योगः कर्मसु कौशलम्

PARUL INSTITUTE

UNIT-1 INTRODUCTION AND SECURITY THREATS

Prepared by:
Kajol Patel
PIET- DS

Computer and Network Security-3350704

Outlines

- Introduction and Security Threats
- Threats to security
- Steps to Attack
- Confidentiality, Integrity, Availability
- Types of attack

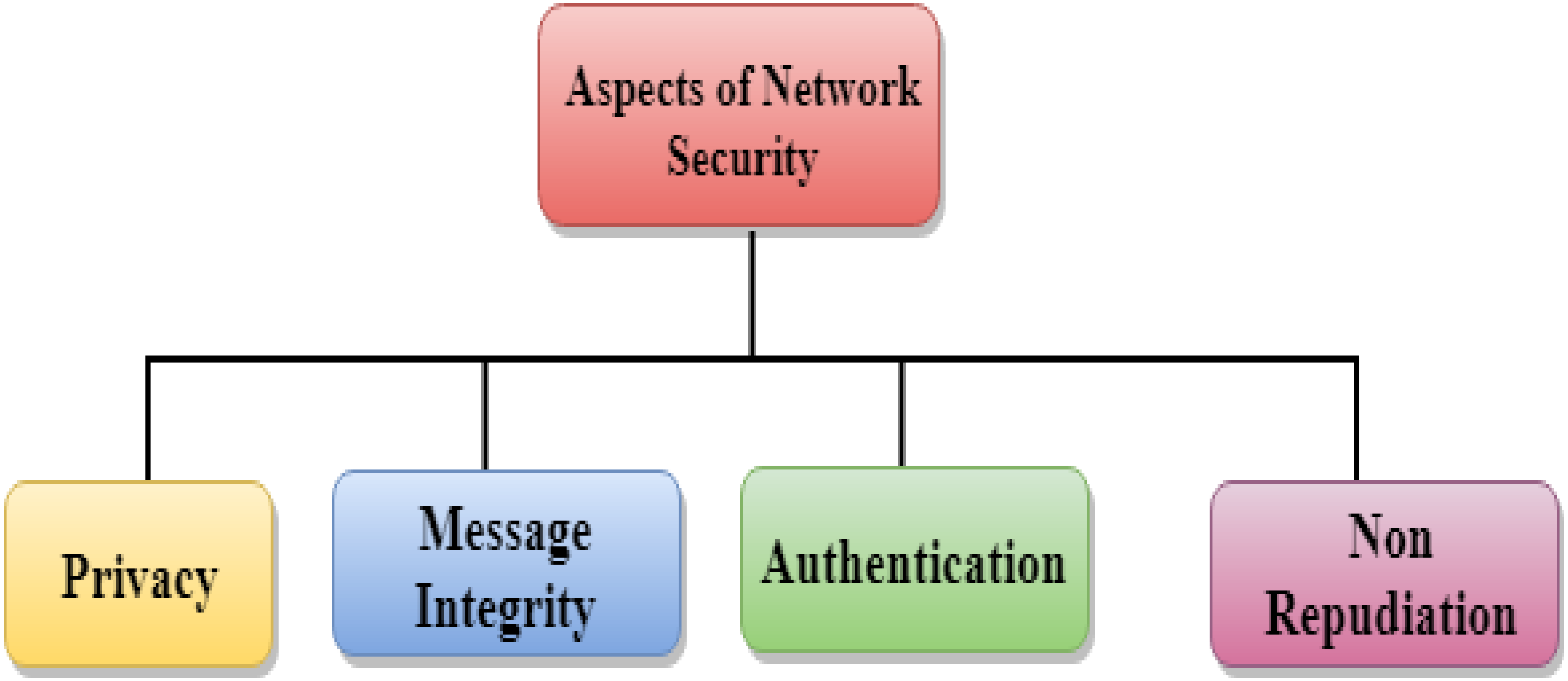
Introduction and Security Threats

- **Computer network security** consists of measures taken by some organizations or business to monitor and prevent unauthorized access from the outside attackers/hackers
- Different approaches to computer network security management have different requirements depending on the size of the computer network
- **For example**, a home office requires basic network security while large businesses require high maintenance to prevent the network from malicious attacks

Cont …

- There are numerous perspectives that make up organize security – the main components are prevention, protection and security The ultimate goal of network security is to create a connected network that protects against illegal/abnormal activity while simultaneously allowing you to perform the activities you need to

Aspects of Network Security


Aspects of Network Security

Privacy

Message Integrity

Authentication

Non Repudiation

Cont …

- **Privacy:** Privacy implies both the sender and the receiver expects confidentiality The transmitted message ought to be sent uniquely to the planned receiver while the message ought to be misty for different clients
- **Message Integrity:** Data integrity means that the data must arrive at the receiver exactly as it was sent There must be no changes in the data/message content during transmission, either maliciously or accident, in a transit

Cont …

- **Authentication:** Authentication means that the receiver is sure of the sender identity, i e , no unauthorised person has sent the message
- **Non-Repudiation:** Non Repudiation means that the receiver must be able to prove that the received message has come from a specific sender The sender must not deny sending a message that he or she send

Threats of Security

- **Followings are the threats of Security:**
  - Viruses and Worms
  - Intruders
  - Insiders
  - Criminal
  - Organizations
  - Terrorists
  - Information
  - Warfare

Cont….

- **VIRUS:**
  - A computer virus is a malicious program that self-replicates via copying itself to another program. In different phrases, the computer
  - virus spreads with the aid of itself into other executable code or documents.
  - Almost all viruses are connected to an executable document, which means the virus may also exist on your pc but it surely cannot infect your computer unless you run or open the malicious program.
  - It is important to note that a virus cannot be spread without a human action(such as running an infected program).

Cont….

- **Worms:**
  - Worm is similar to a virus by design and is considered to be a sub-class of a virus.
  - Worms spread from computer to computer , but in contrast to a pandemic, it has the functionality to travel without human action
  - A bug takes advantage of record or information delivery functions in your device, that is what permits it to travel unaided.

Cont….

- **INTRUDERS:**
  - One of the 2 most publicized threats to safety is the intruder (the other is viruses), frequently known as a hacker or cracker..
  - Intruders can be categorised in three Classes:
- **MASQUERADER:**
  - An individual who isn't always authorized to use the computer and who penetrates a gadget's access controls to make the most a legitimate consumer's account.

Cont….

- **INTRUDERS:**
  - A valid consumer who accesses records, packages, or sources for which such access isn't always legal, or who is legal for such access however misuses his or her privileges
- **Clandestine user:**
  - An person who takeover supervisory manage of the system and uses this control to suppress audit collection.

Cont….

- **INSIDERS:**
  - A malicious insider threat to an organization is a modern or former worker, contractor, or other commercial enterprise accomplice who has or had legal get entry to an agency's network, system, or facts.
  - He/she is intentionally handed or misused that access to in a way that negatively affected the confidentiality, integrity, or availability of the organization's data or information structures..
  - Employees already have access and knowledge about the structure and content of corporate databases

Cont….

- **TERRORISTS:**
  - The terrorists use cyberspace to cause uncertainty.
  - Cyber attacks occur in two forms, one used to attack data, and others focused on control systems
- **INFORMATION WARFARE:**
  - Information warfare (IW) is a concept involving the warfare area use and management of information and verbal exchange era in pursuit of a aggressive advantage over an opponent.

Cont….

- **CRIMINAL ORGANIZATION:**
  - Organized crime is a class of transnational, countrywide, or neighbourhood groupings of fairly centralized organizations run through criminals who intend to interact in illegal interest, maximum usually for money and profit.

AVENUE OF ATTACK

- **Two reasons for attack:**

1. Specifically targeted by the attacker
2. Opportunistic target

STEPS IN ATTACK

- **Step 1:**

  Information gathering: The attacker will gather as much information about organization as possible.

- **Step 2:**

  Determination of target system: Then determine what target systems are available and active.

- **Step 3:**

  Find vulnerability & suitable tools: To perform a port scan which gives indication of which services are running on target machine.

- **Step 4:**

  Attack to the target system

SECURITY BASICS

- Confidentiality
- Integrity
- Availability

INTEGRITY
AVAILABILITY
INFORMATION SECURITY
101
1010
000001
CONFIDENTIALITY

Cont….

- **Confidentiality:**
- When we talk about confidentiality of information, we are talking about protecting or securing the data and the information from disclosure to unauthorized parties (wrong Person).
- now a days Information has value, especially Bank account statements, personal information, credit card numbers, trade secrets, government documents.

Cont….

- **Integrity:**
- It refers to protecting information from being modified by unauthorized parties.
- Information only has value if it is correct. Information that has been tampered with could prove costly.
- For example, if you were sending an online money transfer for 100 rs, but the information was tampered in such a way that you actually sent 10,000 rs , it could be very costly for you.

Cont….

- **Availability:**
- Availability means that information is accessible to authorized users. It is basically an assurance that your system and data are accessible by authorized users whenever it’s needed. Similar to confidentiality and integrity, availability also holds a great value.

Types of attack

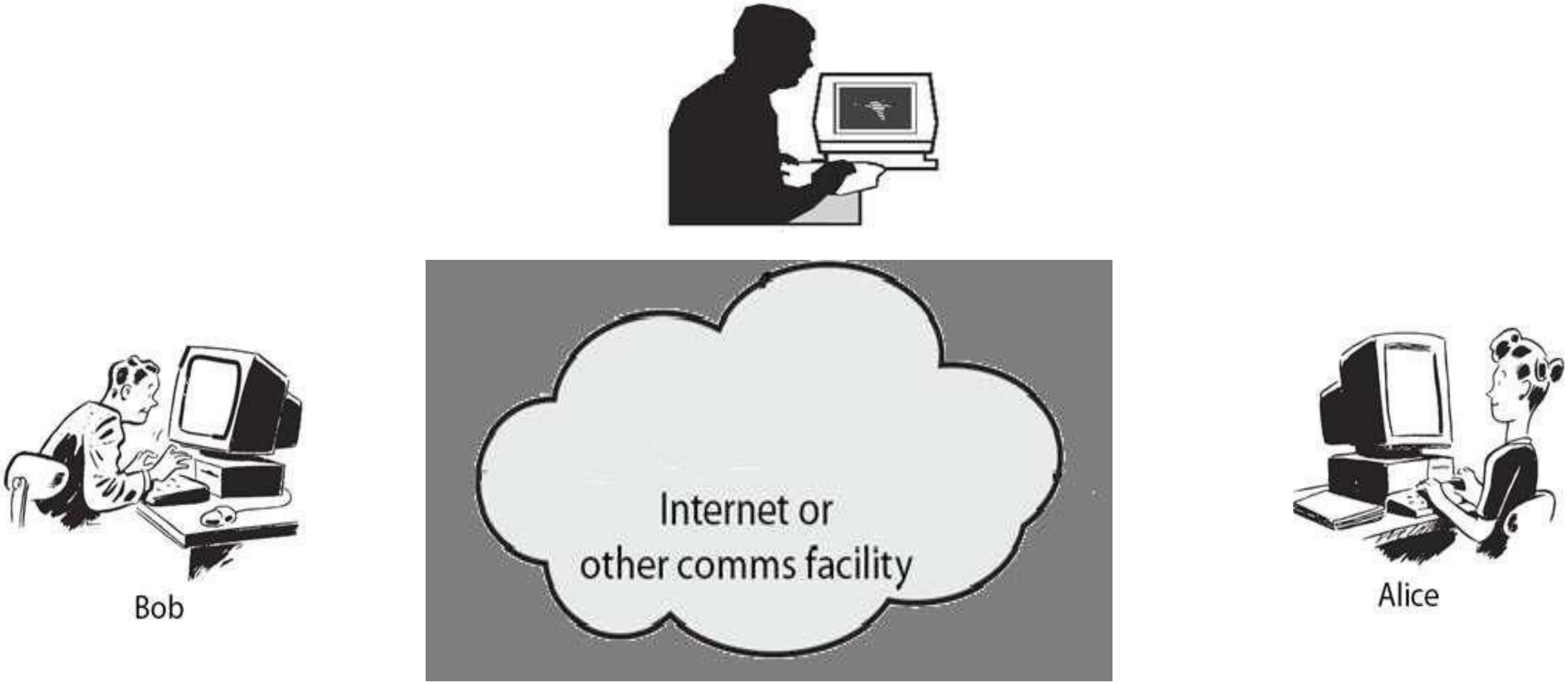
- There are mainly two types:
- **Passive attacks**:
  - A Passive attack attempts to learn or make use of information from the system but does not affect system resources.
  - Passive attacks are in the nature of eavesdropping on, or monitoring of, transmission. The goal of opponent is to obtain information that is being transmitted.

Cont….

- **Active attacks**:
- An Active attack attempts to alter system resources or affect their operations.
- Active attacks involve some modification of the data stream or creation of a false stream.

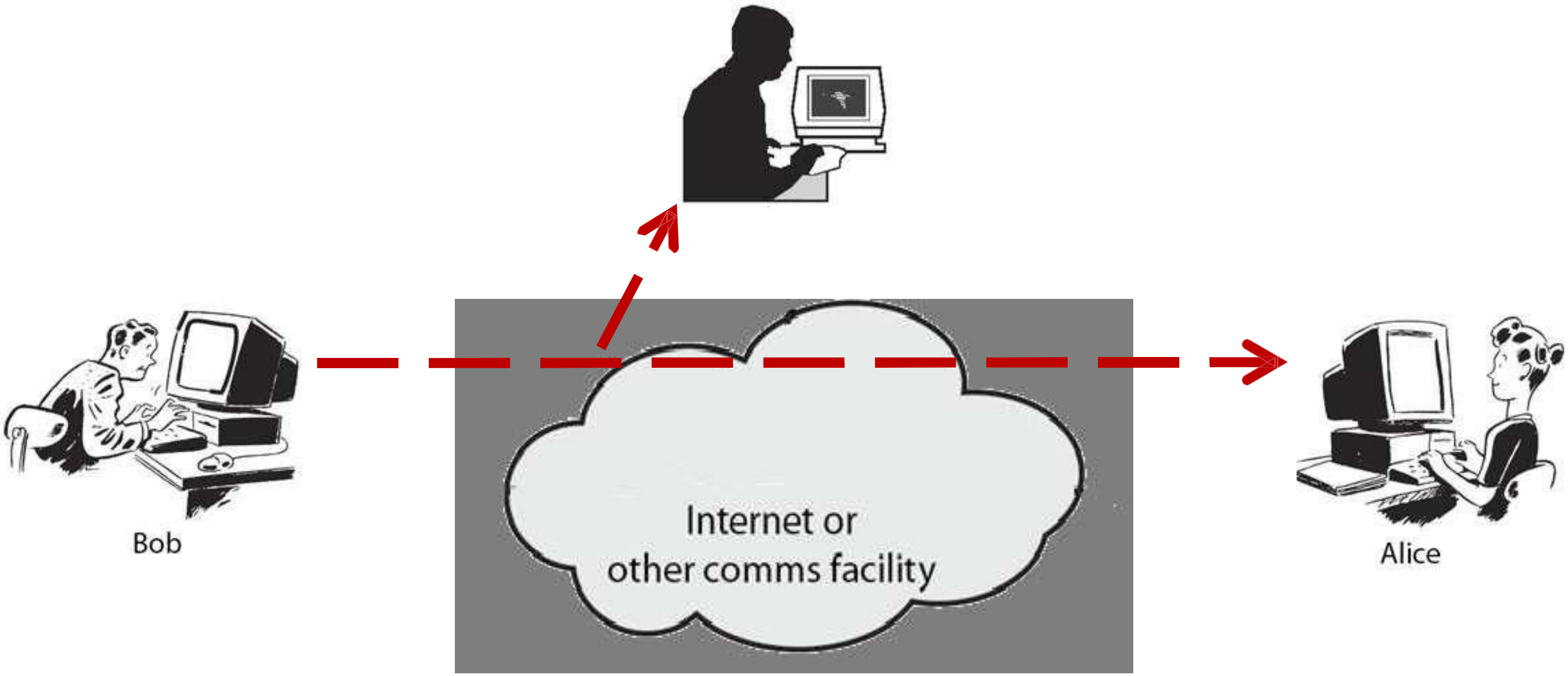
Cont….

- □ **Passive Attack - Interception**



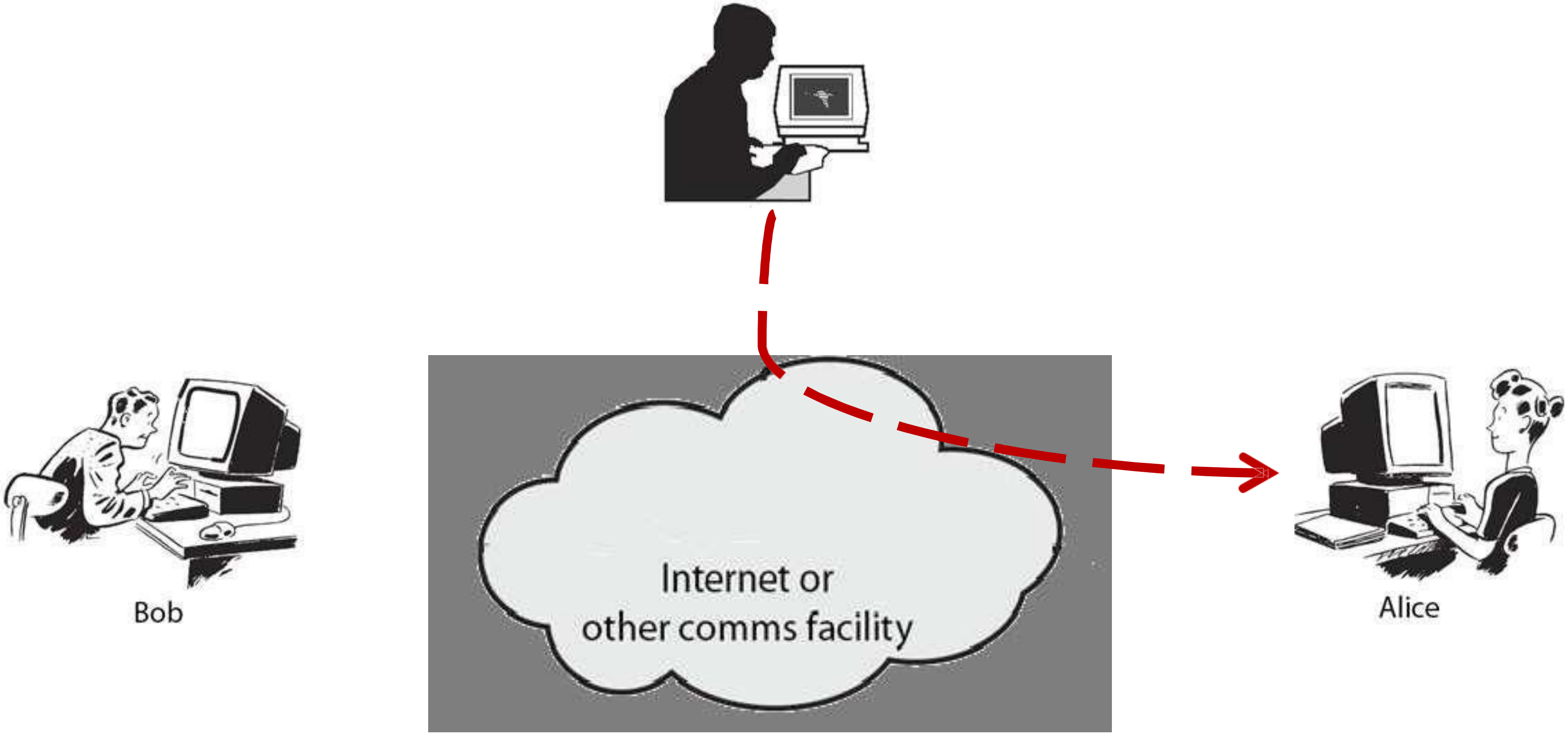
Cont….

- **Passive Attack: Traffic Analysis**



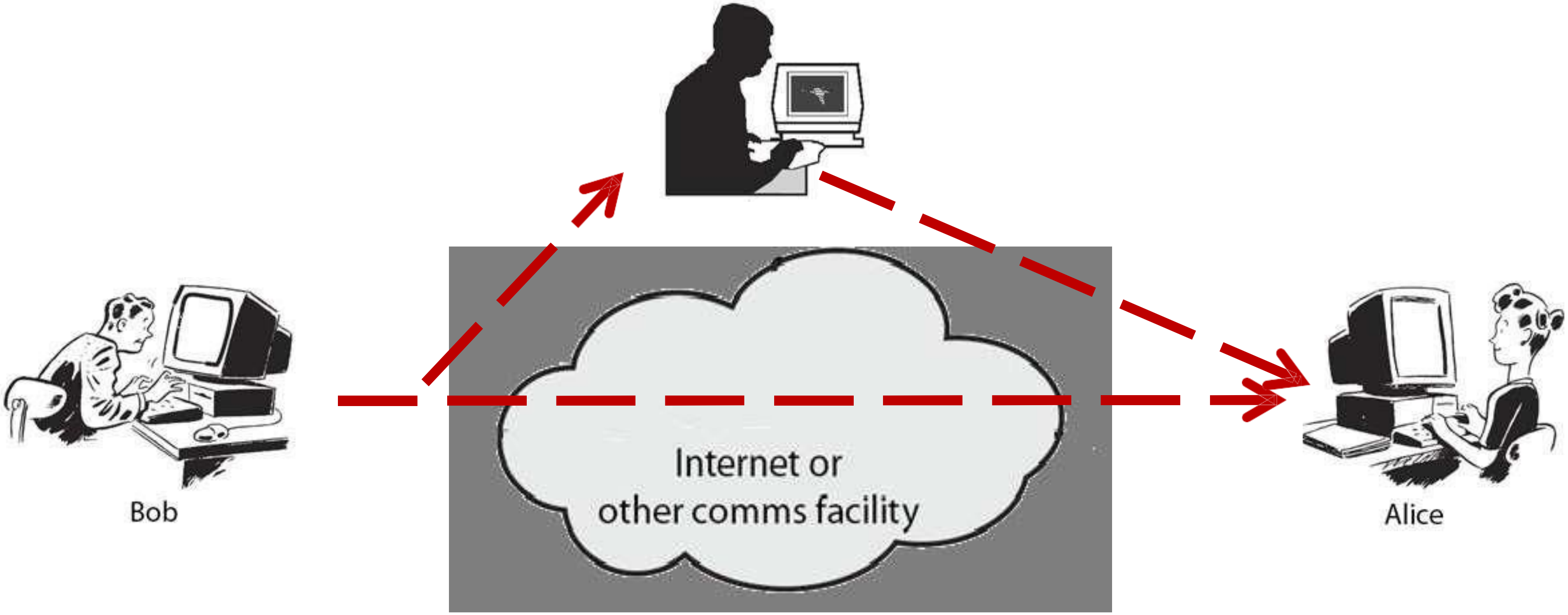
Cont….

- **Active Attack: Masquerade:**



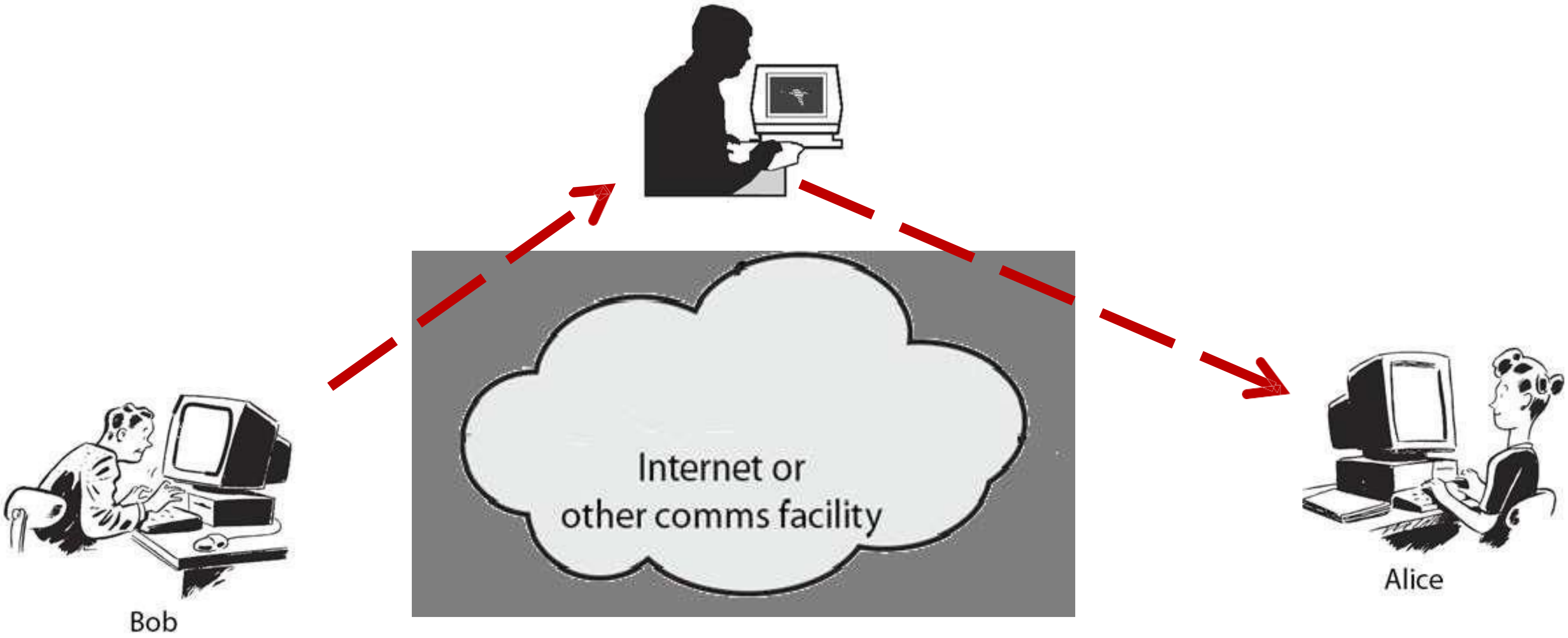
Cont….

- **Passive Attack: Replay**



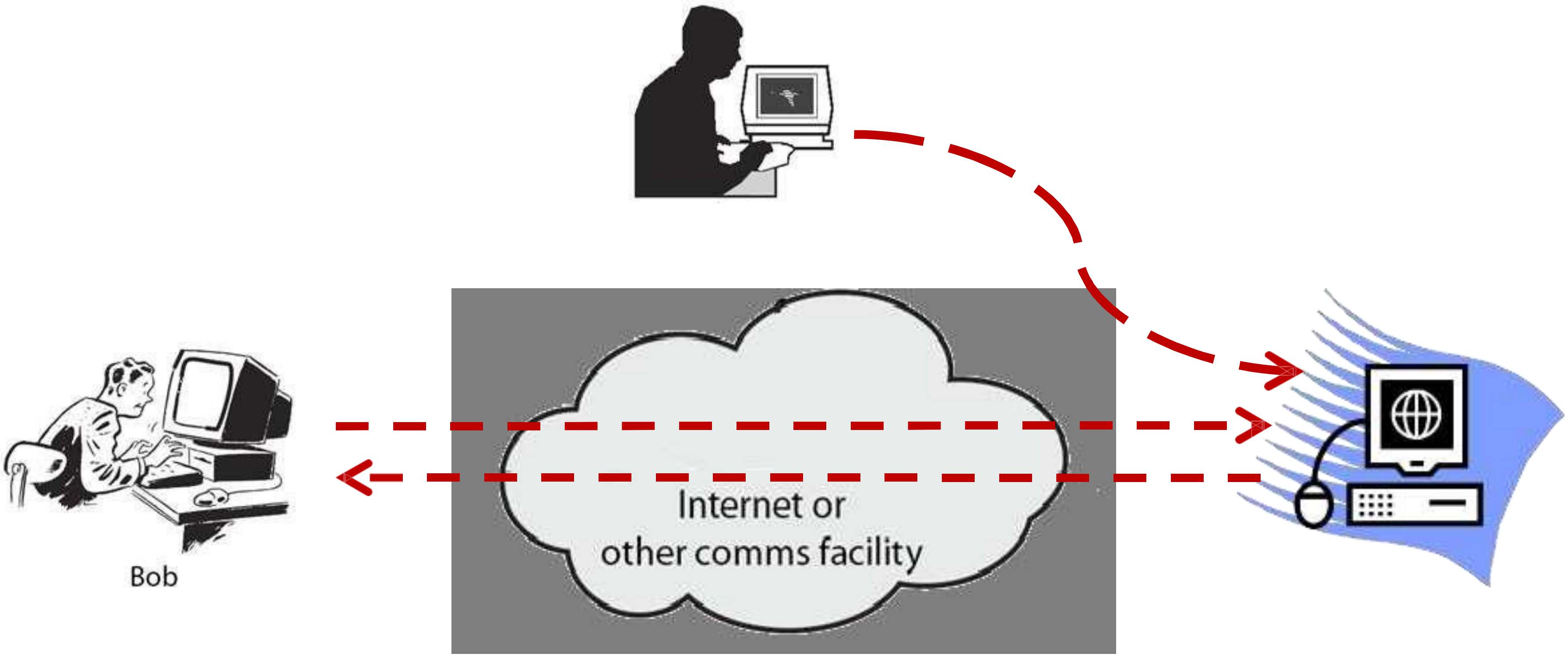
Cont….

- **Modification of message:**



Cont….

- **Active Attack: Denial of service:**



Other Types Of Attack

- backdoors and trapdoors
- sniffing
- Spoofing
- TCP/IP Hacking,
- Phishing attacks,
- Distributed DOS,
- SQL Injection
- Malware : Viruses, Logic bombs

Backdoors and Trapdoors

- This can have two different meanings.

1. During the development of a complicated operating system or any application, programmers add backdoors or maintenance hooks. These back doors allow them to examine operations inside the code while the program is running.
2. The second type of back door refers to gaining access to a network and inserting a program or utility that creates an entrance for an attacker.

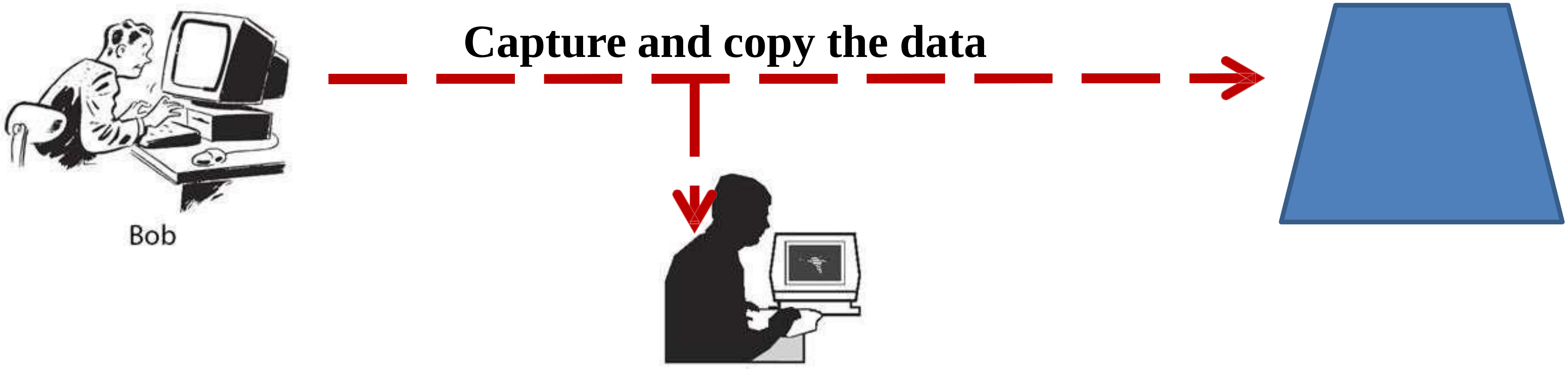
Cont….

- The program may allow a certain user to log in without a password or gain administrative privileges.

- Trapdoor is also known as backdoor .it is secret entry point into to get the illegal access to the software or also used for the debug process by the developers

Sniffing

- □ It is a process of monitoring and capturing all data packets passing through a given network using software or a hardware .
- □ Attackers use sniffers to capture data containing sensitive information such as password ,account details etc.



Capture and copy the data

Spoofing

- It happens when an attacker or malicious program successfully acts on another persons behalf by impersonating data .
- **Example of spoofing** is when an email is sent from a unauthorized or false sender address, that asks the recipient to provide sensitive data. This email could also contain a link to a malicious website that contains malware.

TCP/IP hacking

- When an unauthorized person or user hack or hijack a network connection of another user .
- **For example** .the attacker monitors the network transmission and analyse the sources and destination IP address of the two computer .Once the attackers discovers the IP address of one of the user ,they can knock one of the users off their connections using a denial of services attack and then resume communication by spoofing the ip-address of the disconnected user .It is combination of sniffing and spoofing

SQL injection

- It is a techniques where malicious users can inject SQL commands into an SL statement ,via web pages .
- Injected SQL commands can alter SQL commands or statement and compromise the security of a web application

Logic Bomb

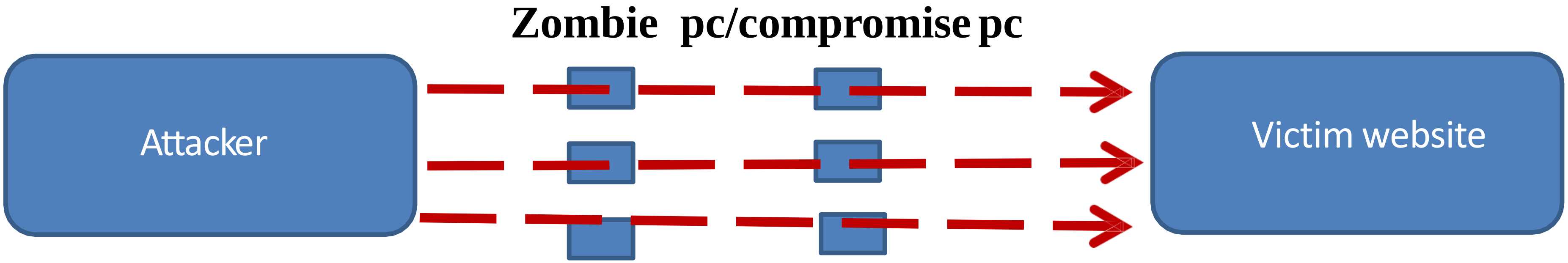
- It is some kind of triggered code or program which is embedded in any important software that is to explode when certain condition are met .
- The condition can be anything like any presence of file or absence of file ,or it can be just act like a time bomb which is set according to a particular time or a day .

Phishing attack

- In this kind of attack the hacker created a fake account or a fake website that looks exactly same as the original one .
- When the users attempt to log in his /her details, hackers records their data and used for its own purpose

Distributed denial of services (DDos)

- Ddos attack means using several computers and connections .the computers behind such as attack are often distributed around the world and will be a part of BOTNET.(zombie system)

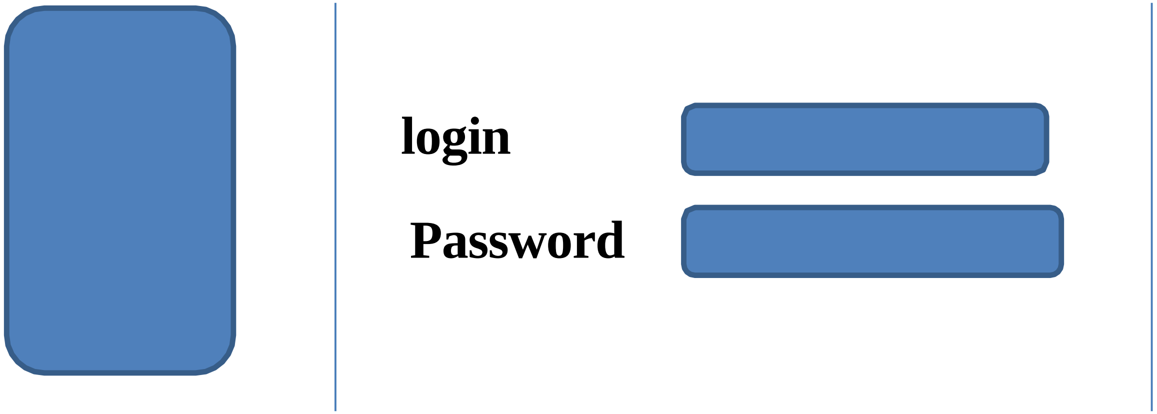


Man in the middle attack

- In this kind of attack the attacker secretly relays and possibly alters the communications b/w two parties who believe they are directly communicating with each other .

Trojan horse

- Its alike a virus.
- But doesn’t modify the data and also doesn’t replicate the data.
- It’s a hidden kind of code which is intended to leak your confidential data /message or information.



login

Password

When you entered your password and id the trojan horse is reading the keys you are typing and after that it take a record/snapshot.

Thank You