Chapter – 1

Introduction and Security Threats

Introduction

Requirements and need of information security:

•Security is to make sure that the **unauthorized person does not get the access** to the private data.

•Now a days, the physical data are converted into electric one(digital data), so there is a chance to copy or alter the data.

•With the use of distributed system, data are shared among different users and due to that there is a chance of violation in security of data.

Introduction

- Some examples of security violations are:
  - User A transmits secure data to User B and User C read it.
  - User A transmits data to User B and User E intercepts it and modifies it.
  - Sometimes not only intercept, E constructs his own message.
- So, we can say that there is a need of security.
- Security architecture X.800 for OSI, defines systematic approach to provide better security against threats.

Introduction

Data Security:

- Data security is the means keeping data safe from corruption and access to those data is controlled.

Computer security:

- Computer security includes protection of information and property from theft, corruption, or natural disaster.
- With protection, allow information and properties to remain accessible to users.

Introduction

Network Security:

- Protect network and the network accessible resources from unauthorized network access, continuous monitoring and measurement of its effectiveness.

Internet Security:

- It is required to protect information during their transmission over a collection of internet.

Introduction

Threat and Attack

- **Threat:**
  - Anything that has the potential to cause serious harm to a **computer** system is called **threat** in **computer security**.
- **Attack:**
  - An intelligent act that intentionally attempt to hide security services and violate the security policies of a system.

Introduction

The OSI security architecture:

- The OSI (**O**pen **S**ystem **I**nterconnection) was developed as an international standard.
- **X.800** is a security architecture for OSI.
- It defines systematic approach to provide security.
- It focuses on **Security attacks, Security mechanisms and Security services.**
- **Security attacks:**
  - Any action that compromises the security of information of an organization.

Introduction

- **Security mechanisms:**
  - A process that is designed to detect, prevent or recover from security attack.
- **Security services:**
  - A processing or communication service that enhances the security of data processing and information transfer of an organization.
  - The services are intended to counter security attacks and they make use of one or more security mechanism to provide the service.

1.1 Threats to Security

- **1.1.1 Viruses:**
- Virus is a part of software that may harm other programs by modifying them.
- It is a kind of **malware** (malicious software).
- It **spreads from one computer to another**, leaving infections as it travels.
- Generally **viruses attached to the executable (.exe) files** and when user runs that program viruses spread in the system.
- They may create mild effects and can cause crash of data and software, may cause **denial-of-service** attack.

1.1 Threats to Security

- They also can be spread as they travel from one system to another using external devices, network or infected emails.
- They may infect memory, a floppy disk, a hard drive, a backup tape, or any other type of storage.
- Viruses can protect themselves by hiding in their host programs, by operating in delayed fashion, or by changing their physical characteristics to avoid detection.
- Virus is not independent program. It depends upon a host program, which it infects.
- Virus requires host to spread.

1.1 Threats to Security

- Types of viruses are as under:
- **Parasitic virus:** It is the most common form of virus.
- A parasitic virus attaches it self to executable files and replicates, when infected program is executed, by finding other executable files to infect.
- **Memory Resident Virus:** Stay in main memory and then infect every exe files that is executed.
- **Boot sector virus:** Infects a master boot record of the disk and spreads when system is booted from the disk containing virus.

1.1 Threats to Security

- **Stealth Virus:** A form of virus explicitly designed to hide itself from detection by antivirus software.
- **Polymorphic Virus:** A virus that keeps changing its signature (identity) on every execution.
- This makes it very difficult to detect.
- **Metamorphic Virus:** Same As polymorphic virus.
- The difference is that a metamorphic virus rewrites itself completely at every time, making its detection much harder.

1.1 Threats to Security

- **Macro Virus**: A virus that attacks macros, are named as macro virus.
- This type of virus affects special software like Microsoft word or excel.
- It affects every documents created by that application and spread quite easily with that documents such like with mail.

1.1 Threats to Security

1.1.2 Worms:

- Worms is an **independent** program.
- A worm is a computer program that can **copy itself** and **send copies** from computer to computer across network connection.
- Worms are **standalone software** and do not require a host program or **human help to spread**.
- Worms **don’t alter or delete file**.
- Worms consumes too much system memory, slowing down computers, also causing web servers, network servers and individual computer to stop responding.

1.1 Threats to Security

- A worm can take advantage of file or information transport feature on system, which then allows it to travel without help.
- Worm may replicate itself by:
  - Email facility
  - Remote login capability
  - Remote execution capability
- Worm may also **hide its presence by naming itself as a system process** or by some other names that may not be noticed by the operator.

1.1 Threats to Security

1.1.3 Intruders:

- **“Intrude”** means put oneself purposely(intentionally) into a place or situation where one is unwelcome or uninvited.
- An intruder is unauthorized individual trying to access resources illegally.
- The main aim of intruders is to gain access to the system and intrude(interrupt) the privacy of the network.
- **Intruders** may be **insiders** or may be **outsiders**.
- Intruders attacks range from the gentle to the serious one.

1.1 Threats to Security

- They are mainly classified into **three** categories:
- **1**. **Masquerade**: An individual who is not authorized to use the computer but he gets access to the computer system and exploit (misuse or take advantage of) **user data and account.**
- **2. Misfeasor:** A legal user who accesses data, programs or resources for which he is not authorized.
- **3. Clandestine user:** User who gains administrative access to the system.
- The **masquerade** is likely to be an **outsider**, the **misfeasor** generally is an **insider** and **clandestine** user can be either **insider or outsider.**

1.1 Threats to Security

- **1.1.4 Insiders:**
- An insider threat is **a malicious threat** to an organization that comes from **people within the organization**.
- Insiders are more dangerous than outside intruders.
- Insiders can be employees, former employees, contractors, partners or business associates, who have inside information of organization's security, data and computer system.
- The threat may involve fraud, the theft (robbery) of confidential information, the theft of intelligent property, or the damage of computer system.

1.1 Threats to Security

- The attacks made by insiders are generally passive attacks that are more difficult to detect.
- There are some attacks that can be committed by insiders, such as the unauthorized release of copyrighted information, or the damage of properties that only employees can access.
- So prevention is better to avoid the insider’s attack.
- Encryption is better solution in prevention to insiders.

1.1 Threats to Security

- **1.1.5 Criminal organizations:**
- Due to increasing the computer networks and internet uses, criminal organizations turn into the electronic world to misuse.
- Common types of activities done by criminal organizations are: Fraud, blackmail and faking.
- One difference between criminal group and the “average” hacker is the level of organization is much higher than a simple hacker.
- They have more money and financial supports compare with hackers.

1.1 Threats to Security

- Attacks by criminal organizations usually fall into the **“structured threat”** category.
- They are done by great amount of **planning**, a longer period of **time** to conduct the activity, more **financial banking** to complete it.

1.1 Threats to Security

- **1.1.6 Terrorist :**
- A cyber terrorist is a criminal who uses computer technology and the internet especially to cause fear and trouble.
- Some cyber-terrorists spread computer viruses and others threatens people electronically.
- Cyber terrorists might have ethical or religious reasons for wanting to terrorize and others do it for personal reason.
- Cyber terrorism is sometimes referred to as electronic terrorism or information war.

1.1 Threats to Security

- **1.1.7 Information warfare :**
- It is actually the **war** conducted **against** the **information** and **information processing** equipment used **by enemy**.
- It falls into highly structured threat category.
- Information is used as weapon by an enemy.
- This type of threat is characterized by a much longer period of preparation, very high financial backing and a large and organized group of attackers.
- Targeted areas of information warfare are, water, electricity, oil and gas refineries and distribution, banking and finance, telecommunications.

1.2 Avenue of attack

- A computer system is attacked because of general reasons like: it is specifically targeted by the attacker, or it is a target of opportunity.
- The attacker chose the target not because of the hardware or software the organization is running but for another reason, such as a political reason.
- An example of this type of attack would be an individual in one country attacking a government system in another country.
- Alternatively the attacker may be targeting the organization as part of a “**hacktivist**” attack.
- committing some sort of electronic fraud is another reason a specific system might be targeted for attack.

1.2 Avenue of attack

- **Steps in attack:**
- **1. Inspection:** For attacker to enter into targeted network, the attacker will need to **gather as much information** about the organization as possible.
- There are number of ways to do this, including **studying the website** of organization, looking for posting in **news** group or **analyze the security policies.**
- Also an attacker can go through the financial report of the targeted industry.

1.2 Avenue of attack

- The first step in the technical part of an attack is often to determine **what target system** are **available and active.**
- This is often done with “ping”.
- This includes activities like internet search, dumpster diving, social engineering etc.
- **2. Scanning:**
- The next step is often to perform a port scan.
- This will help to **identify which ports are open**, which gives an identification of services running on the target machine.

1.2 Avenue of attack

- Also identifying which OS and which specific application is running on the targeted system.
- This can be done by ping, trace route, port scanning tools etc.
- **3. Getting access:**
- Once scanning is done, the attacker should have a list of possible target machines.
- Knowing the operating helps the attacker decide which tools to use in the attack.
- In addition to information about specific weakness, some sites may also provide tools that can be used against those weakness.

1.2 Avenue of attack

- An attacker can search for known weakness and tools can be used against them.
- They download the information and tools and then use them against a site.
- If administrator of the targeted system has not installed correct patch then the attack will be successful.
- If the patch has been installed, the attacker will move on the next possible weakness.
- If all possible patches are installed, the attacker will have to use brute-force attack, which involves guessing user id and password.

1.2 Avenue of attack

- This can be done by OS attacks, SQL injection, cross site scripting, checking online database etc.
- **4. Maintaining access:**
- After getting access of system, attacker needs to maintain that access.
- That can be done by viruses, worms, key loggers, backdoors etc.
- **5. Covering your tracks:**
- This can be done by network proxies, SMAC/MAC address changer etc.

1.3 Security Basics (CIA)

- **Confidentiality:**
- It is the **assurance** that the **transmitted data would be protected from unauthorized access**.
- It also means that, only the sender and intended recipient should be able to access the data.
- The other aspect of confidentiality is the **protection of traffic flow** from analysis.
- This requires that an attacker not be able to observe the source and destination, frequency, length or other characteristics of the traffic on a communication facility.

1.3 Security Basics (CIA)

- To maintain data confidentiality, first require **strict authentication**, second: **use strict access control** and third: **ensure encryption of data**.
- It provides protection from passive attack.
- **Integrity:**
- Data integrity ensures that data received is exactly the same as sent by an authorized sender.
- It specifies that content of the message must not be altered during transmission from sender to receiver.
- The data can’t be changed except by an authorized entity.

1.3 Security Basics (CIA)

- It ensures that only authorized parties are able to modify computer system assets and transmitted information.
- Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.
- **1. Connection oriented integrity service:**
- It provides integrity of all user data on a connection and detects any modification, insertion, deletion or reply of any data within entire data sequence.
- It provides protection against message stream modification and denial-of-service both.

1.3 Security Basics (CIA)

- **2.Connection less integrity service:**
- It generally provides protection against message modification only.
- To maintain data integrity, there should be resistance to the change and replacement of data.

1.3 Security Basics (CIA)

- **Availability:**
- It states that the **resources** should be **available to authorized** parties all the time.
- It is violated by **technical issues** (like a malfunctioning part of a computer system), by **natural issues** (like wind or water or fire) or by **human causes** (accidental or deliberate).
- To maintain the data availability, there should be load balancing, quick backup and restoring of data.
- This service provides the **security against denial-of-service** attacks.

1.3 Security Basics (CIA)

Security Services:

•X.800 defines a security service to **ensure security of the systems or of data transfers**. Services are to recover from attack.

•Security services implement security policies and they are implemented by security mechanisms.

•In general security service is a mechanism set up for protecting a system or network.

•Different security services are: **A**uthentication, **A**ccess control, Data **C**onfidentiality, Data **I**ntegrity, **N**on-repudiation(rejection) and **A**vailability.

1.3 Security Basics (CIA)

1. Authentication:

- Assuring that communication is authentic.
- Two types of authentic services are defined in X.800
- **1) Peer entity authentication:**
- This service ensures that both the communicating parties are real and no intruder (opponent) is trying to access the resources or data between them.
- **2) Data origin authentication:**
- Used for the identify the source of data unit.

1.3 Security Basics (CIA)

- It does not provide protection against the duplication or modification of data units.
- It is used in Email where there are no prior interactions between the two interacting users.

2. Access Control:

- It is prevention of the unauthorized entity to use of resource.
- It determines who should be able to access what.
- This service tries to ensure that only the legal users are provided information.

1.3 Security Basics (CIA)

- Each entity trying to gain access must first be identified or authenticated.
- Access control can be classified into: Role management and Rule management.

3. Non – repudiation:

- Non-repudiation prevents either sender or receiver from denying a transmitted message.
- Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

1.4 Types of Attack

Security attacks:

- A Security attack is **an unauthorized activity** committed to **compromise the security of a given system or network**.
- An attack can be launched by a person who is insider or an outsider, known as intruders.
- An intruder is unauthorized individual trying to access resources illegally.
- It is the responsibility of system or network to take care of security of its own self.
- Security attacks are generally classified as active or passive.

1.4 Types of Attack

Passive attack:

- It is not a direct attack. It can be an insider's job.
- These attacks are monitoring or keeping eye on transmitting data.
- The goal of the passive attacker is to get information that is being transmitted.
- Generally attacker doesn't perform any modification.
- Passive attacks are very difficult to detect or prevent, as they are not a direct attack.

1.4 Types of Attack

Passive attack:

- Types of passive attacks are:

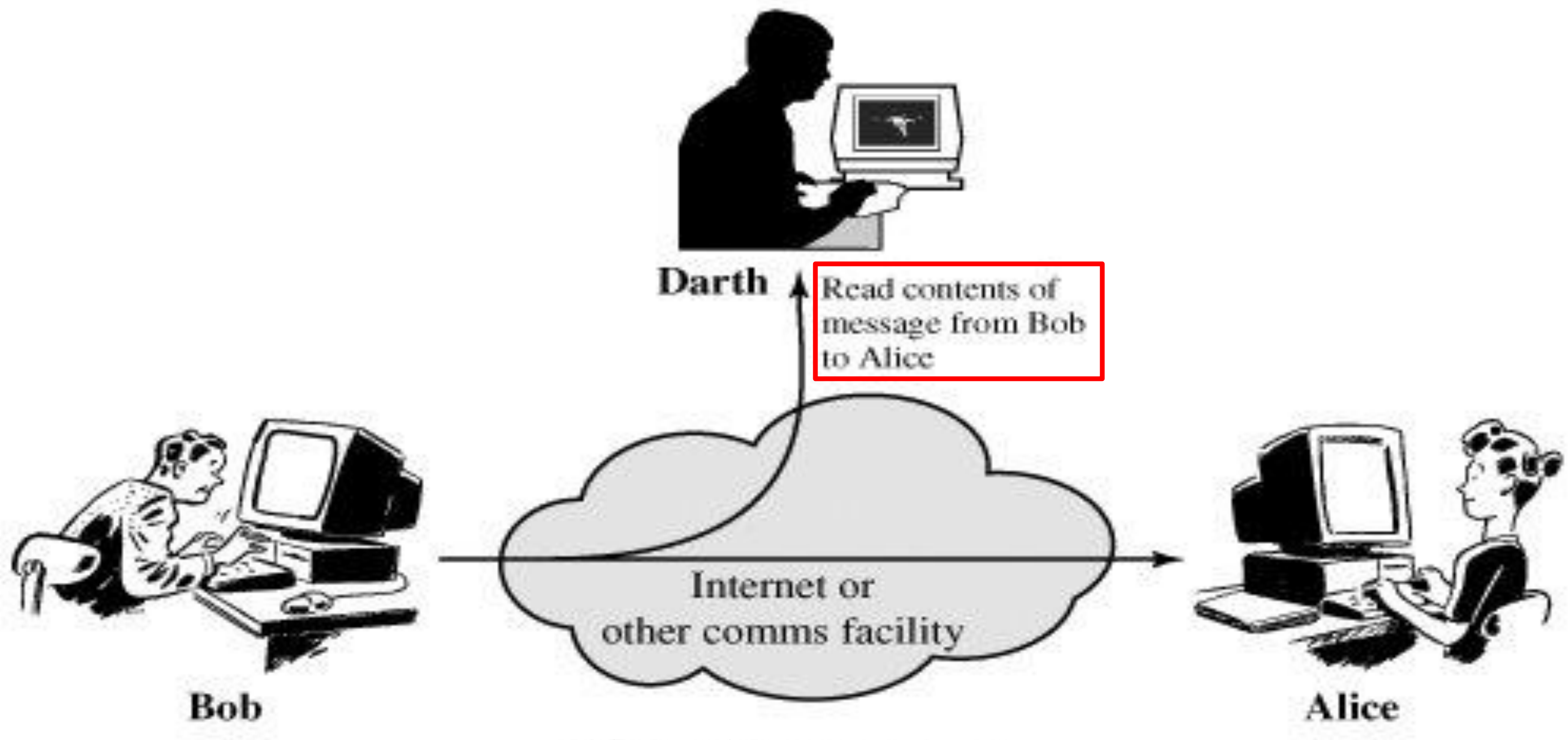
  a) Release of message content

  b) Traffic analysis

1.4 Types of Attack

A) Release of message content:

- A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents

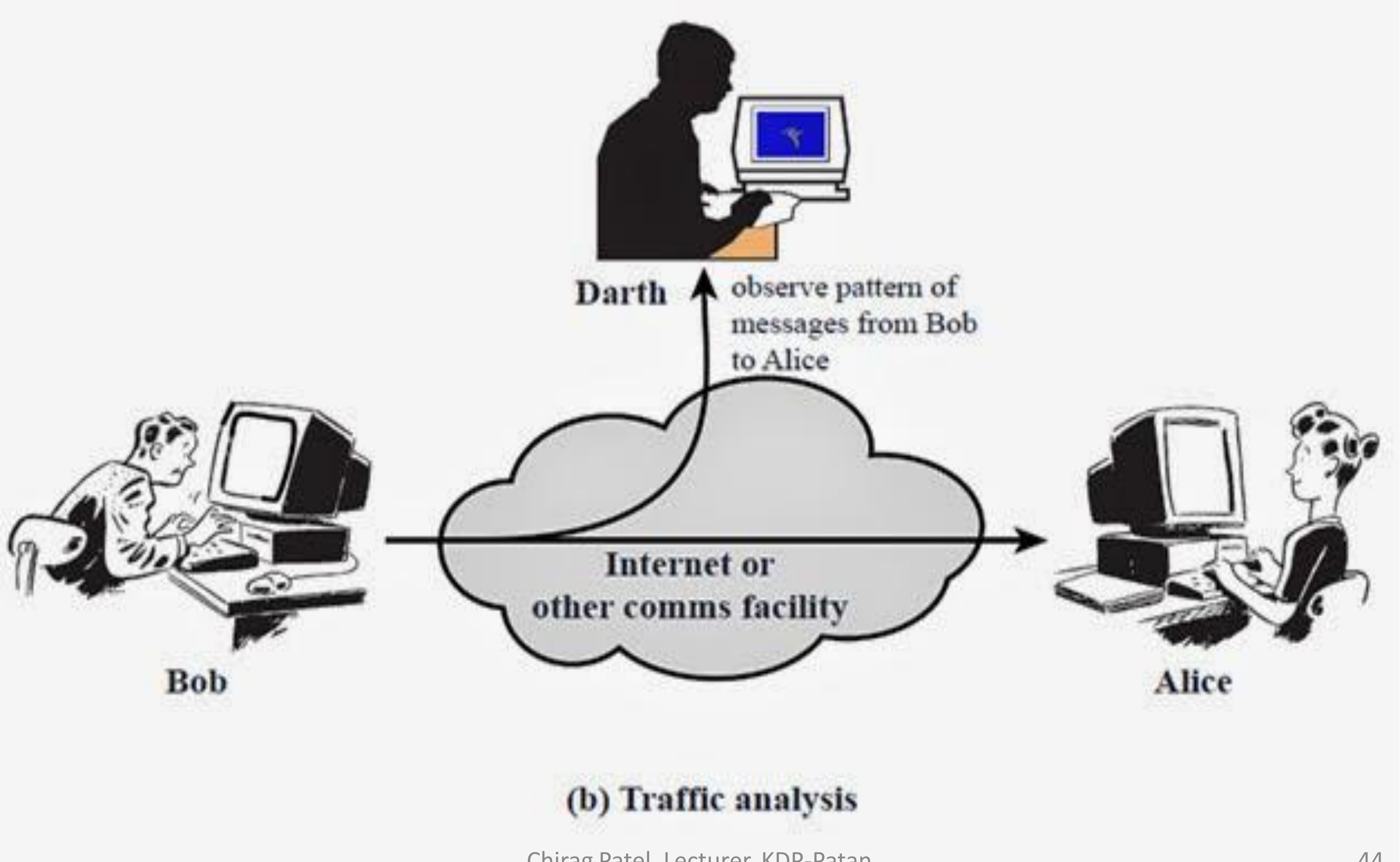
1.4 Types of Attack

A) Release of message content:

- A telephone conversation, an email and a transferred file may get accessed by passive attacks to acquire secret information.
- We would like to prevent an opponent from learning the content of these transmission.

1.4 Types of Attack

B) Traffic Analysis:


Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

(b) Traffic analysis

1.4 Types of Attack

B) Traffic Analysis:

- In this type of attack, attacker **monitors frequency and length of messages.**
- Attacker could determine the location and identity of communication hosts.
- This information might be useful in guessing the nature of the communication that was taking place.
- Prevention is better than detection in case of passive attacks.
- We can prevent passive attacks by encryption.

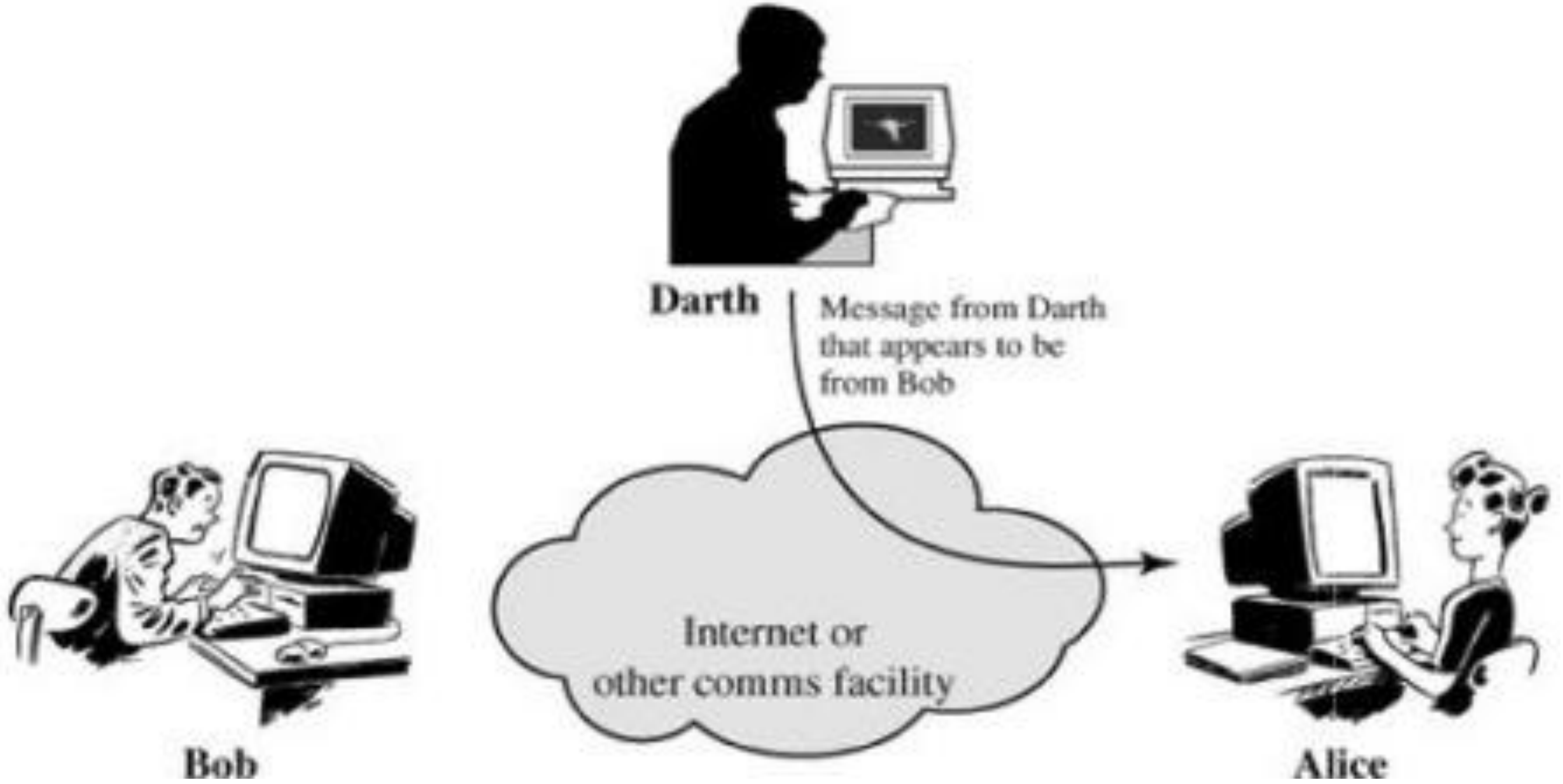
1.4 Types of Attack

Active attack:

- It is kind of **direct attack.**
- Active attacks **modify data or it creates a false stream.**
- These attacks can’t be prevented easily.
- Different active attacks are:
- **A) Masquerade**
- **B) Modification of message**
- **C) Message Reply**
- **D) Denial of service attack**

1.4 Types of Attack

- **A) Masquerade:**

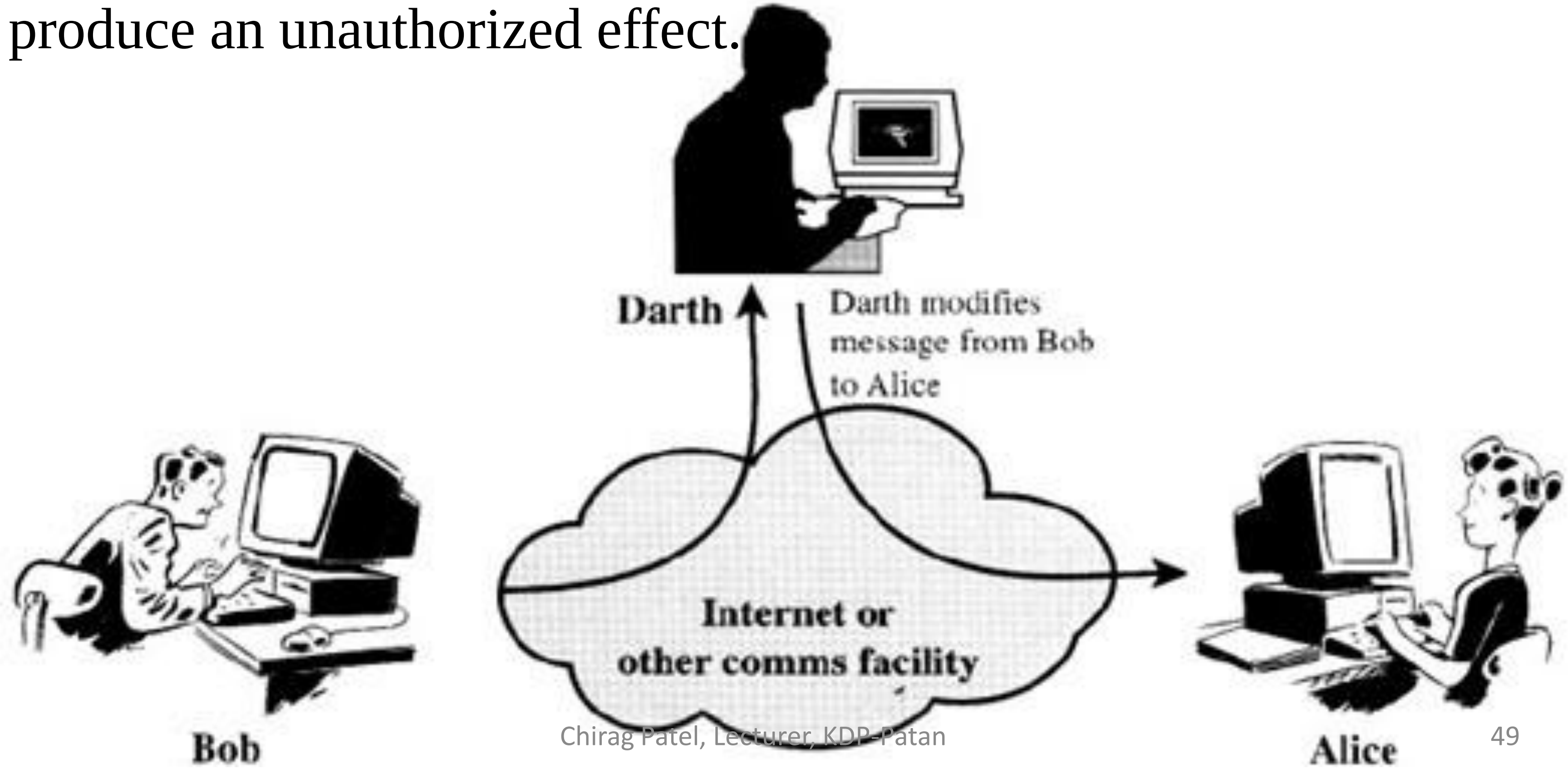

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

1.4 Types of Attack

- **A) Masquerade:**
- A masquerade takes place when an **intruder pretends to be sender or receiver** of any confidential communication.
- It is known as masquerade because attacker has a **mask of an authorized user.**
- An intruder can capture the user id and password of a legal user, and log in as a valid user.

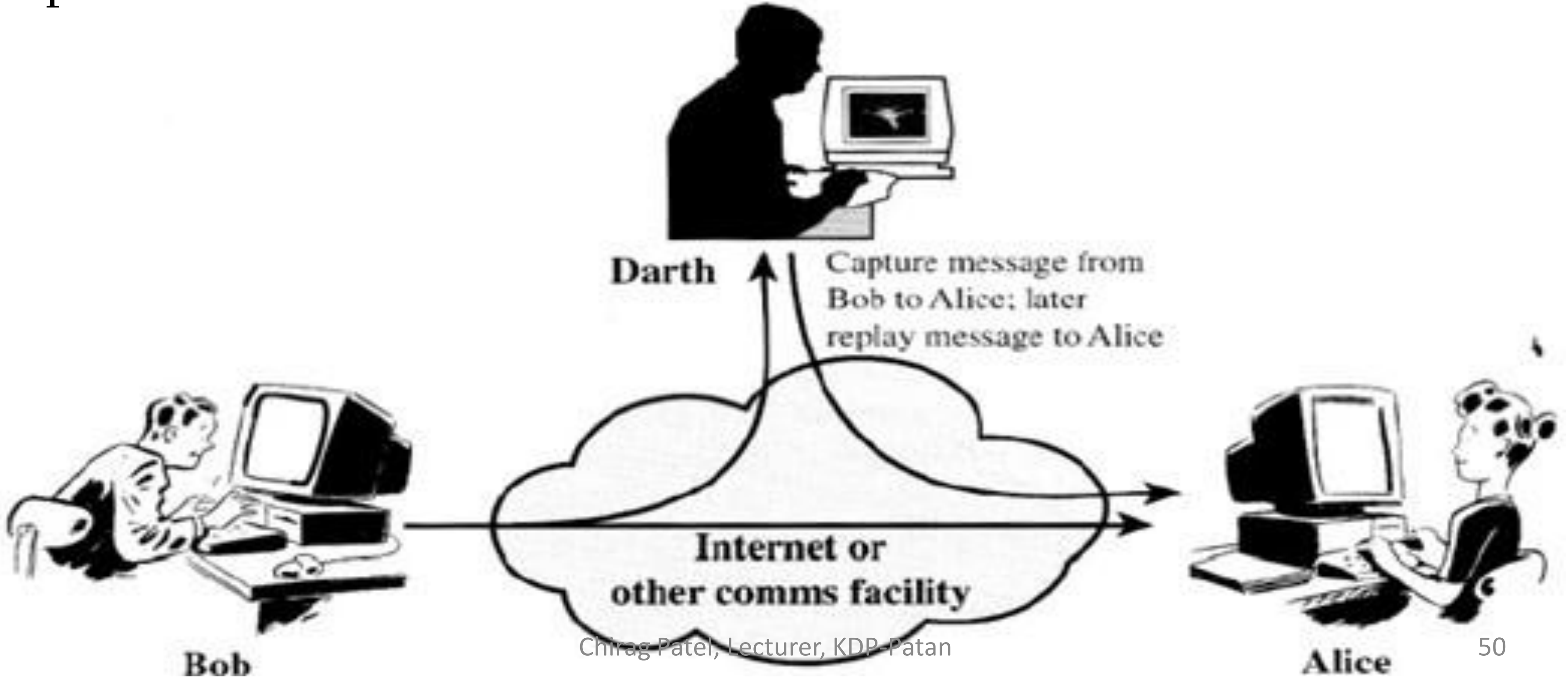
1.4 Types of Attack

- **B) Modification of message:**
- Modification of message means that some portion of a authentic message is changed, or the message is delayed or reordered, to produce an unauthorized effect.


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

1.4 Types of Attack

- **C) Message Reply:**
- In this attack, there is a reuse of captured data at a later time.
- Data transmission is not only taken but retransmitted later to produce an unauthorized effect.

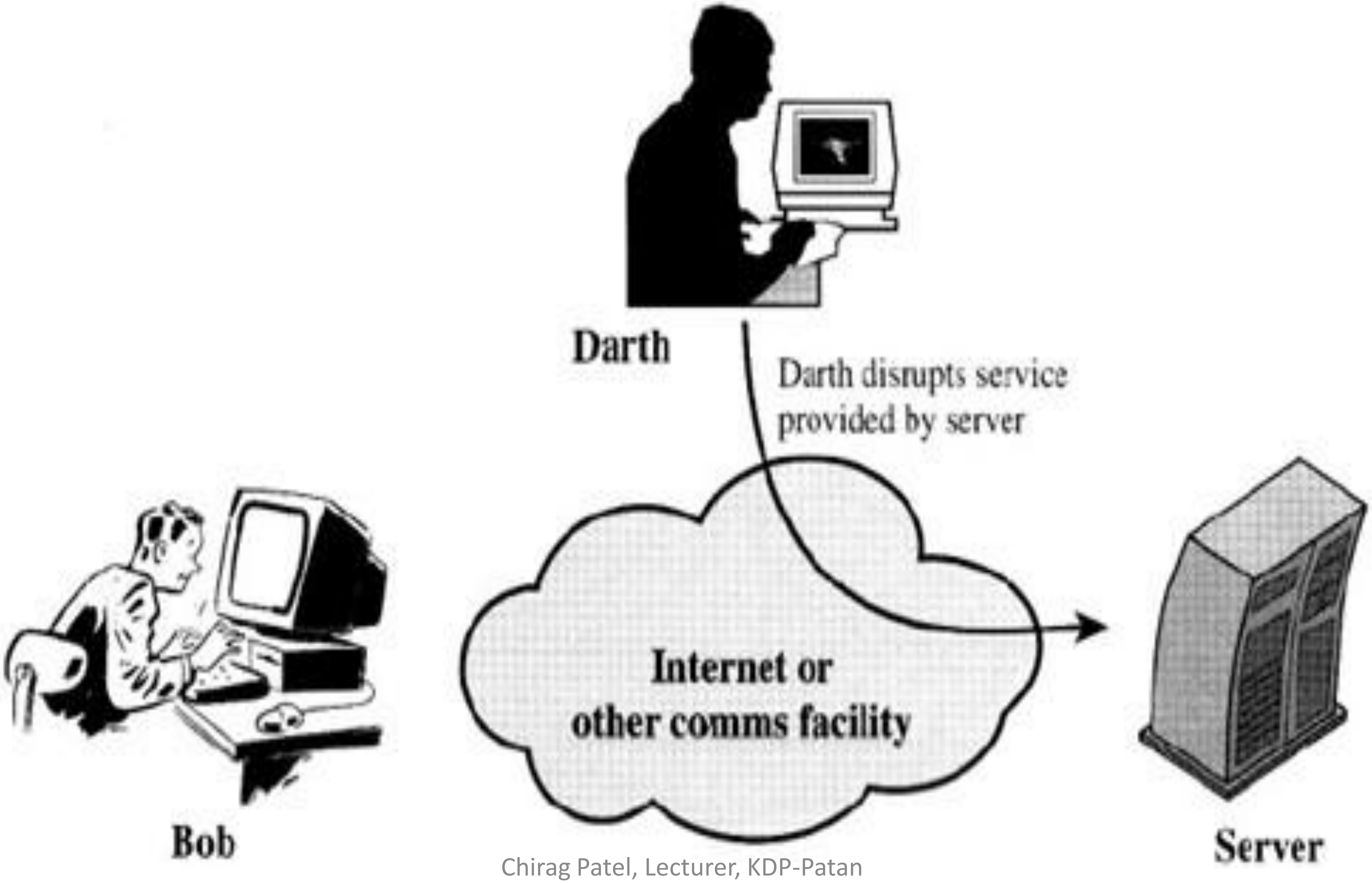

Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

1.4 Types of Attack

- **D) Denial of service attack:**
- The denial of service stops the normal use of communication facilities.
- It try to stop authentic user from accessing some services for which they are eligible.
- DOS can interrupt the entire network.

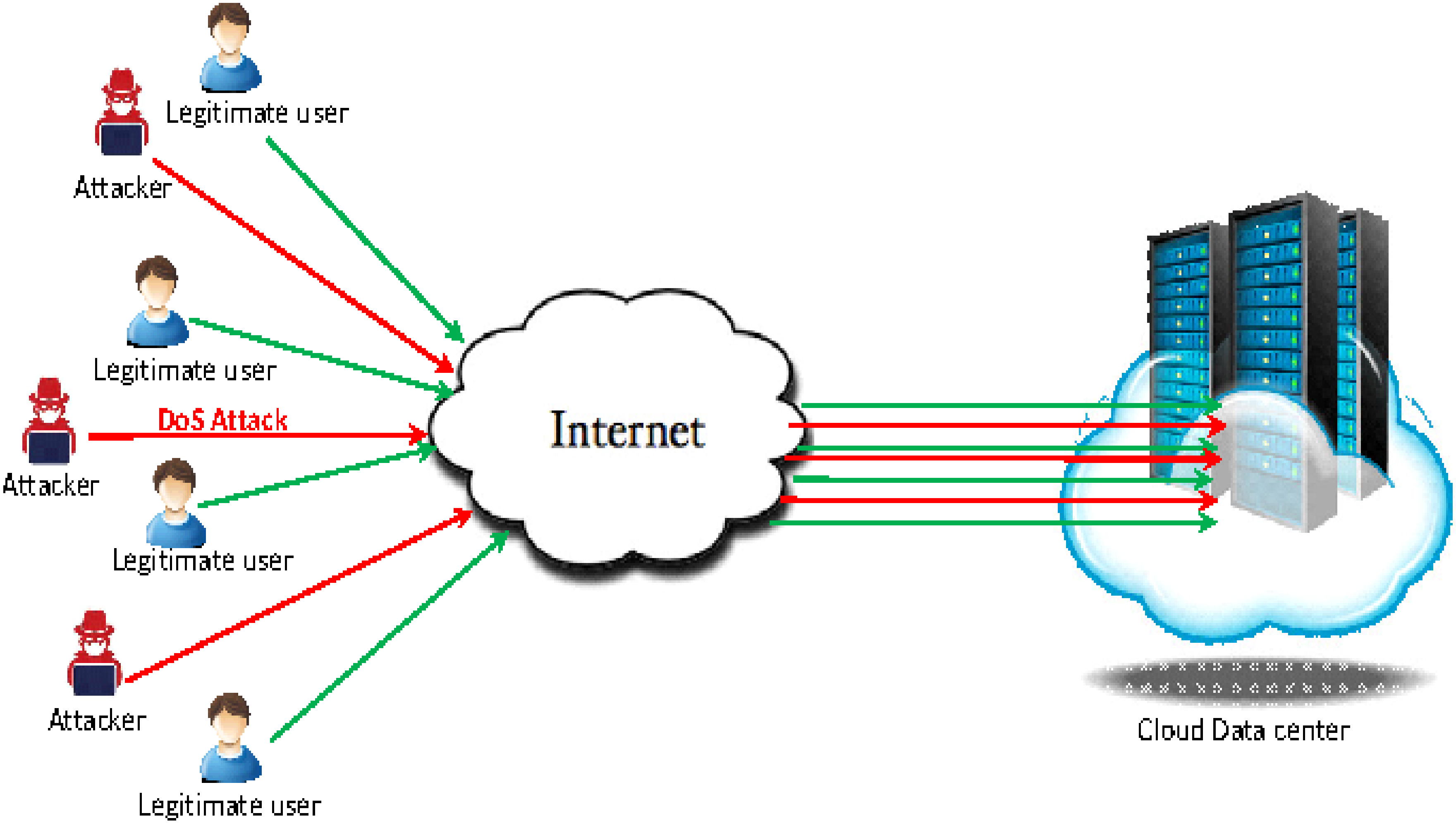
1.4 Types of Attack

- **D) Denial of service attack:**


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

1.4 Types of Attack

- **Denial of service (DOS) attack:**



1.4 Types of Attack

- Denial of Service (DOS) attacks has become **a major threat to current computer networks.**
- The denial of service stops the normal use of communication facilities.
- It try to **stop authentic user from accessing** some services for which they are eligible.
- It is designed to **crash or hang the network by flooding** it with useless traffic.
- It happens when a system, such as web server, has been flooded with illegal requests and makes it impossible to respond to real requests or tasks.

1.4 Types of Attack

- DOS **disables entire network** or **overload network with messages** so its performance get decrease.
- DOS is actually **wastage of network resources in real terms**.
- After gaining access to your network, the attacker can do any of the following:
    - Block the traffic of network.
    - Flood a computer or entire network with traffic until a shutdown occurs because of overload.
    - Send invalid data to application or network.

1.4 Types of Attack

- Results of DOS attacks are:
  - Unavailability of particular network.
  - Slow performance of network.
  - There may be flood of useless messages in your account.
- Better defenses to DOS are:
  - Filter inbound and outbound traffic.
  - Better data structure.
  - SYN cookies.

1.4 Types of Attack

- **Backdoors and Trapdoors:**
- A backdoor **is a secret entry point** into a program.
- Backdoors also known **as trapdoors**.
- Backdoors are bits of code attached in programs by programmer to quickly gain access at later time.
- They can be used at testing or debugging phase.
- A netwrok administrator may **intentionally create or install a backdoor program** for **trouble shooting or other official use.**
- Usually backdoors are useful to programmers but become threat when they are misused.

1.4 Types of Attack

- **Backdoors and Trapdoors:**
- Hackers use backdoor to install malicious software or programs.
- Hacker often plant a backdoor on previously compromised systems to gain later access.
- They are very hard to remove.
- Revise a system is better solution for backdoor.

1.4 Types of Attack

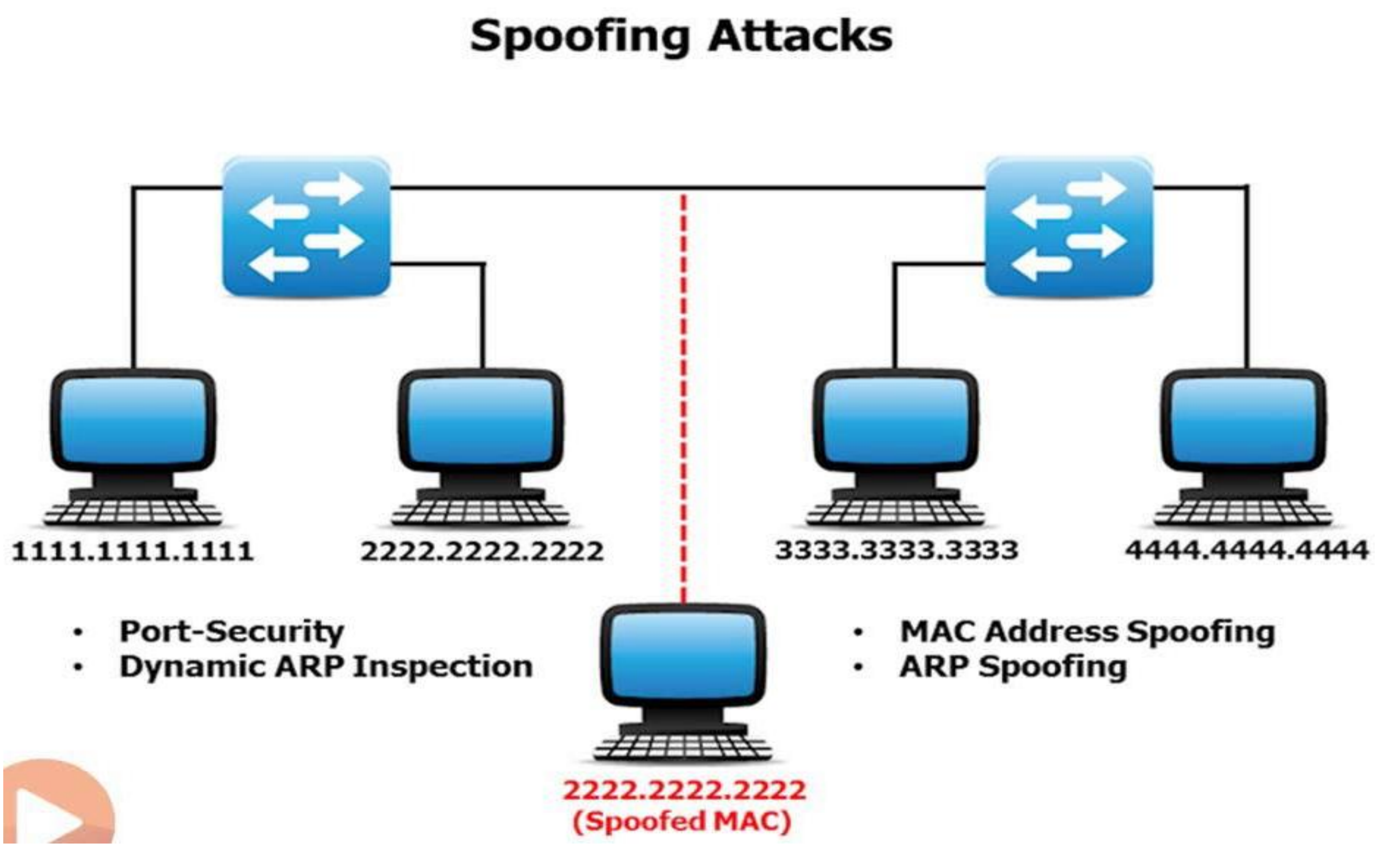
- **Sniffing:**
- Sniffer is an application or device that can **read, monitor or capture network packets or network data.**
- Sniffer are also known as **network analyzer**.
- **“The process used by attacker to capture network traffic using sniffer is called sniffing.”**
- Sniffers are used by hackers to capture sensitive network information, such as password, account information etc.
- Sniffing generally referred as “passive” attack, where attackers can be silent/invisible in the network.

1.4 Types of Attack

- **Sniffing:**
- To prevent these attacks:
  - The data that is travelling can be encrypted.
  - Transmission link can be encoded.
- Example of sniffers are: Wireshark, Dsniff, Sniffit etc.

1.4 Types of Attack

- **Spoofing:**



1.4 Types of Attack

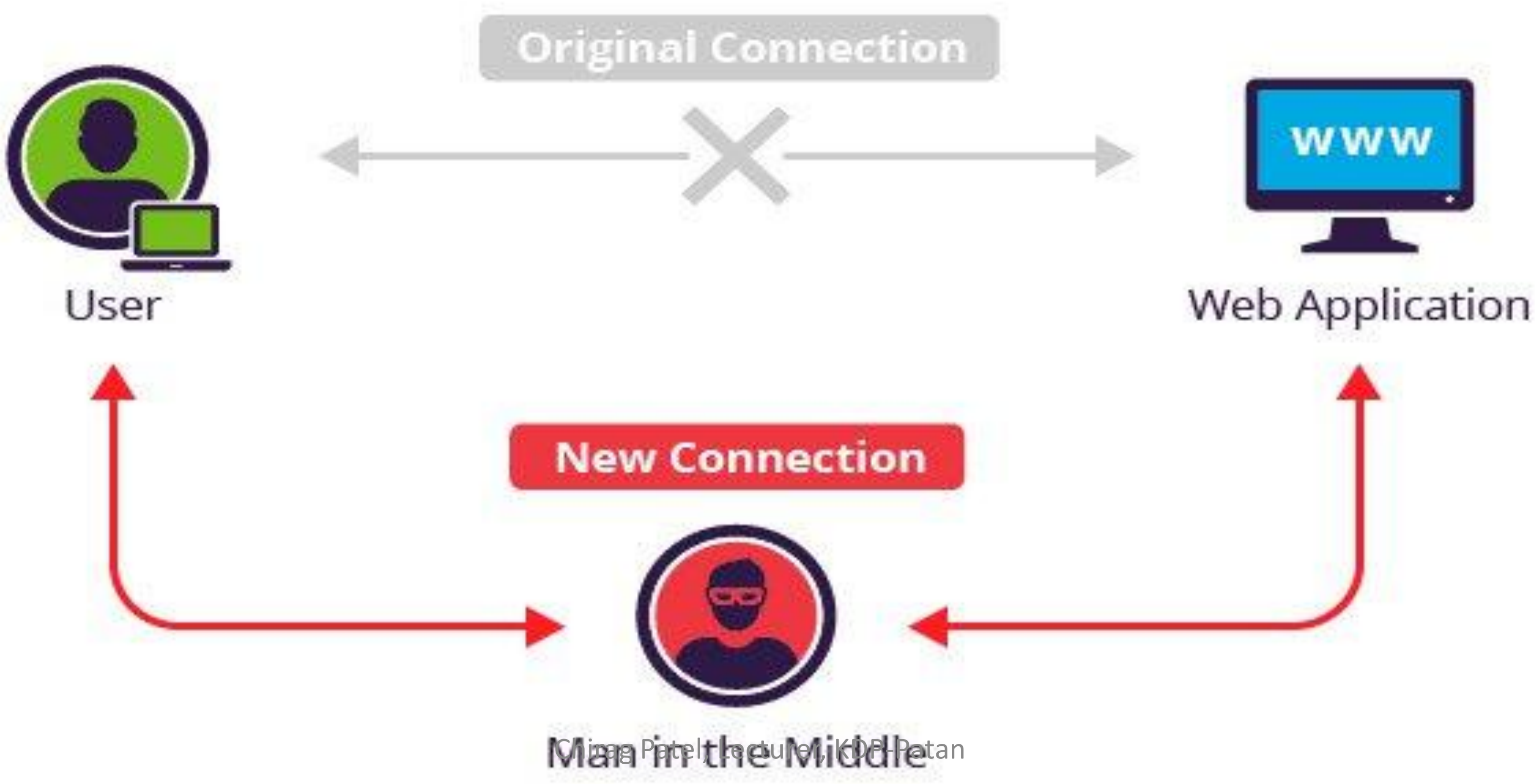
- **Spoofing:**
- Spoofing is done **when an attacker pretends to be someone else**.
- Spoofing can be done by faking an identity, such as email spoofing, IP spoofing.
- Spoofing is also called as **IP spoofing or Identity spoofing**.
- IP spoofing is done by hiding or faking a computer's IP address.
- Attacker use special programs to make IP packets that seems like originated from valid IP address.
- After getting access of the network with IP address, attacker can modify, reroute or delete data.

1.4 Types of Attack

- **Spoofing:**
- E-mail spoofing involves sending messages from a bogus e-mail address or faking the e-mail address of another user.
- DOS attack often use IP spoofing.
- Solution to this attack are:
  - Packet filtering
  - Use appropriate network protocol

1.4 Types of Attack

- **Man In The Middle Attack:**
- In this type of attack, the attacker puts him self in between two other hosts that are communicating.



1.4 Types of Attack

- **Man In The Middle Attack:**
- In this type of attack, attacker assumes your identity, tries to read your data and replies to your opponent as you.
- The person on other end might believe that its you.
- In MITM, attacker can get traffic, block traffic or delay traffic.
- Solution for this attack is to use cryptographic protocol like SSL.

1.4 Types of Attack

- **Reply Attack:**
- It involves **passive capture of data** and **replies it later** on to produce unauthorized effect.
- A reply attack is also known **as Play Back attack.**
- Ex. Suppose in communication of A and B, A sends key to B to prove his identity.
- But C listens the conversation and keeps information which are needed to prove his identity to B.
- Later C contacts B and prove his authenticity.
- This attack can be prevented using strong digital signature that includes time stamp keys.

1.4 Types of Attack

- **TCP/IP hacking:**
- TCP/IP hacking means **getting the control of an already existing session between client and a server.**
- Main advantage to attacker is that he/she doesn’t have to pass through any authentic mechanism.
- Attacker starts his work after the user completes the authentication process.
- Then attacker performs DOS attack and slows down the system.
- This type of attack generally used in **web and telnet session**.

1.4 Types of Attack

- **TCP/IP hacking:**
- To protect from TCP/IP hacking:
  - Ensure your wireless network uses WPA encryption.
  - Provide a VPN to your users when they are away from the office.
  - Be very careful with your organization’s social networking account.

1.4 Types of Attack

- **Phishing:**
- Phishing is same as fishing in a lake, here phishers attempt to take your personal information.
- Phishing is use of fake e-mails or instant messages that appear to be genuine but are designed to trick users.
- The main goal of phishing is to obtain user information that can be used as an attack.
- A complete phishing attack involves three roles of phishers.
- **First :** mailers send large number of fake emails, which direct users to fake websites.

1.4 Types of Attack

- **Second:** Phishers set up fake website, which prompts user to provide confidential information.
- **Third:** Phishers use the confidential information to achieve a pay-out.
- **Types of Phishing:**
- **Clone phishing:** In which phisher creates cloned emails and doing malicious activities.
- **By using phone apps:** Latest smart phones are not fully secure.
- API and applications can be used to fool customers.
- **Tab nabbing:** This is one of the more recent types of phishing attack.

1.4 Types of Attack

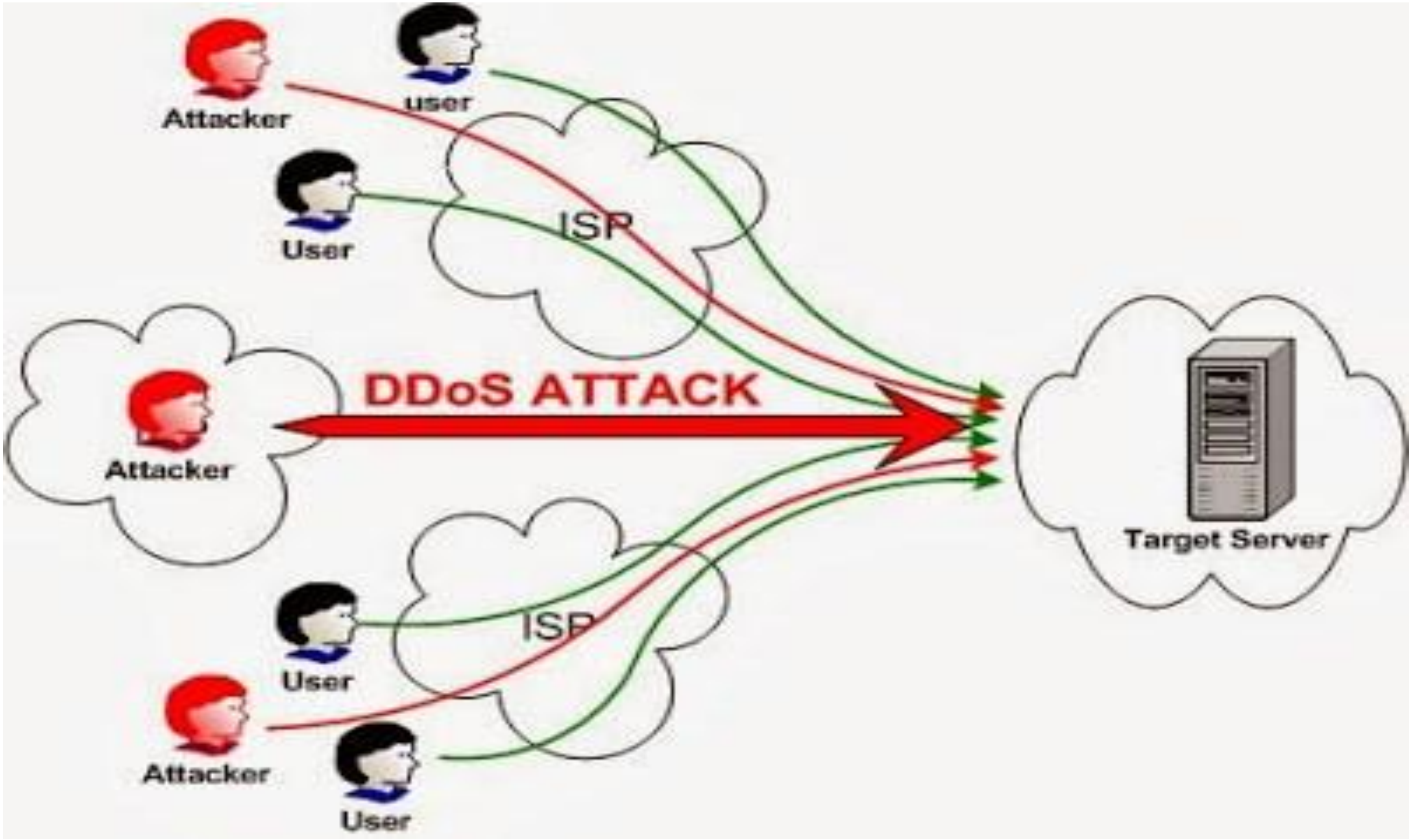
- It take advantage of people who have multiple tabs open at any one time.
- Phisher gets information of their popular websites through cookies.
- Then hacker creates page same as website and asks credentials from users.
- To prevent phishing:
  - Do not respond to suspicious email.
  - Use dedicated system for payments.
  - Use strong authentication mechanism for payment.
  - Use reputed websites only.

1.4 Types of Attack

- **DDOS:**
- DDOS stands for **D**istributed **D**enial **o**f **S**ervice attack.
- A DDOS is where the attack source is more than one, sometimes thousands of IP attacks one target.
- A DDOS attack is the attack where a collection of system perform a DOS attack on single target.
- Now a days, such attacks are essentially launched using botnets.
- DDOS consumes network bandwidth.
- DDOS attack is much harder to detect as there is no single attacker to defend from.

1.4 Types of Attack

- **DDOS:**



1.4 Types of Attack

DOS	DDOS
Full form of DOS is Denial Of Service.	Full form of DDOS is Distributed Denial Of Service attack.
It is basically is just sending requests to a server continuously and stop server from answering other request.	It is same as DOS attack but it is performed by multiple computers towards the same target.
DOS attack uses one computer and one internet connection.	DDOS attack uses multiple computers and internet connections.
DOS is less harder to detect than DDOS.	It is much harder to detect compare to DOS.
It is less costly compare to DDOS.	It is more costly than DOS.

1.4 Types of Attack

- **SQL injection:**
- SQL injection is type of attack in which an attacker injects some SQL codes in place of original codes to get access the database.
- SQL injection is common weakness found in web applications.
- It is the type of attack that takes advantage of improper coding of your web applications.
- Insufficient input validation and improper construction of SQL statements in web application can expose them to SQL injection attacks.
- Using SQL injection attack, an attacker can:
  - Add new data to the database.

1.4 Types of Attack

  - Modify the current data in the database.
  - Cause the entire database to be deleted.
- SQL injections can generally used to perform the following types of attacks:
- Authentication bypass: An attacker can use SQL injection to bypass authentication process.
- Information Expose: It allows attacker to get sensitive information in database directly or indirectly.
- SQL injection allows users to gain access of unauthorized access.
- Attacker can modify or delete data for which they are not authorized.

1.4 Types of Attack

- **Malware:**
- Malware is abbreviated term of “Malicious Software”.
- Malware is any program or file that is harmful to a computer system.
- There are various types of malware including spyware, key loggers, true viruses, worms, root kit etc.
- Various factors can make computers more weak to malware attacks, including defects in OS design, giving too much permissions etc.
- For the protection from the malware:
- Be careful about what email attachment you open.
- Be careful while surfing and stay away from doubtful websites.
- Maintain updated quality of an antivirus.

1.4 Types of Attack

- **Logic bomb:**
- It is a computer virus that remains hidden until it is triggered.
- It is also called “Slag Code”.
- It needs host program to execute.
- It doesn’t replicate itself.
- Once logic bomb is triggered, that can perform any number of malicious activities.
- Logic bombs are very difficult to detect before they are triggered.
- An attacker can easily insert three or four lines of computer code into a long program without anyone detecting the insertion.

1.4 Types of Attack

- Prevention to logic bombs:
- Do not download pirated software.
- Be careful with installing freeware applications.
- Be careful when opening email attachments.
- Do not click on suspicious web links.
- Always update your antivirus software.

1.4 Types of Attack

- **Trojan horse:**
- Trojan horse also called as Trojans.
- It is kind of program that appears harmless, but is actually malicious.
- It is a program that contains hidden codes when invoked, perform some unwanted or malicious activities.
- It does not replicate itself.
- It needs host program to execute.
- The main purpose of Trojans is to release information to attackers.
- Trojans often used to spread a virus/worms or to install a backdoor or to simply destroy data.

1.4 Types of Attack

- To prevent from Trojans:
- Never open unwelcome emails from unknown senders.
- Avoid downloading and installing programs unless you fully trust the publisher.
- Use appropriate and licensed antivirus and firewall software.
- Ensure that your operating system always be up to date.

****