Goals



Taxonomy of Attacks With Relation To Security Goals



Security Attacks

Snooping

Traffic analysis

Threat to confidentiality

Modification

Masquerading

Replaying

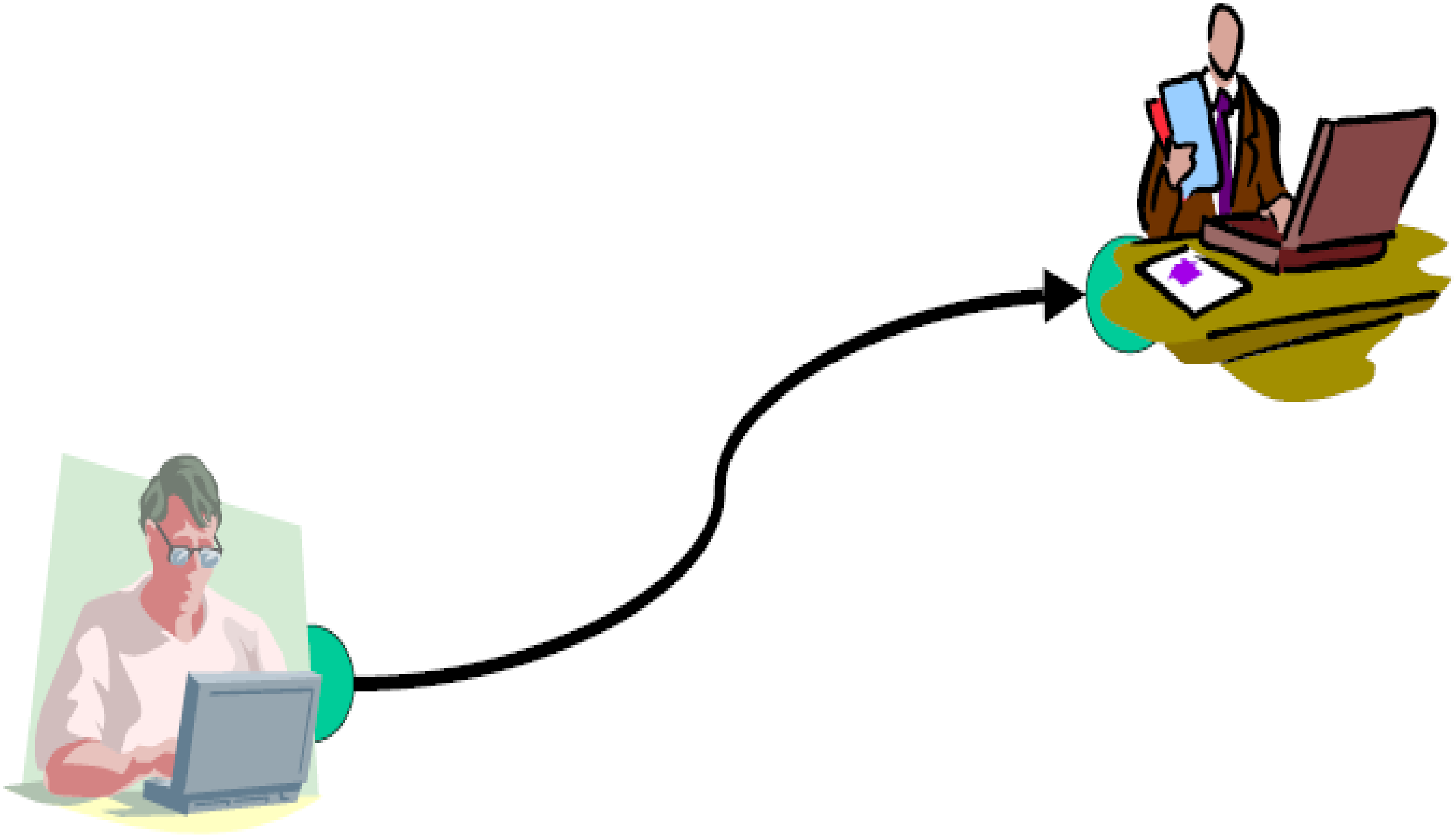
Repudiation

Threat to integrity

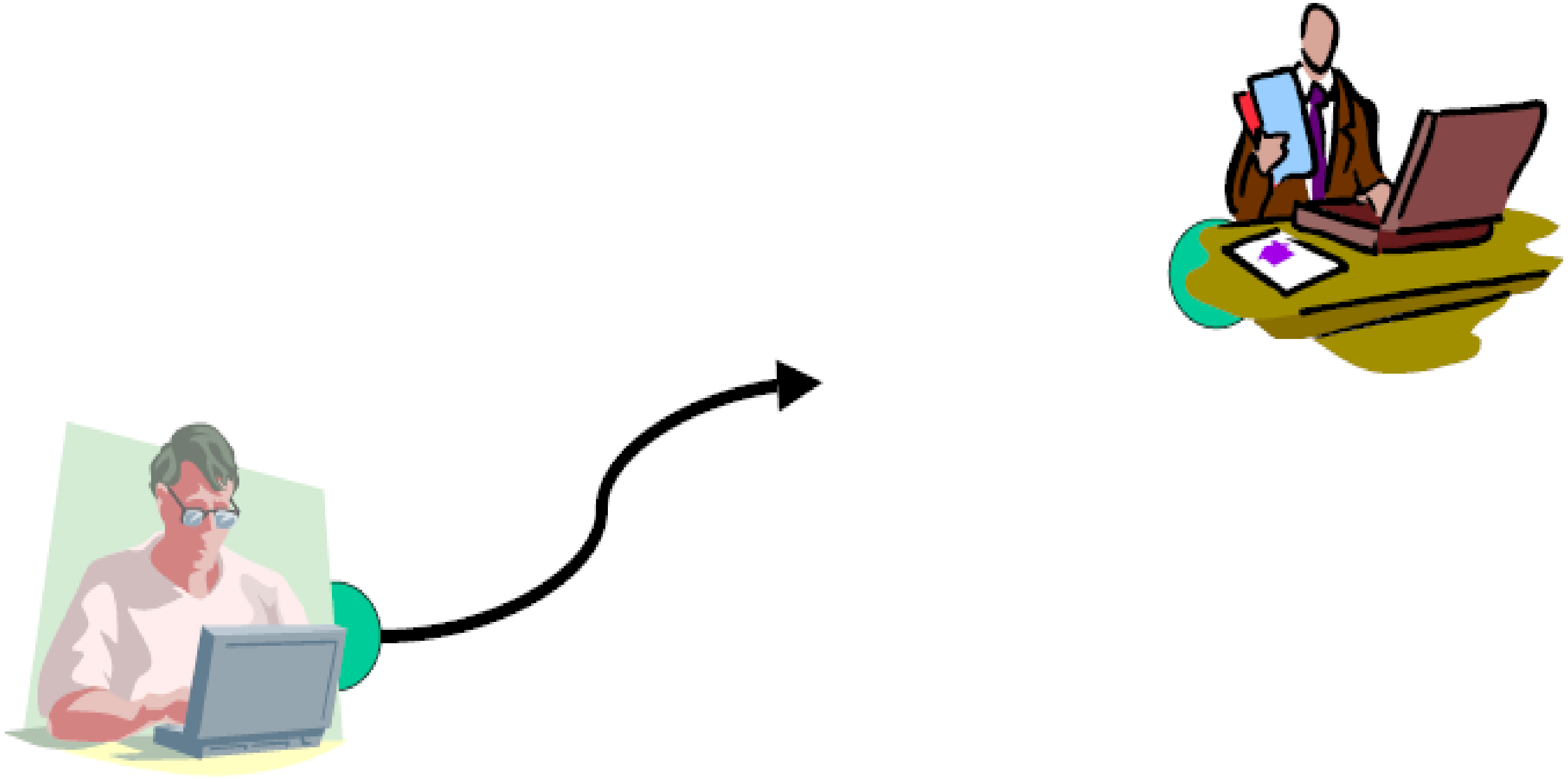
Denial of service

Threat to availability

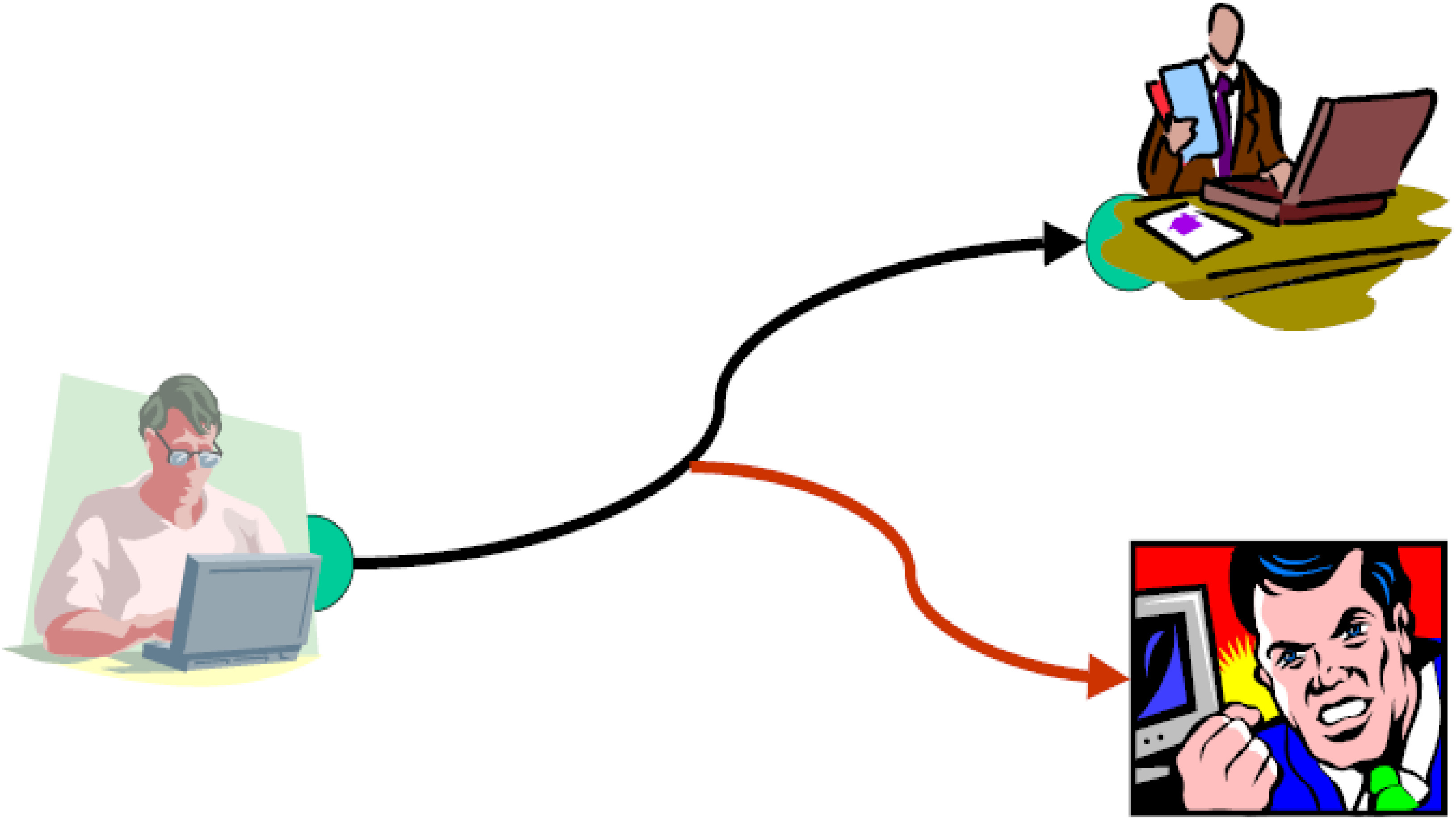
Information Transferring



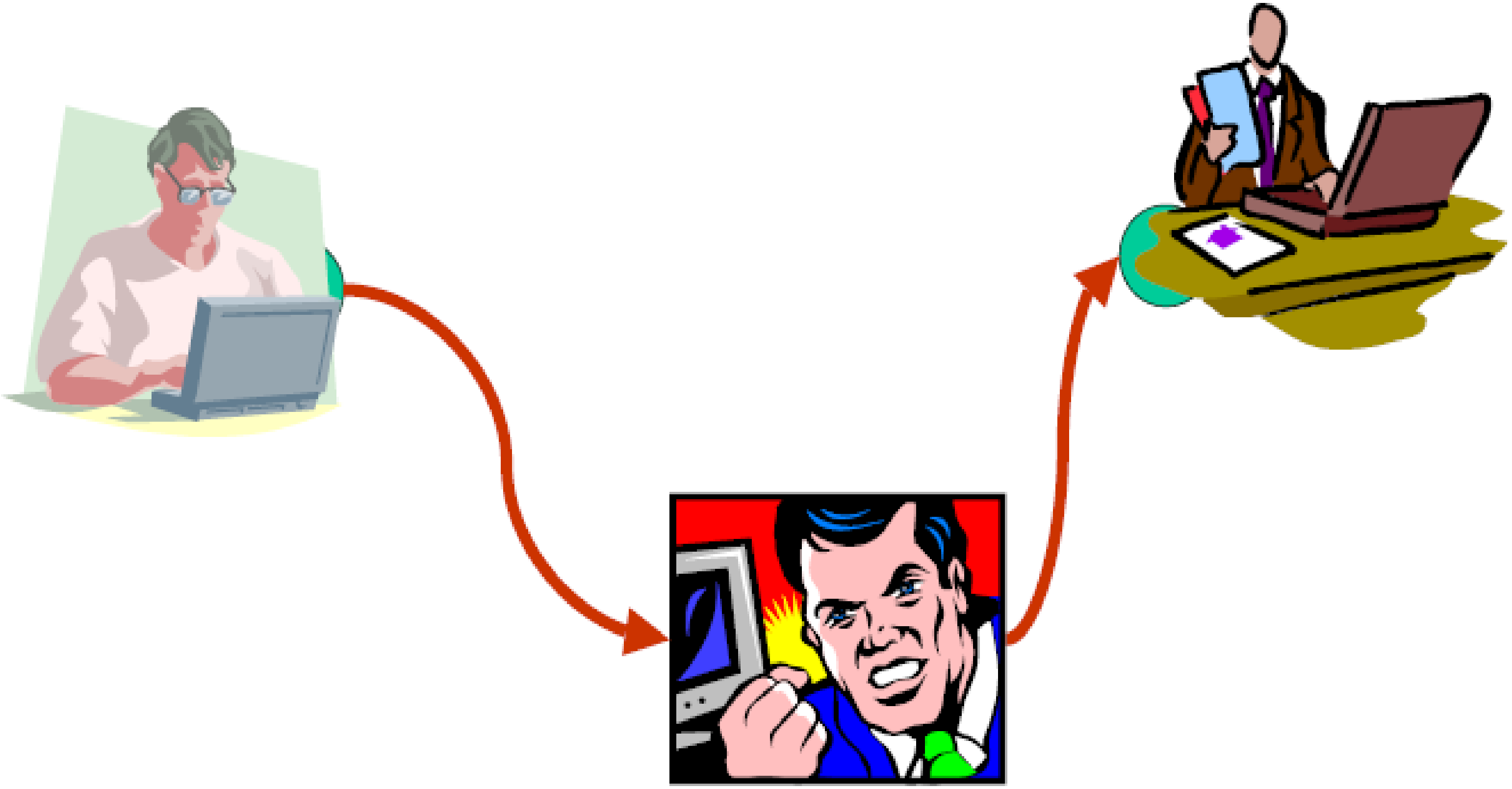
Attack: Interruption



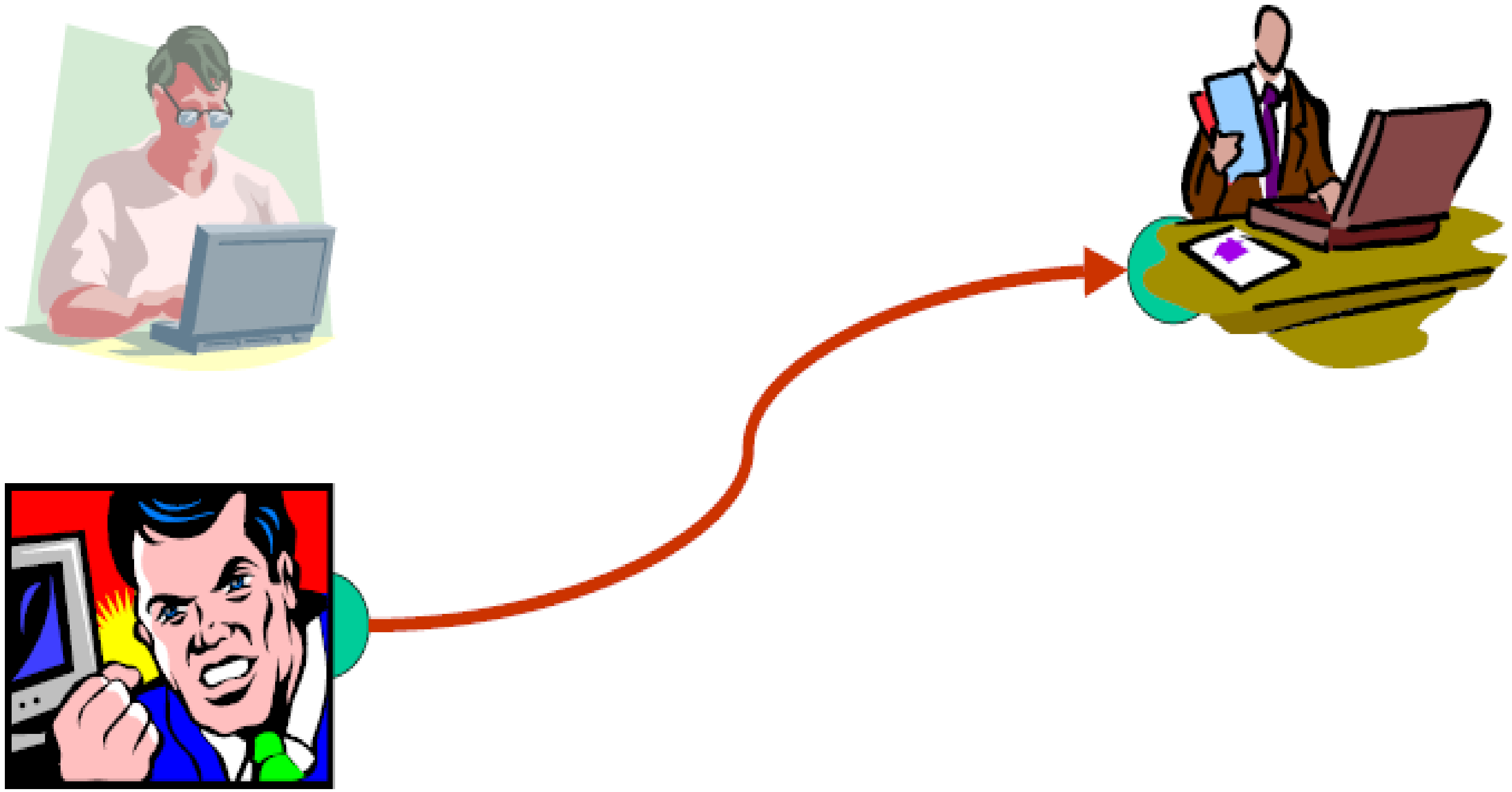
Attack: Interception



Attack: Modification



Attack: Fabrication



Security Attacks

- Security attacks have a wide range of attacks. But will focus of generic types of attacks
  - ✓ **Passive attacks**
  - ✓ **Active attacks**

Passive Attacks

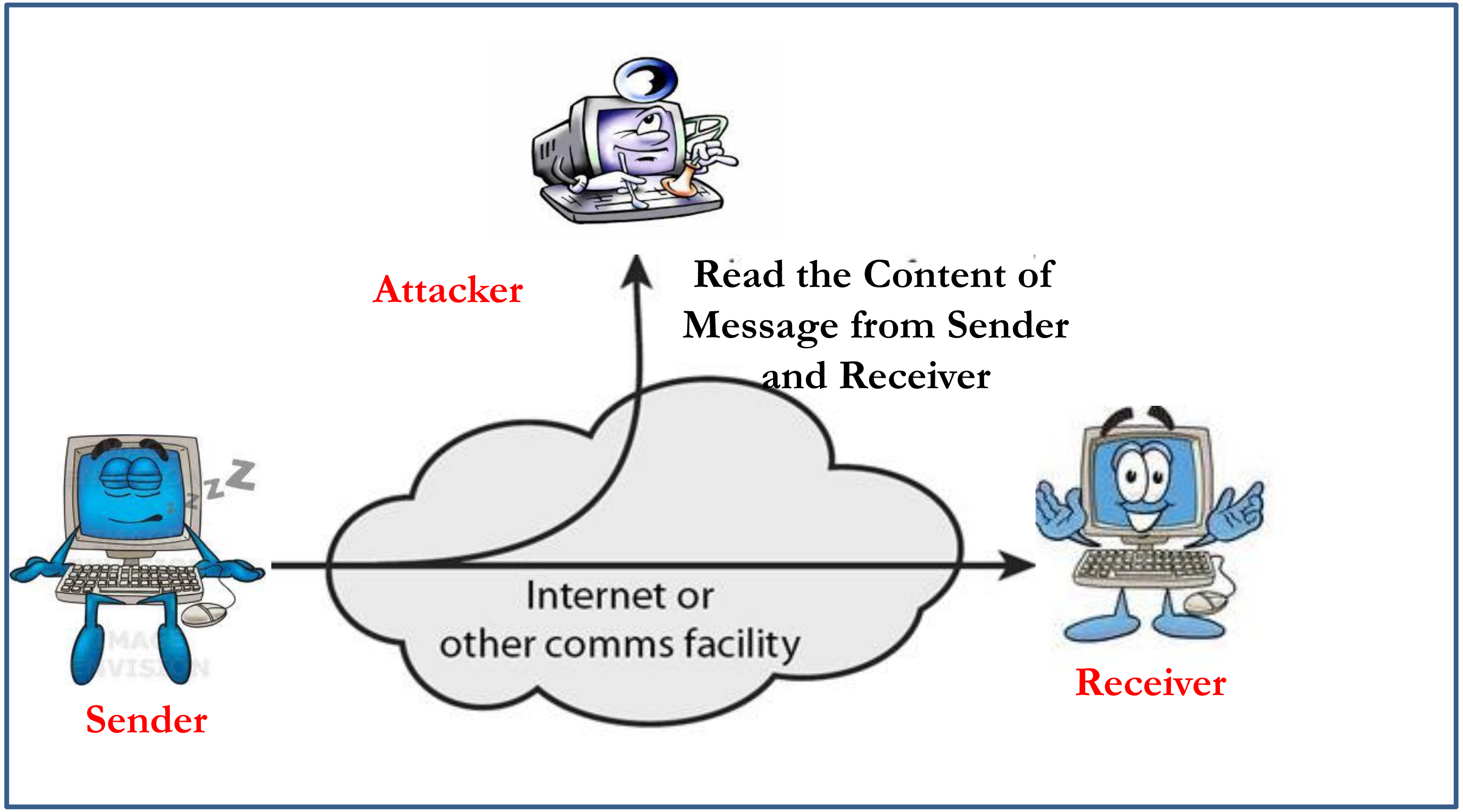
- Passive attacks
  - ✓ Includes unauthorized reading of a message of file and traffic analysis
  - ✓ Attempt to learn or make use of information from the system but does not affect system resources.

Passive Attacks

- Passive attacks threatens Confidentiality
  - ✓ **Obtain message contents (Spoofing)**
  - ✓ **Monitor traffic flows (Traffic Analysis)**

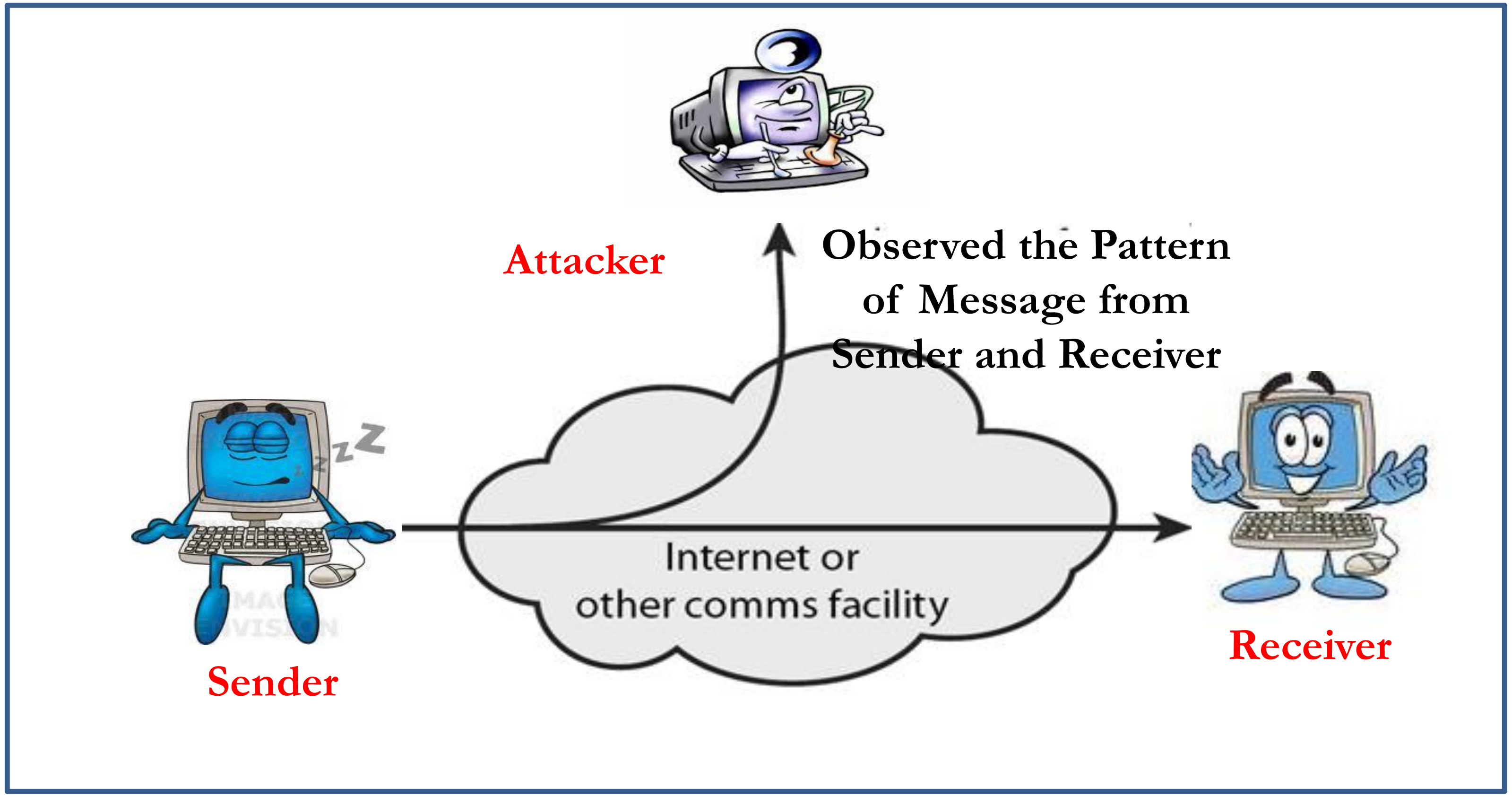
Obtain Message Contents (Spoofing)

- **Snooping** refers to unauthorized access to or interception of data.


Attacker
Read the Content of Message from Sender and Receiver
Internet or other comms facility
Sender
Receiver

Monitor Traffic Flows (Traffic Analysis)

- **Traffic analysis** refers to obtaining some other type of information by monitoring online traffic.


Attacker
Observed the Pattern of Message from Sender and Receiver
Internet or other comms facility
Sender
Receiver

Challenge of Passive Attacks

- Passive Attacks are difficult to **detect** because they do not involve any alteration of the data.

Active Attacks

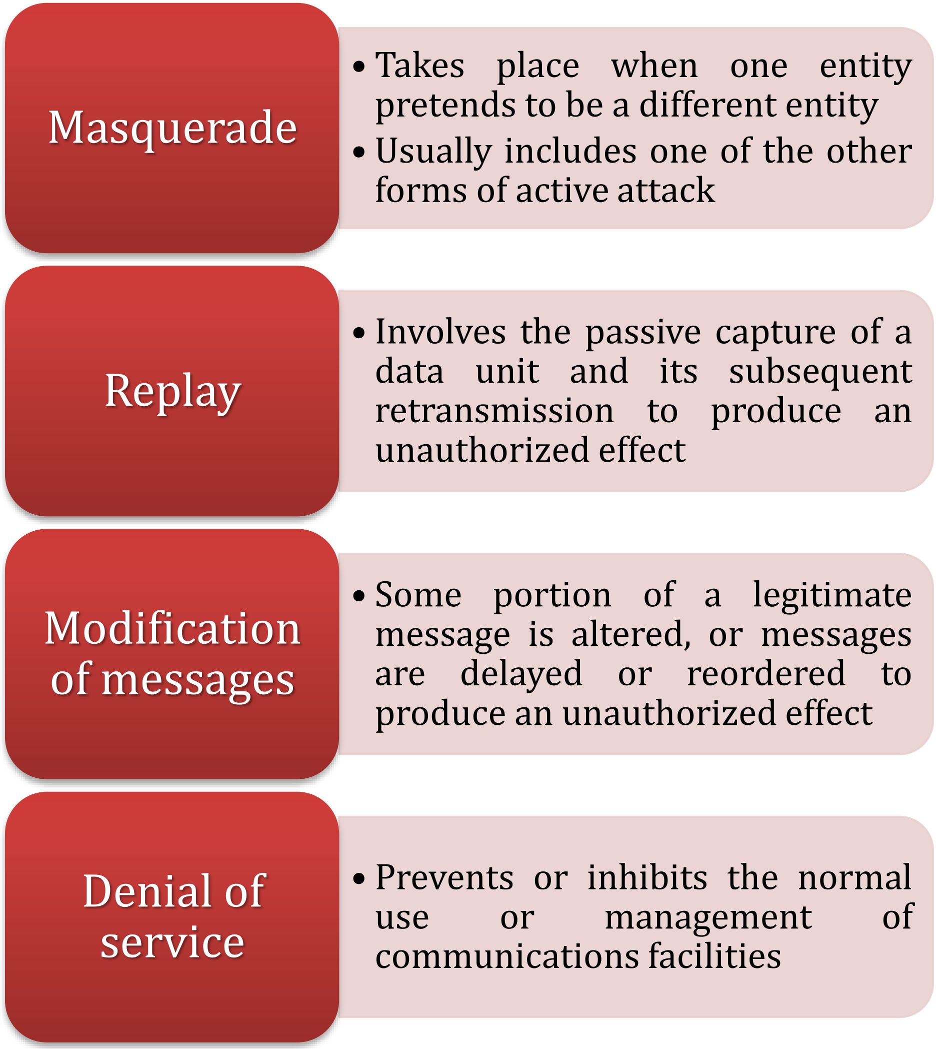
- ❖ **Active attacks**

  - ✓ Include such as modification of messages or files, and denial of service.

  - ✓ Attempt to alter system resources or affect their operation.

Active Attacks

- Active Attacks threatens Integrity
  - ✓ **Modification of Data Stream/Modify messages in transit**
  - ✓ **Masquerade of one entity as some other**
  - ✓ **Replay previous messages**
  - ✓ **Denial of service**



Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

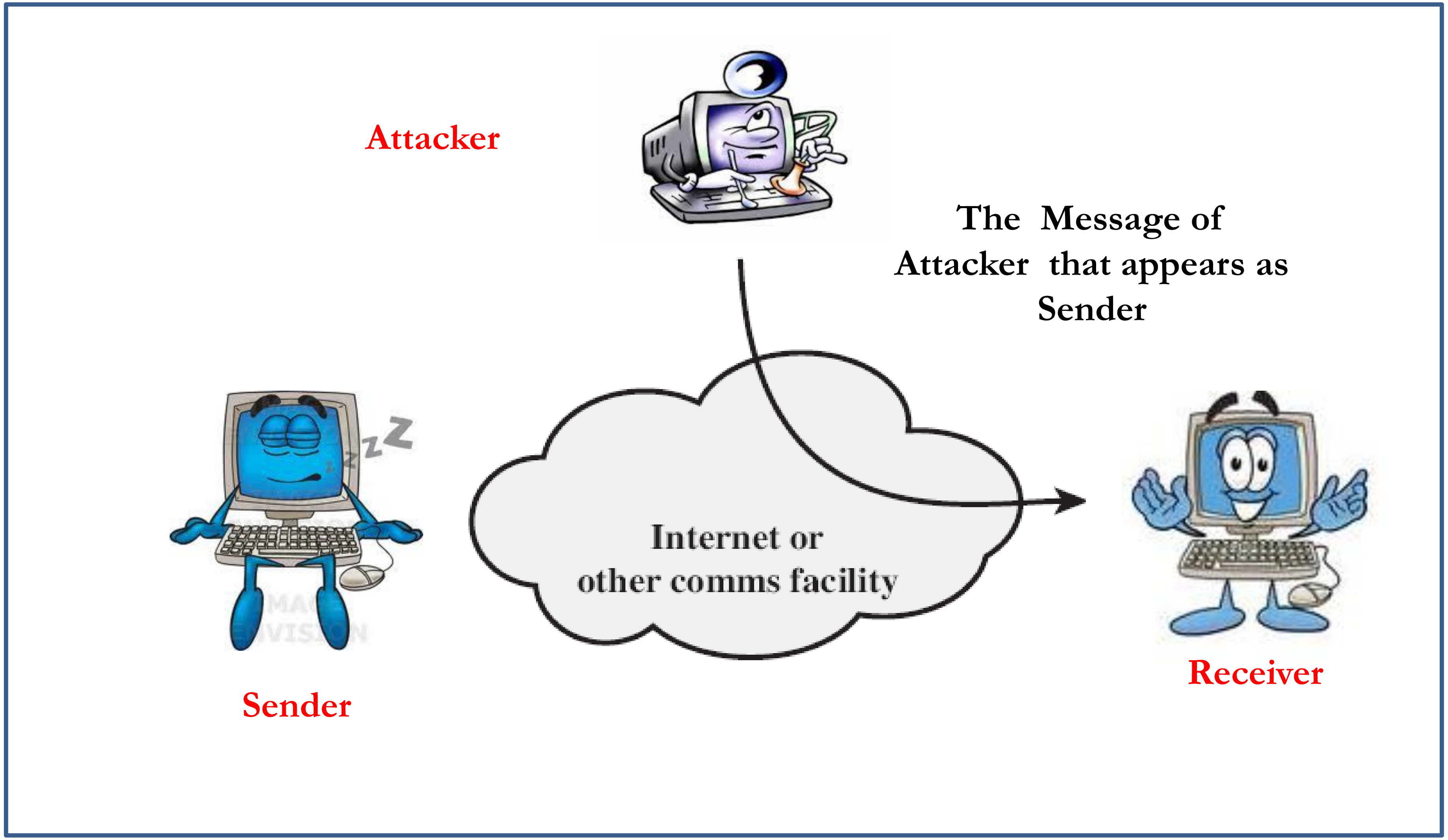
Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

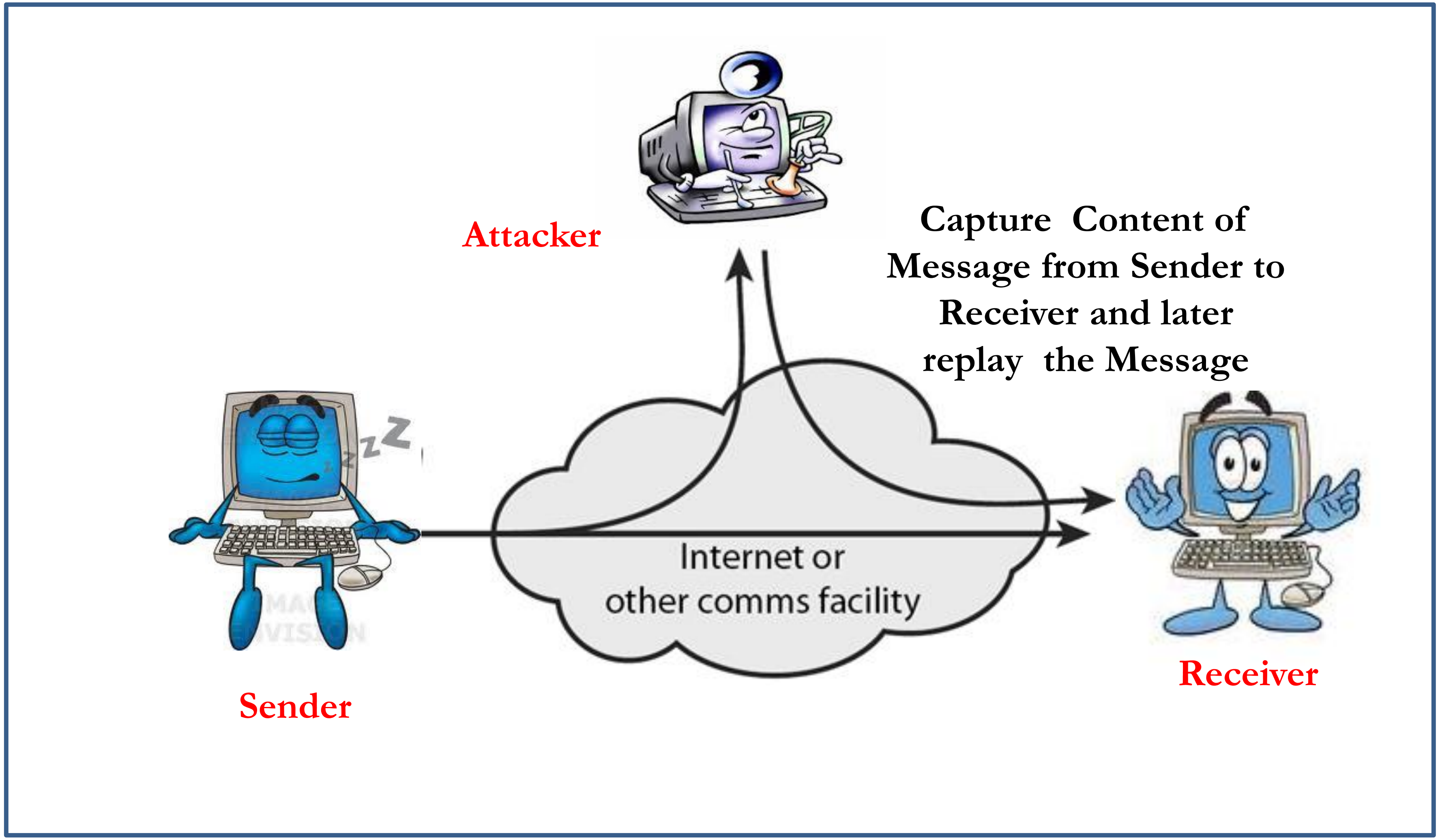
Denial of service

- Prevents or inhibits the normal use or management of communications facilities

Masquerade Attack

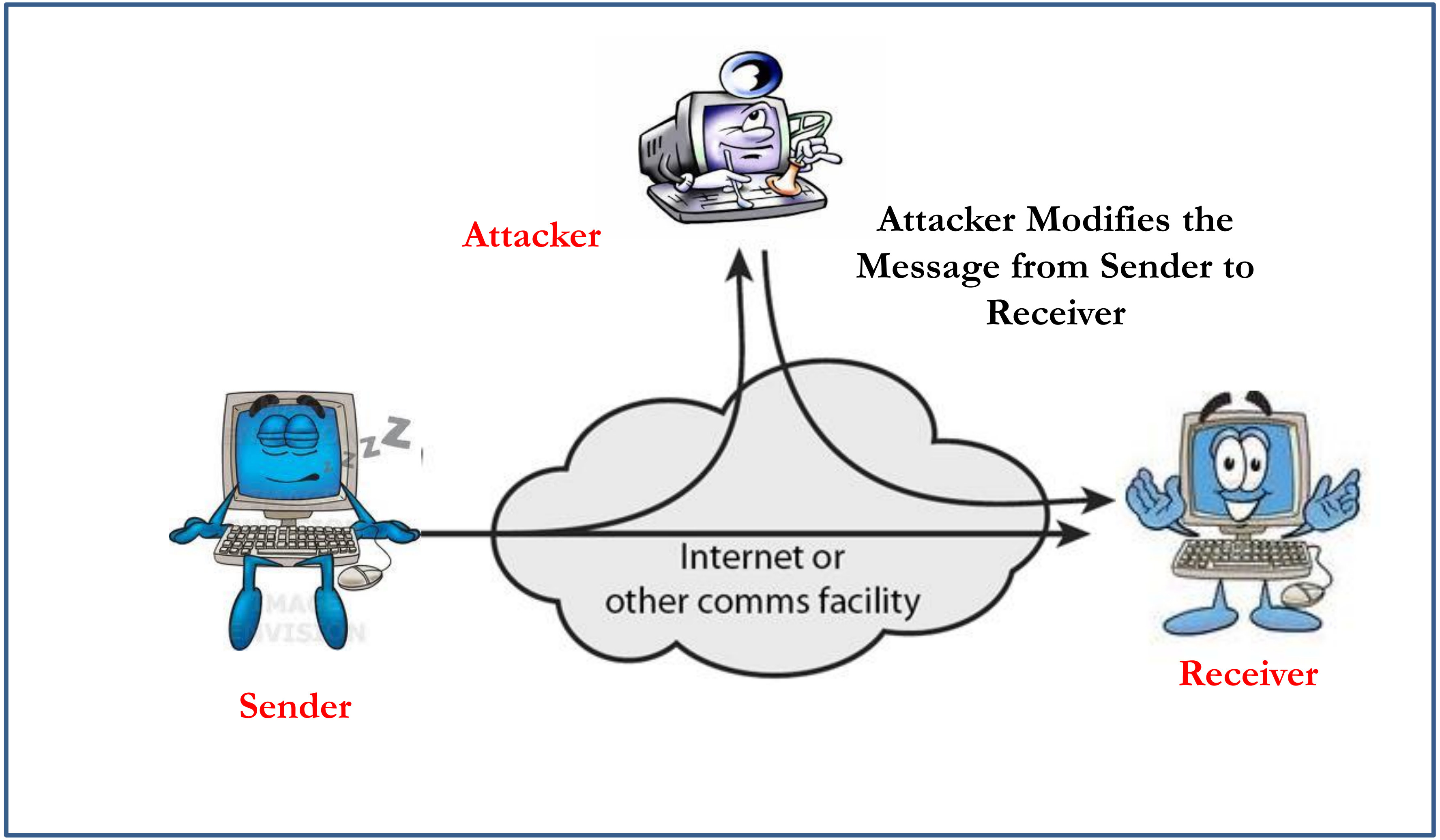


Replay Attack



Attacker
Capture Content of Message from Sender to Receiver and later replay the Message
Internet or other comms facility
Sender
Receiver

Modification of Messages



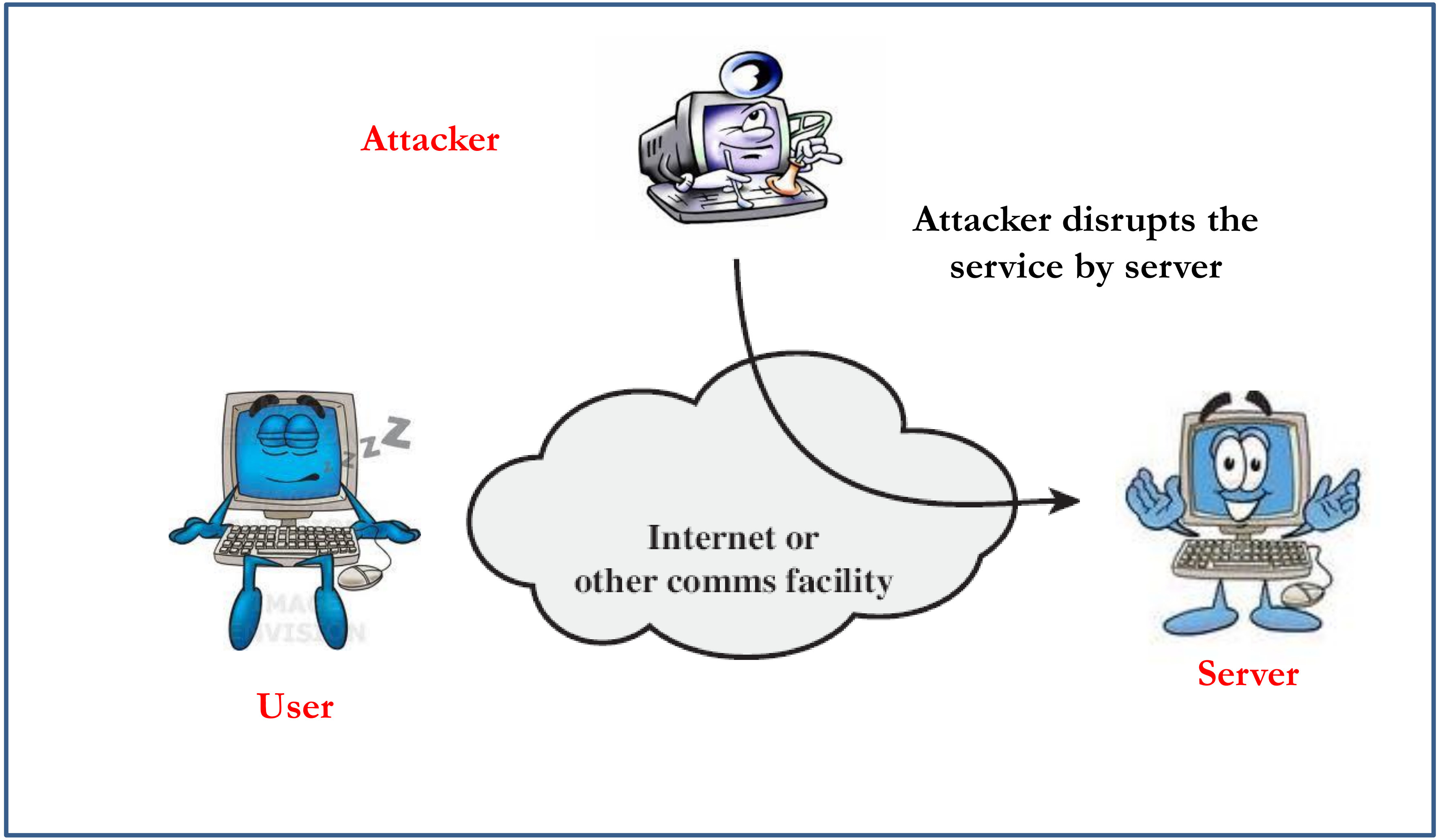
Attacker

Attacker Modifies the
Message from Sender to
Receiver

Sender

Receiver

Denial of Service


Attacker
Attacker disrupts the service by server
Internet or other comms facility
User
Server

Denial of Service Attack

- Denial of Service Attack threatens Availability
- Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.
- The denial of service prevents or inhibits the normal use or management of communications facilities.

Observations

- Active attacks present the opposite characteristics of passive attacks.
- Passive Attacks are difficult to detect, measures are available to prevent their success.
- Active attacks is quite difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities.

Challenge

- The goal is to detect active attacks and to recover from any disruption or delays caused by **Attacker**

Outline

- OSI Security Architecture: Introduction
- Security Goals
- Security Attacks
  - ✓ Taxonomy of Attacks

Thank U