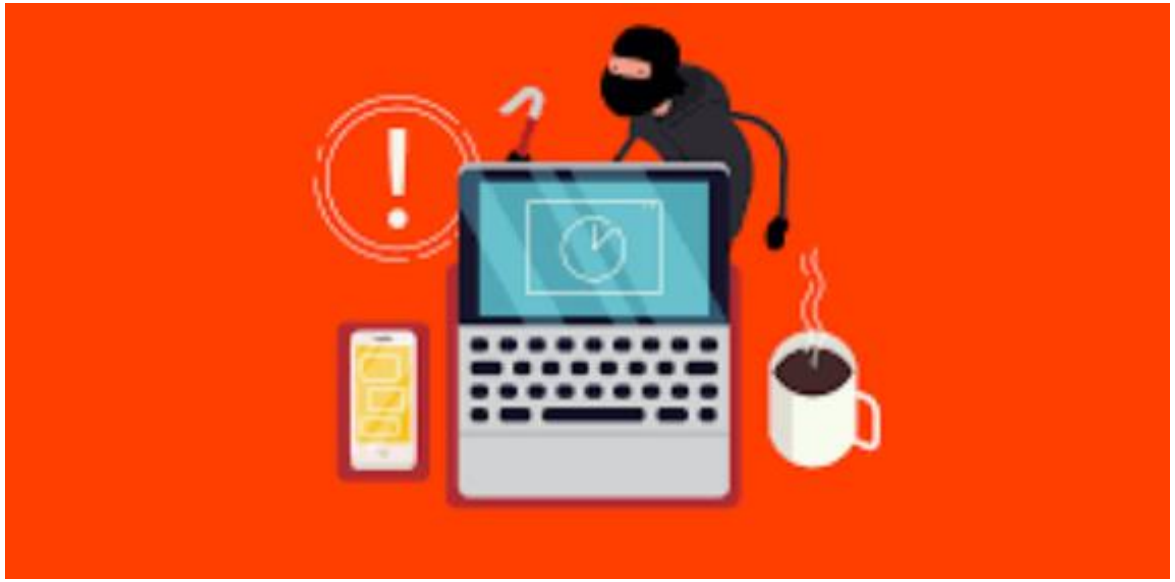
# Unit-03 Tools and Methods Used in Cybercrime



# Basic Stages of Attack

**1. Initial uncovering:**

1. In the first step called as *reconnaissance*, the attacker gathers information, as much as possible, about the target by legitimate means.
2. In the second step, the attacker uncovers as much information as possible on the company's internal network.

**2. Network probe:** A "ping sweep" of the network IP addresses is performed to seek out potential targets, and then a "port scanning" tool is used to discover exactly which services are running on the target system.

**3. Crossing the line toward electronic crime (E-crime):** Now the attacker is toward committing what is technically a "computer crime" by exploiting possible holes on the target system.

**4. Capturing the network:** At this stage, the attacker attempts to "own" the network. The attacker gains a foothold in the internal network quickly and easily.

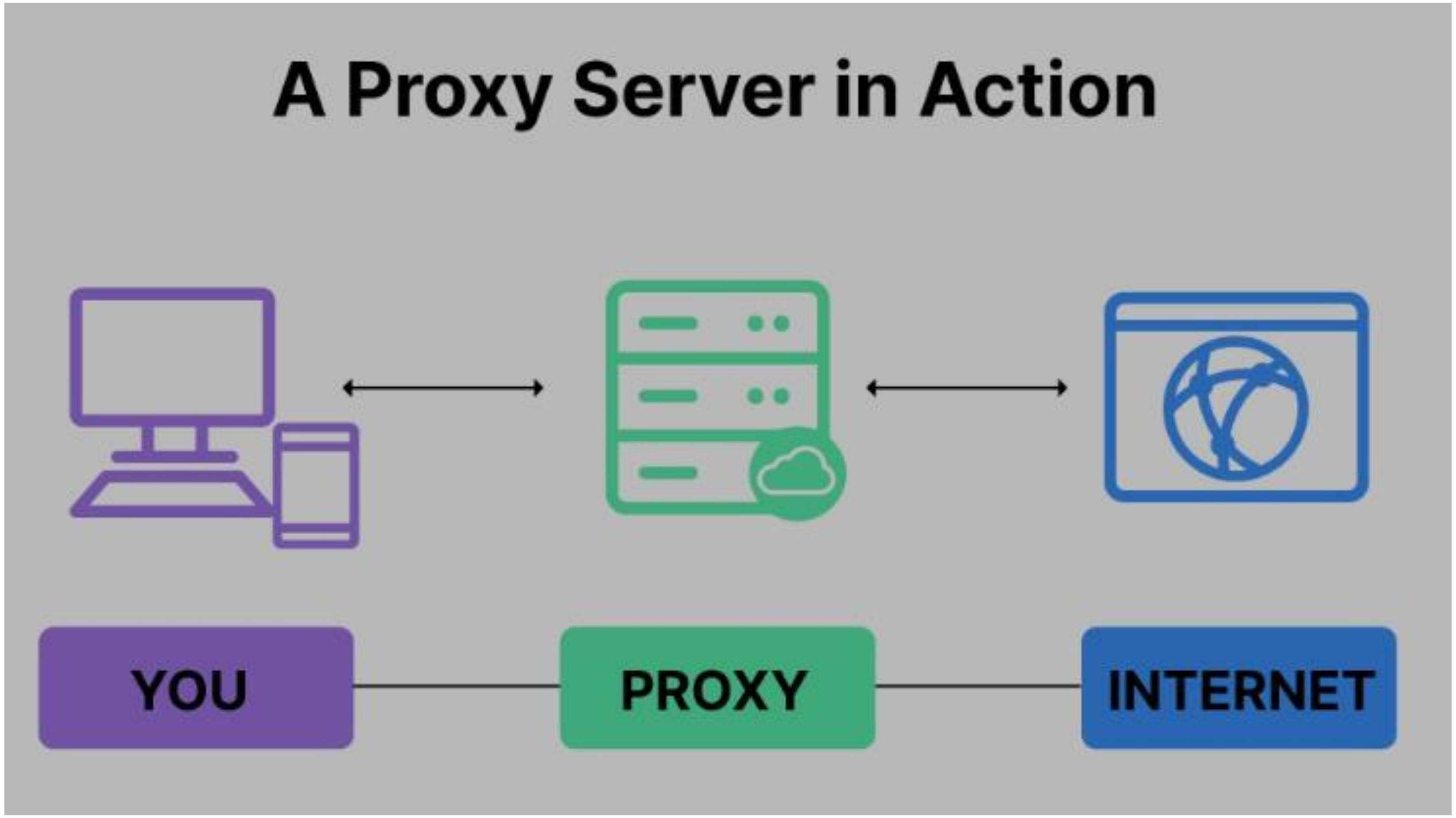
**5. Grab the data:** Now that the attacker has "captured the network," he/she takes advantage of his/her position to steal confidential data, customer credit card information, deface webpages, alter processes and even launch attacks at other sites from your network.

**6. Covering tracks:** This is the last step in any cyberattack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected.

# Types of Attacks

- Scareware:-
- Malvertising
- Clickjacking
- Ransomware

# Proxy Server

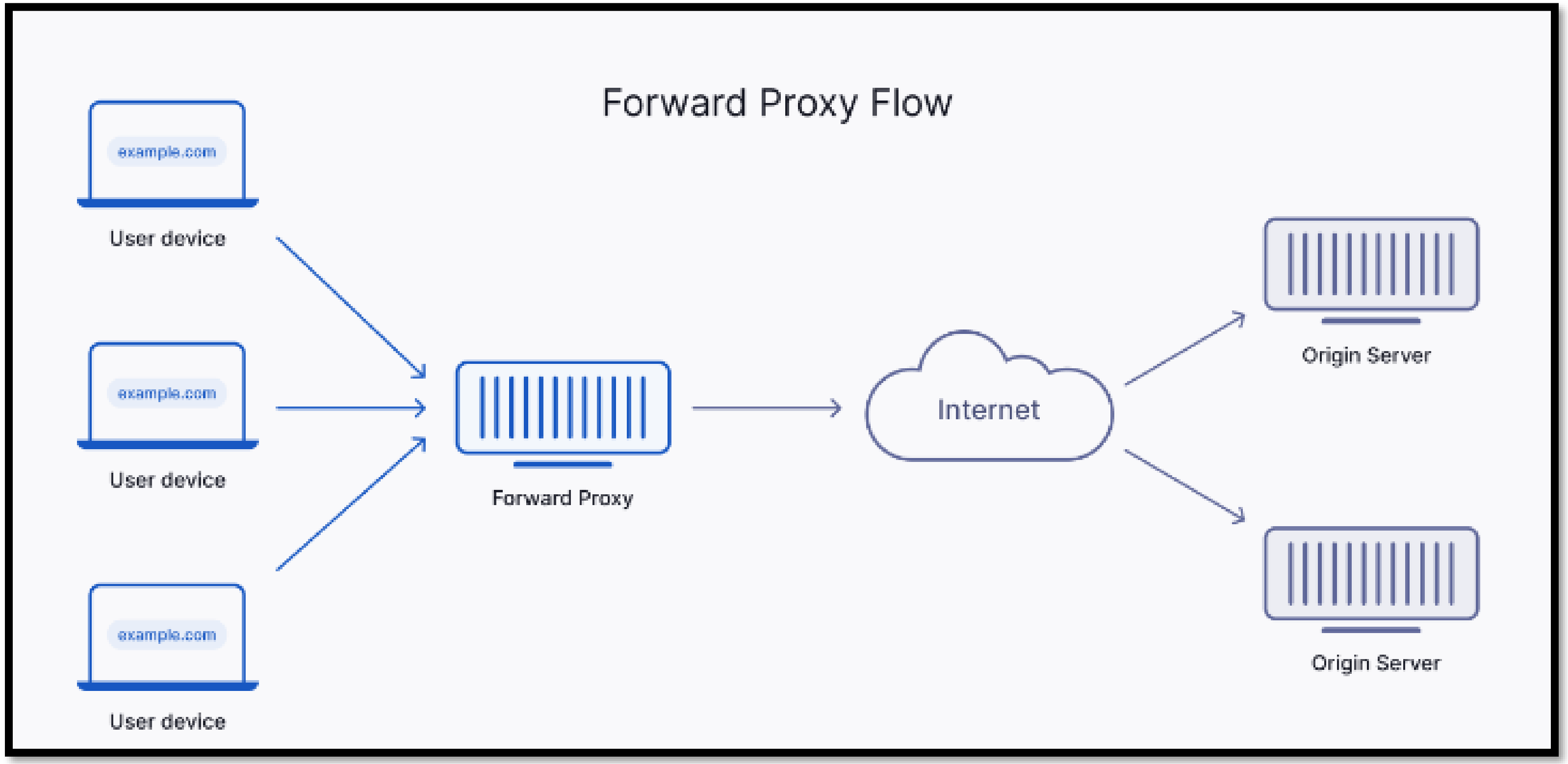


# Proxy Server

- *Proxy server* is a computer on a network which acts as an intermediary for connections with other computers on that network.
- Proxy server refers to a server that acts as an intermediary between the request made by clients, and a particular server for some services or requests for some resources.
- There are different types of proxy servers available that are put into use according to the purpose of a request made by the clients to the servers.

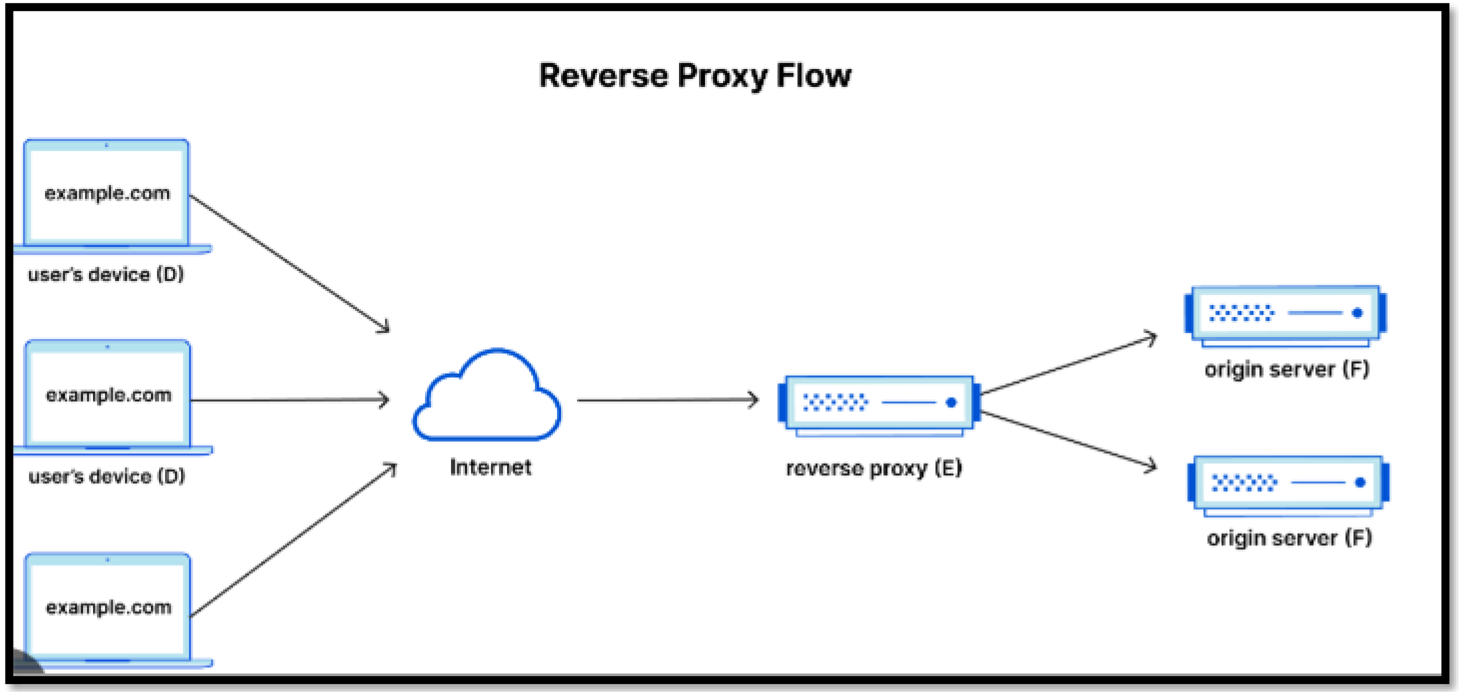
# Types of Proxy Servers

## Forward Proxy:-



# Types of Proxy Servers

## Reverse Proxy:-

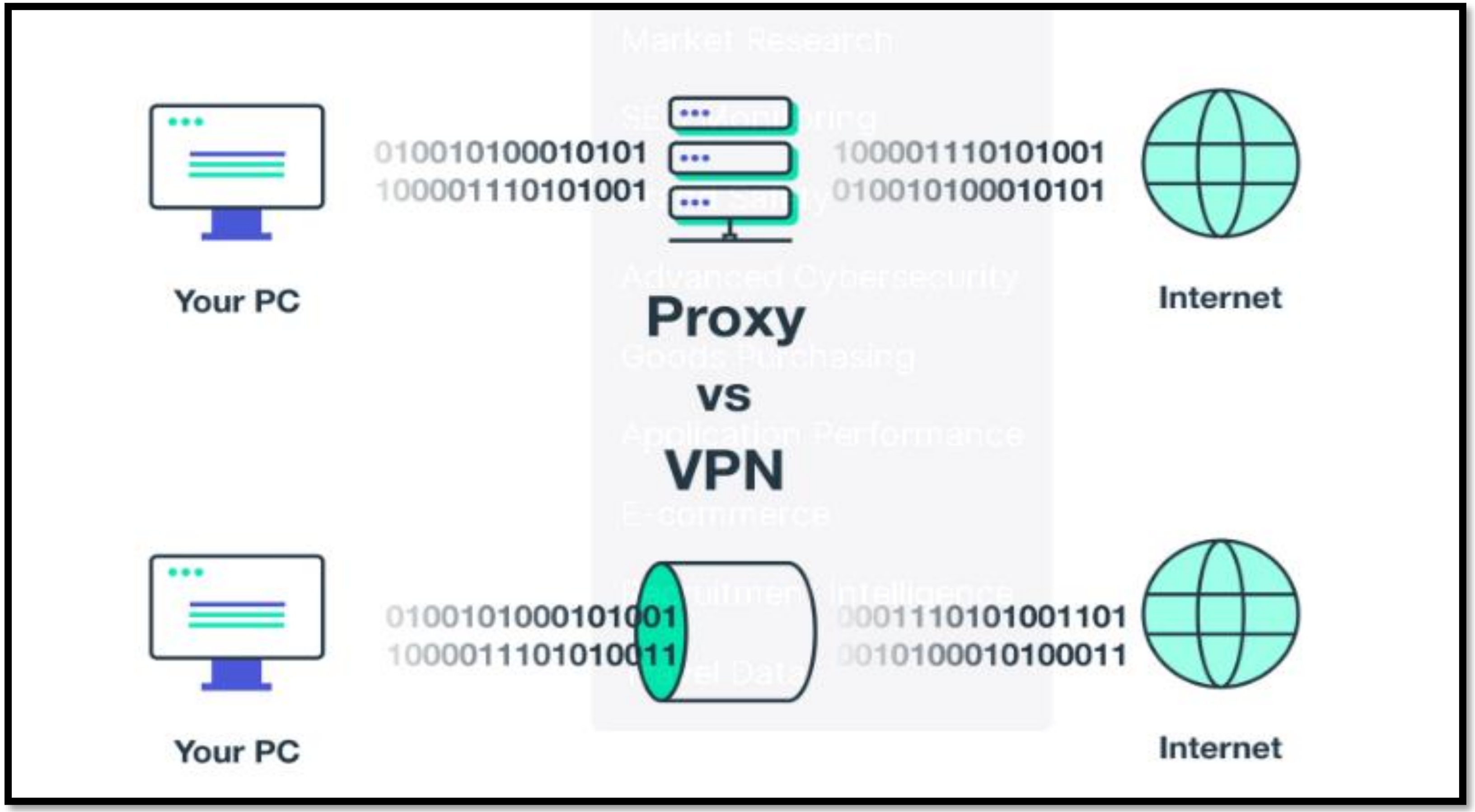


# Types of Proxy Servers

**Anonymous  Proxy:-**

- An anonymous proxy keeps private the browsing history
- Helps to avoid content blocks and targeted marketing, and it blocks online ads
- Provides access to geo-restricted websites
- Runs automated tasks
- It speeds up loading times when caching configuration is set up.

# Difference between Proxy and VPN



# Proxy Servers and Anonymizers

r

A proxy server has following purposes:

- Keep the systems behind the curtain.
- Speed up access to a resource (through “caching”).
- Specialized proxy servers are used to filter unwanted content such as advertisements.
- Proxy server can be used as IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address.
- An anonymous proxy is a tool that attempts to make activity on the Internet untraceable.
- It accesses the Internet on the user’s behalf, protecting personal information by hiding the source computer’s identifying information.

# Phishing Works

**Phishing**

Phishing is a fake or false e-mail which can infect systems with  in addition to stealing personal and financial data.

**How Phishing Works?**

Phishers work in the following ways:

- Planning (decide the target)
- Setup (create methods for delivering the message and to collect the data about the target)
- Attack **(**phisher sends a phony message**)**
- Collection **(**record the information of victims**)**
- Identity theft and fraud **(**use the information that they have gathered to make illegal purchases or commit fraud**).**

# Password Cracking

Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system. Examples of guessable passwords include:

**1.** Blank (none);

**2.** the words like “password,” “passcode” and “admin”;

**3.** series of letters from the “QWERTY” keyboard, for example, qwerty, asdf or qwertyuiop;

**4.** user’s name or login name;

**5.** name of user’s friend/relative/pet;

**6.** user’s birthplace or date of birth, or a relative’s or a friend’s;

**7.** user’s vehicle number, office number, residence number or mobile number;

**8.** name of a celebrity who is considered to be an idol (e.g., actors, actress, spiritual gurus) by the user;

**9.** simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.

# Password Cracking

Password cracking attacks can be classified under three categories as follows:

**1.** Online attacks;

**2.** Offline attacks;

**3.** Non-electronic attacks (e.g., social engineering, shoulder surfing and dumpster diving).

## Online Attacks

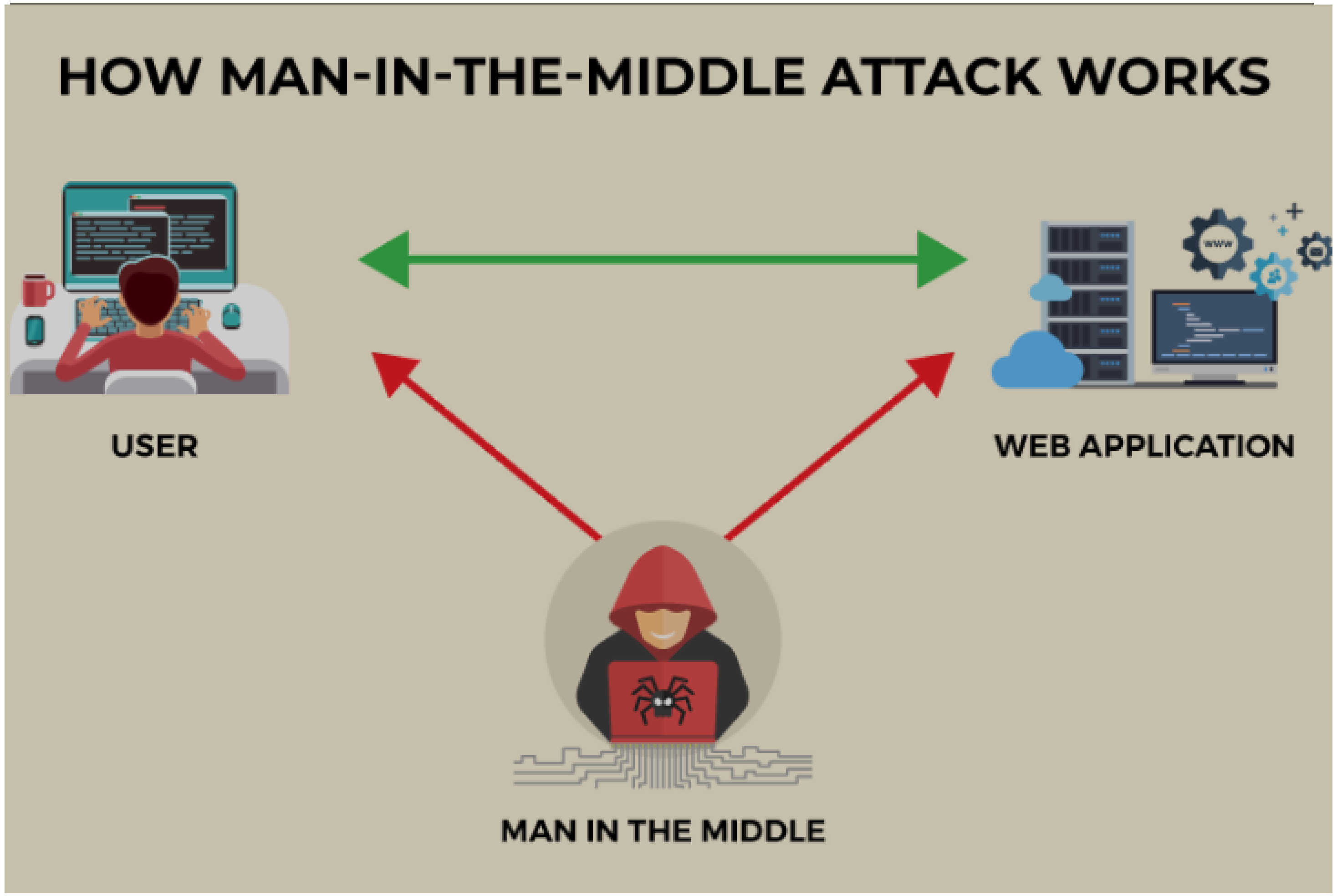
- The most popular online attack is man-in-the middle (MITM) attack, also termed as “bucket-brigade attack” or sometimes “Janus attack.”

- It is a form of active eavesdropping in which the attacker establishes a connection between a victim and the server to which a victim is connected.

## Offline Attacks

- Offline attacks usually require physical access to the computer and copying the password file from the system onto removable media.

# MITM


HOW MAN-IN-THE-MIDDLE ATTACK WORKS
USER
WEB APPLICATION
MAN IN THE MIDDLE

# Password Cracking

**Strong, Weak and Random Passwords**

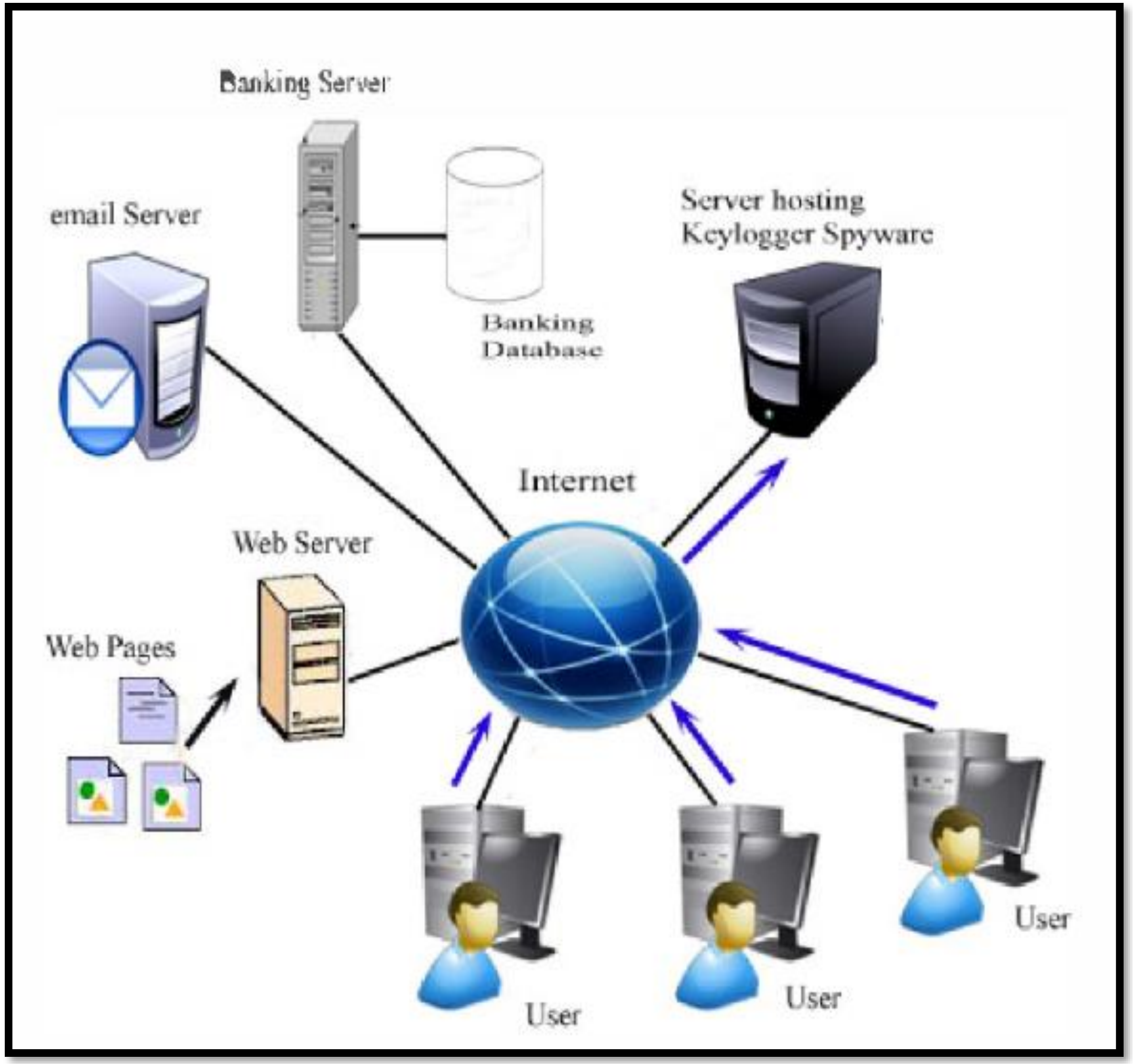
- A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found by executing a brute force attack and by using a subset of all possible passwords.
- A strong password is long enough, random or otherwise difficult to guess – producible only by the user who chooses it.

**Random Passwords**

- Password is stronger if it includes a mix of upper and lower case letters, numbers and other symbols, when allowed, for the same number of characters.

# Keyloggers and Spywares

- Keystroke logging- practice of noting (or logging) the keys struck on a keyboard.
- Keystroke logger or keylogger is quicker and easier way of capturing the passwords and monitoring the victims' IT savvy behavior.
- It can be classified as **software keylogger** and **hardware keylogger**.



# Keyloggers and Spywares

## Software Keyloggers

- Software keyloggers are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded.
- A keylogger usually consists of two files that get installed in the same directory: a dynamic link library (DLL) file and an EXEcutable (EXE) file that installs the DLL file and triggers it to work.

## Hardware Keyloggers

- Hardware keyloggers are small hardware devices connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device.
- These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

# Keyloggers and Spywares

**Anti keylogger**

- Anti keylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool.
  - Firewalls cannot detect the installations of keyloggers on the systems; hence, anti keyloggers can detect installations of keylogger.
  - This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs.
  - Prevents Internet banking frauds.
  - It prevents ID theft.
  - It secures E-Mail and instant messaging/chatting.

**Spywares**

- Spyware is malicious software secretly installed on the user’s personal computer.
- Spywares such as keyloggers are installed by the owner of a shared, corporate or public computer on purpose to secretly monitor other users.

# Virus and Worms

Computer virus is a program that can “infect” legitimate programs by modifying them to include a possibly “evolved” copy of itself.

Viruses can take some typical actions:

**1.** Display a message to prompt an action which may set of the virus

**2.** Delete files inside the system into which viruses enter

**3.** Scramble data on a hard disk

**4.** Cause erratic screen behavior

**5.** Halt the system (PC)

**6.** Just replicate themselves to propagate further harm.

# Virus and Worms

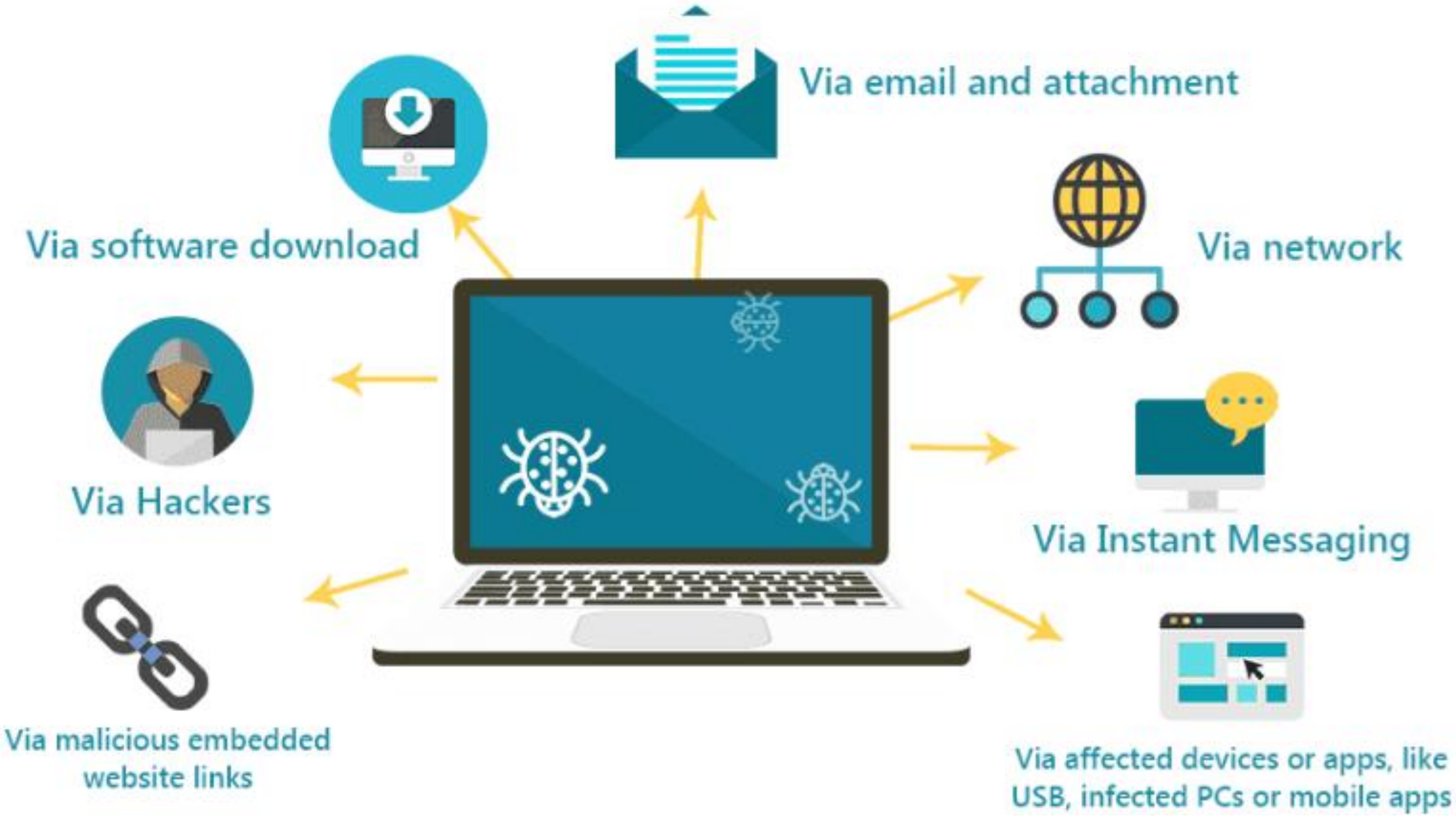
## Types of Viruses

- Computer viruses can be categorized based on attacks on various elements of the system and can put the system and personal data on the system in danger.

    1. Boot sector viruses
    2. Program viruses
    3. Multipartite viruses
    4. Stealth viruses
    5. Polymorphic viruses
    6. Macro viruses
    7. Active X and Java Control

- A **computer worm** is a self-replicating malware computer program which uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention

# How do Virus Spreads


Via software download
Via email and attachment
Via network
Via Hackers
Via Instant Messaging
Via malicious embedded website links
Via affected devices or apps, like USB, infected PCs or mobile apps

# How do Virus Spreads

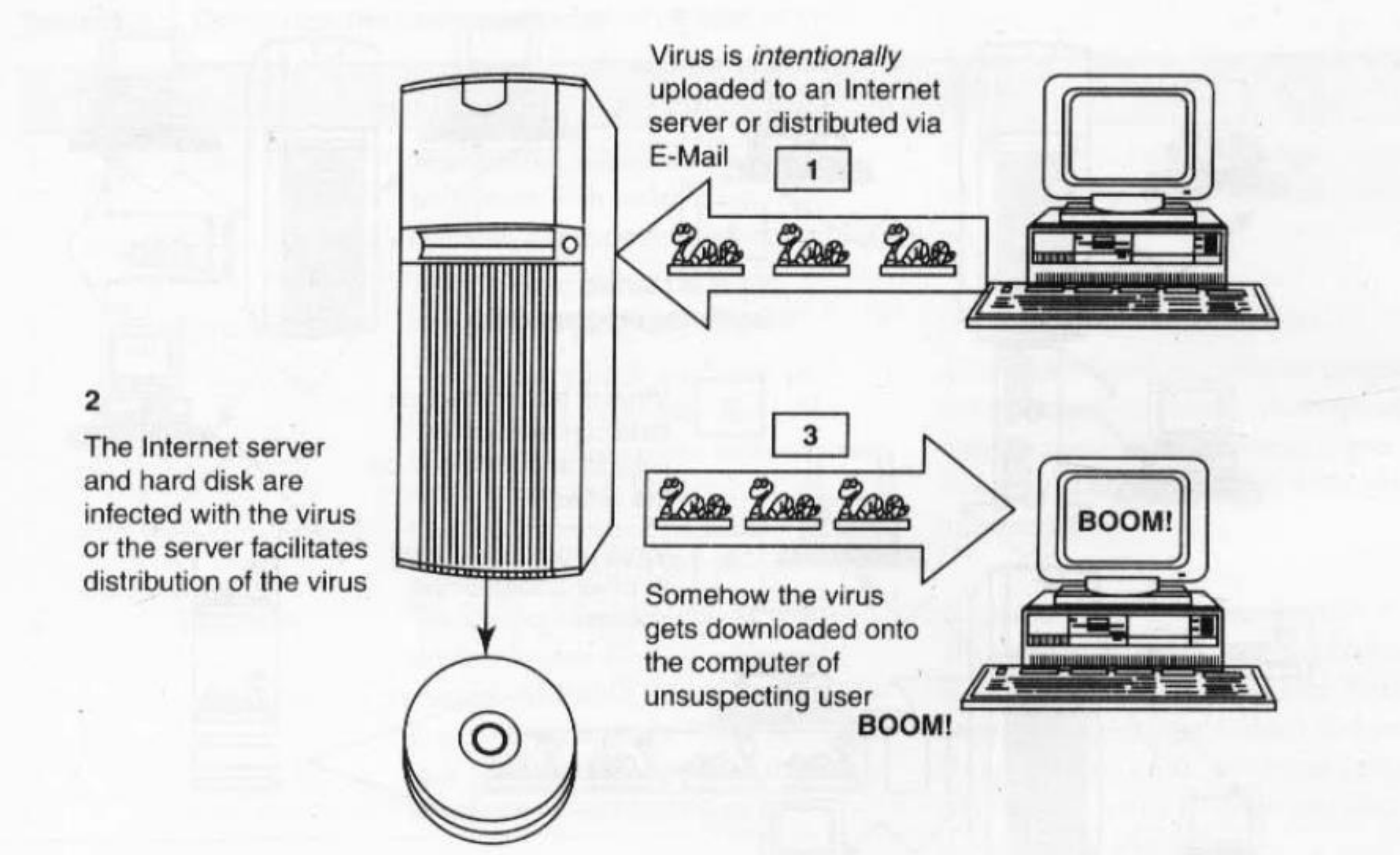

Virus is *intentionally* uploaded to an Internet server or distributed via E-Mail
1
2
The Internet server and hard disk are infected with the virus or the server facilitates distribution of the virus
3
BOOM!
Somehow the virus gets downloaded onto the computer of unsuspecting user
BOOM!

Fig : How Virus spread through Internet

# How do Virus Spreads

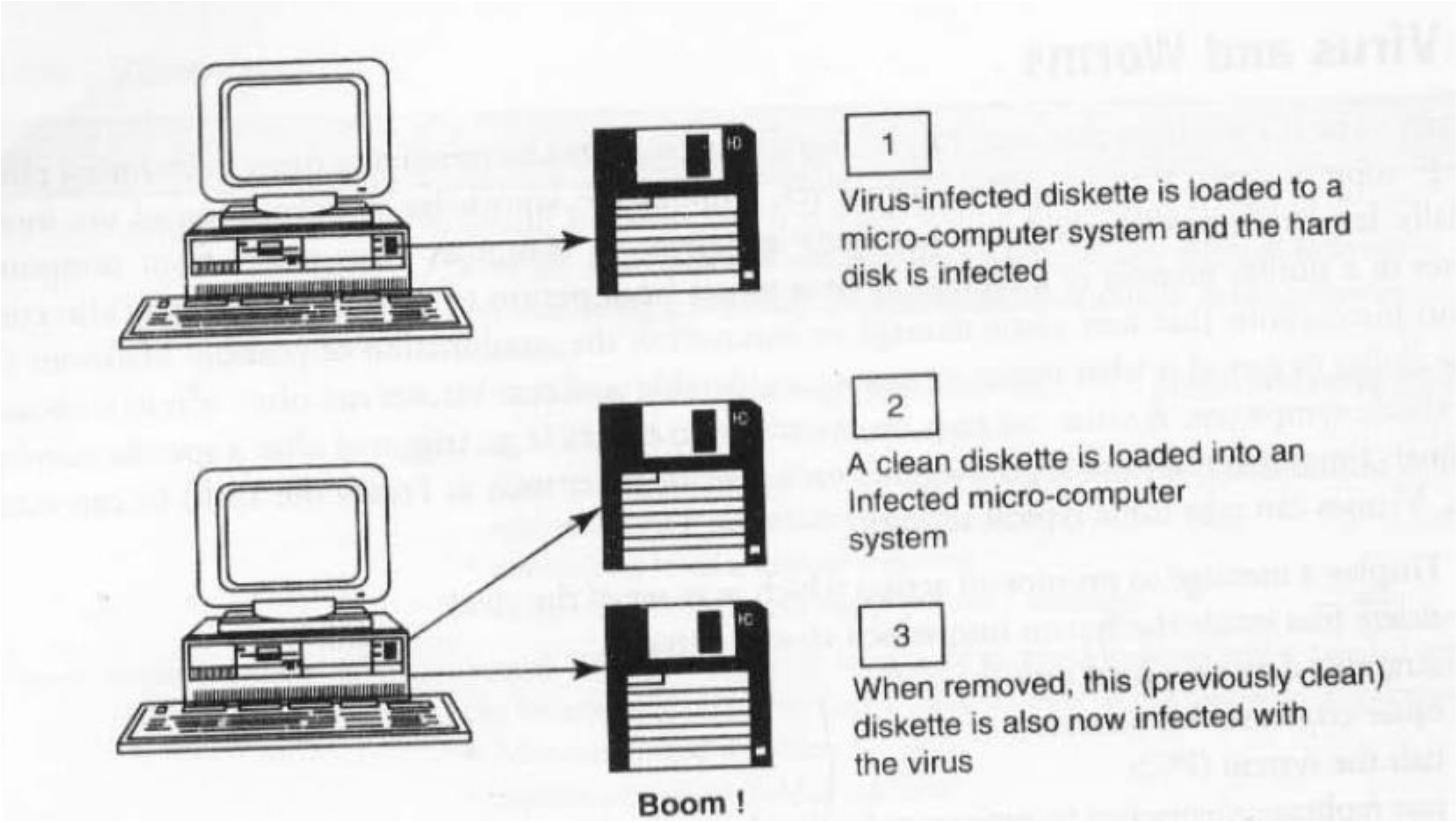

1
Virus-infected diskette is loaded to a micro-computer system and the hard disk is infected
2
A clean diskette is loaded into an Infected micro-computer system
3
When removed, this (previously clean) diskette is also now infected with the virus
Boom !

Fig : How Virus spread through stand alone system

# How do Virus Spreads

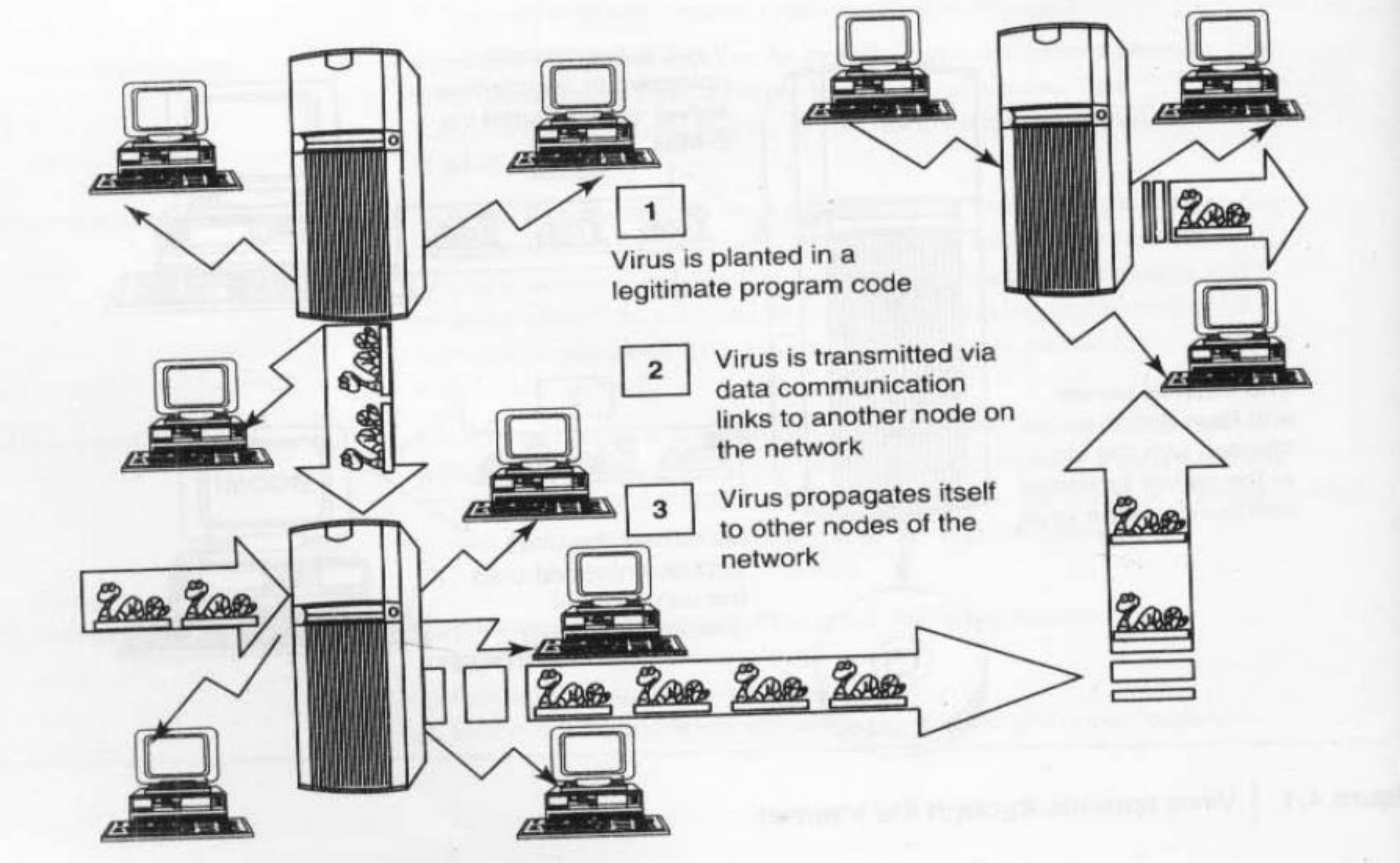

1
Virus is planted in a legitimate program code
2
Virus is transmitted via data communication links to another node on the network
3
Virus propagates itself to other nodes of the network

Fig : How Virus spread through local networks

# Types of Viruses

## 1. Boot Sector Viruses

- Infects the boot record.
- Spreads when System is booted.
- Gains control of machine before the virus detection tools can act .
- Very hard to notice.
- Carrier files: AUTOEXEC.BAT, CONFIG.SYS, IO.SYS

# Types of Viruses

## 2. Program Viruses

- Infects executable program files such as .exe, .ovl, .drv, .bin, .com.
- These programs are loaded in memory during execution, taking the virus with them.
- Program virus becomes active in memory, making copies of itself and infecting files on disk.

# Types of Viruses

### 3. Multipartite Viruses

- It is a hybrid of a boot sector and program viruses. It infects program files along with the boot record when the infected program is active.
- Victim’s local drive and other programs will be affected.

# Types of Viruses

### 4. Stealth Viruses

- Stealth virus uses can disguise itself ,so antivirus software cannot it.
- These viruses attacks operating system processes and binds to files, disk partitions and boot sectors to avoid detection.
- It alters its file size and conceals itself in the computer memory to remain in the system undetected.

# Types of Viruses-Polymorphic Viruses

- Polymorphic virus is a complicated computer virus that changes its form as it propagates to avoid detection by antivirus.
- It is a self-encrypting virus that pairs a mutation engine along with a self-propagating program code.
- A polymorphic virus corrupts data and slows down system resources, sometimes leading to computer malfunctions like blue screen errors.
- Polymorphic Generators are Dark Angel's Multiple Encryptor(DAME), Darwinian Genetic Mutation Engine(DGME) etc..

# Types of Viruses

## Macroviruses

- Many applications ,such MS word, MS Excel, support macros.
- A macro virus operates by injecting its code into macros attached to the type of popular data files associated with office work, like Microsoft Word, Excel, or PowerPoint files.
- A macro virus shares the traits of a typical computer virus. Like a regular computer virus, a macro virus needs human interaction to activate

# Trojan Horse

- Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm.

- Trojans can get into the system in a number of ways, including from a web browser, via E-Mail or in a bundle with other software downloaded from the Internet.

  - Unlike viruses or worms, Trojans do not replicate themselves but they can be equally destructive.

  - On the surface, Trojans appear benign and harmless, but once the infected code is executed, Trojans kick in and perform malicious functions to harm the computer system without the user’s knowledge.

# Backdoor

- A backdoor is a means of access to a computer program that bypasses security mechanisms.
- A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes.
- An attacker often uses backdoors that they detect or install themselves as part of an exploit.
- In some cases, a worm is designed to take advantage of a backdoor created by an earlier attack.

# What a Backdoor Does?

- It allows an attacker to create, delete, rename, copy or edit any file, execute any commands, or change system settings.

- Install arbitrary software and parasites.

- It allows the attacker to control computer hardware devices, modify related settings, and shut down and restart a computer without the user's permission.

- It steals all sensitive personal information, valuable documents, passwords, and login IDs and also tracks web browsing habits.

- It installs a hidden FTP server that can be used by malicious persons for various illegal purposes.

- It degrades internet connection speeds, and overall performance, decreases system security and causes software inability.

# Examples of Backdoor Trojans

- Back Orifice
- Bifrost
- SAP Backdoors
- Onapsis Bizploit

# How to Protect from Trojan Horses and Backdoors

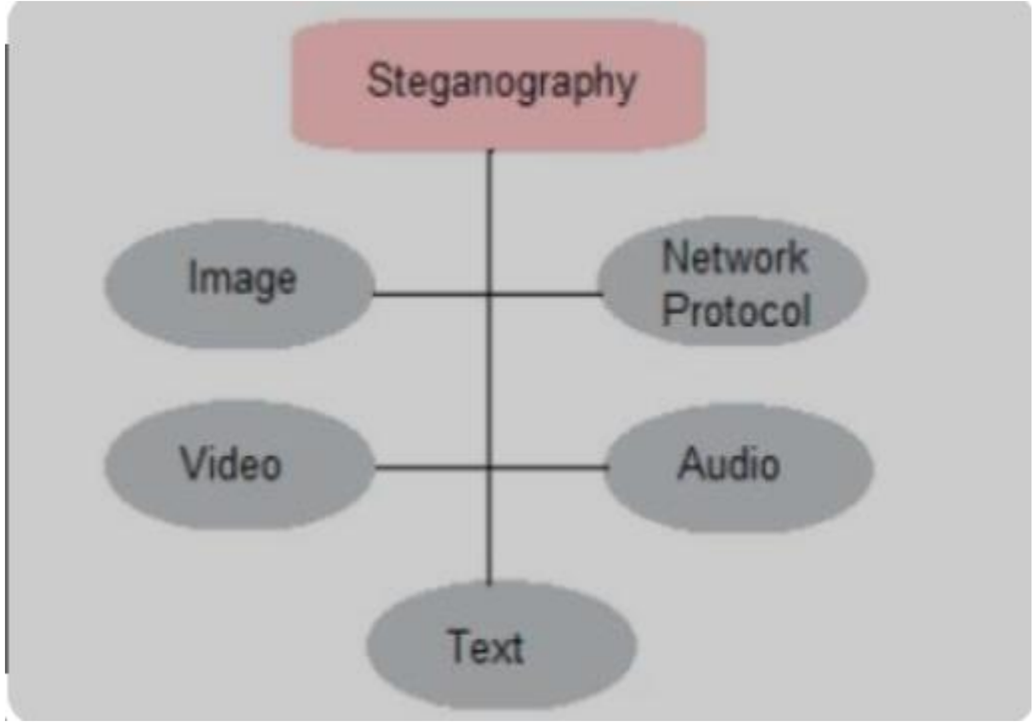
- Stay away from suspect websites/weblinks
- Surf on the Web cautiously
- Install antivirus/Trojan remover software

# Steganography

- The steganography technique involves hiding sensitive information within an ordinary, non-secret file or message so that it will not be detected.
- The sensitive information will then be extracted from the ordinary file or message at its destination, thus avoiding detection.
- Steganography is an additional step that can be used in conjunction with encryption in order to conceal or protect data.

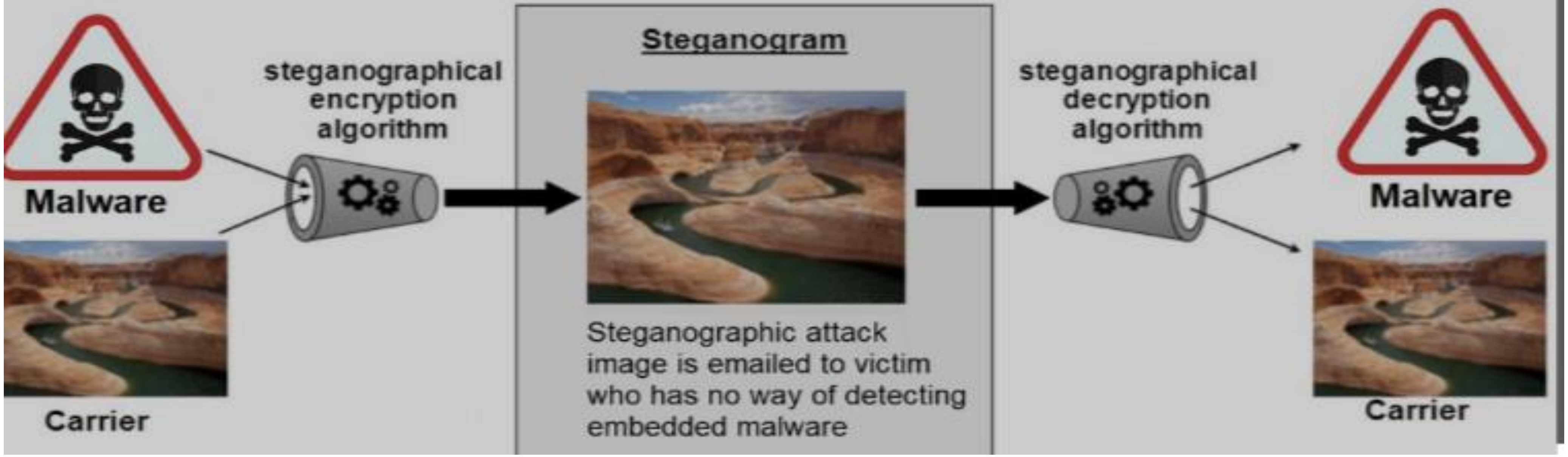
# Different Types of Steganography

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Network or Protocol Steganography



# Steganography

A steganographic attack is the art and science of embedding hidden messages or malware in a carrier medium such as an image or video file in a way the recipient does not realize the file is malicious.

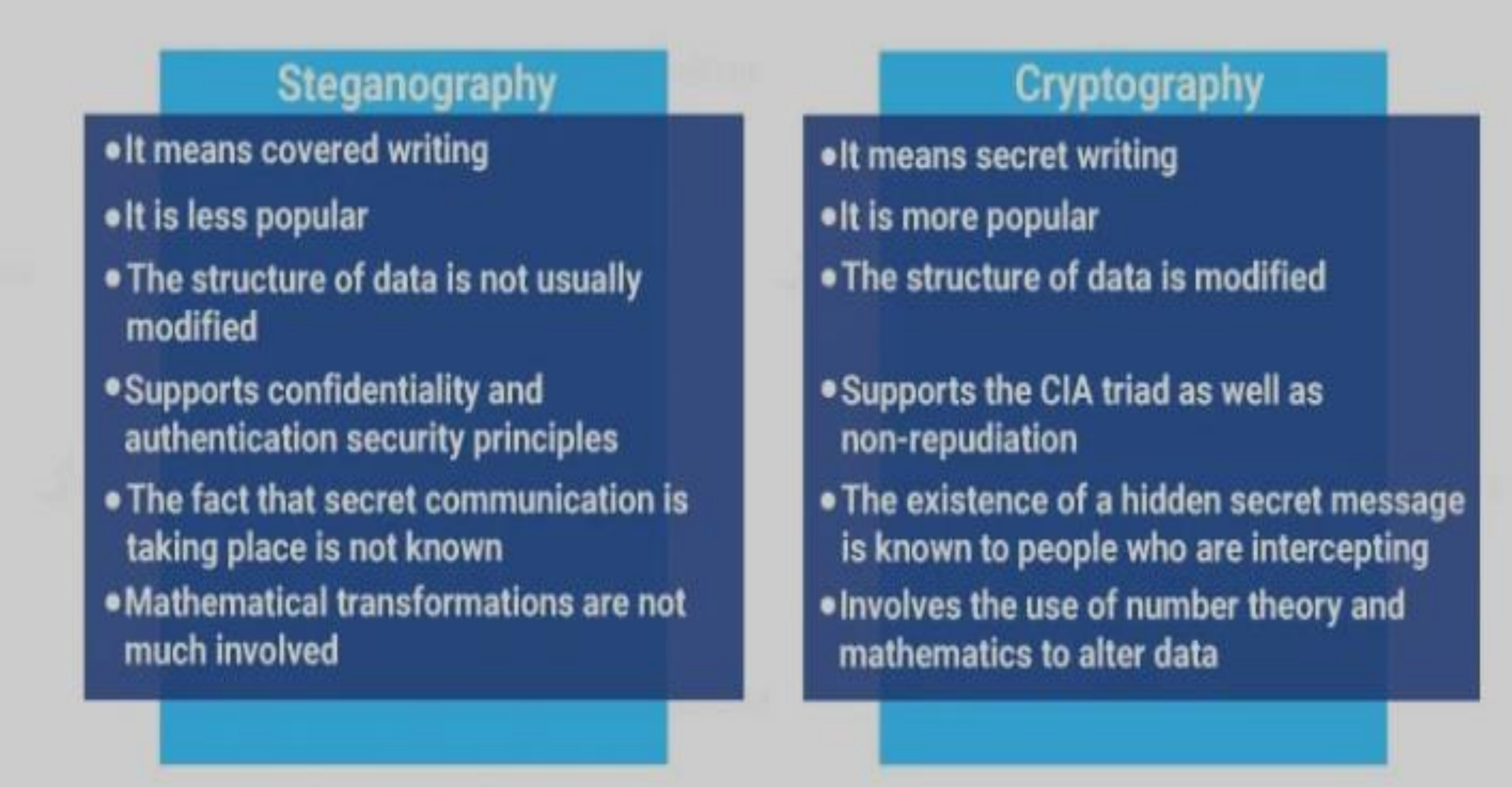

Malware
Carrier
steganographical encryption algorithm
Steganogram
steganographical decryption algorithm
Malware
Carrier

Steganographic attack image is emailed to victim who has no way of detecting embedded malware

# Steganography Examples

- Writing with invisible ink
- Embedding text in a picture (like an artist hiding their initials in a painting they’ve done)
- Backward masking a message in an audio file (remember those stories of evil messages recorded backward on rock and roll records?)
- Concealing information in either metadata or within a file header
- Hiding an image in a video, viewable only if the video is played at a particular frame rate
- Embedding a secret message in either the green, blue, or red channels of an RRB image

# Difference between Steganography and Cryptography



### Steganography

- It means covered writing
- It is less popular
- The structure of data is not usually modified
- Supports confidentiality and authentication security principles
- The fact that secret communication is taking place is not known
- Mathematical transformations are not much involved

### Cryptography

- It means secret writing
- It is more popular
- The structure of data is modified
- Supports the CIA triad as well as non-repudiation
- The existence of a hidden secret message is known to people who are intercepting
- Involves the use of number theory and mathematics to alter data

# How Steganography is different from obufuscation?

- Obfuscation deliberately makes the message hard to interpret, read, or decode.
- Cyber-security professionals employ obfuscation to protect sensitive information such as programming codes.
- The process makes it difficult for hackers to read the codes in the first place, which in turn prevents them from exploiting the data.

# Steganography Techniques

- Secure Cover Selection
- Least Significant Bit
- Palette Based Technique

# Steganography Tools

- **Steghide**: Steghide is a free tool that uses steganography to conceal information in other files, such as media or text.

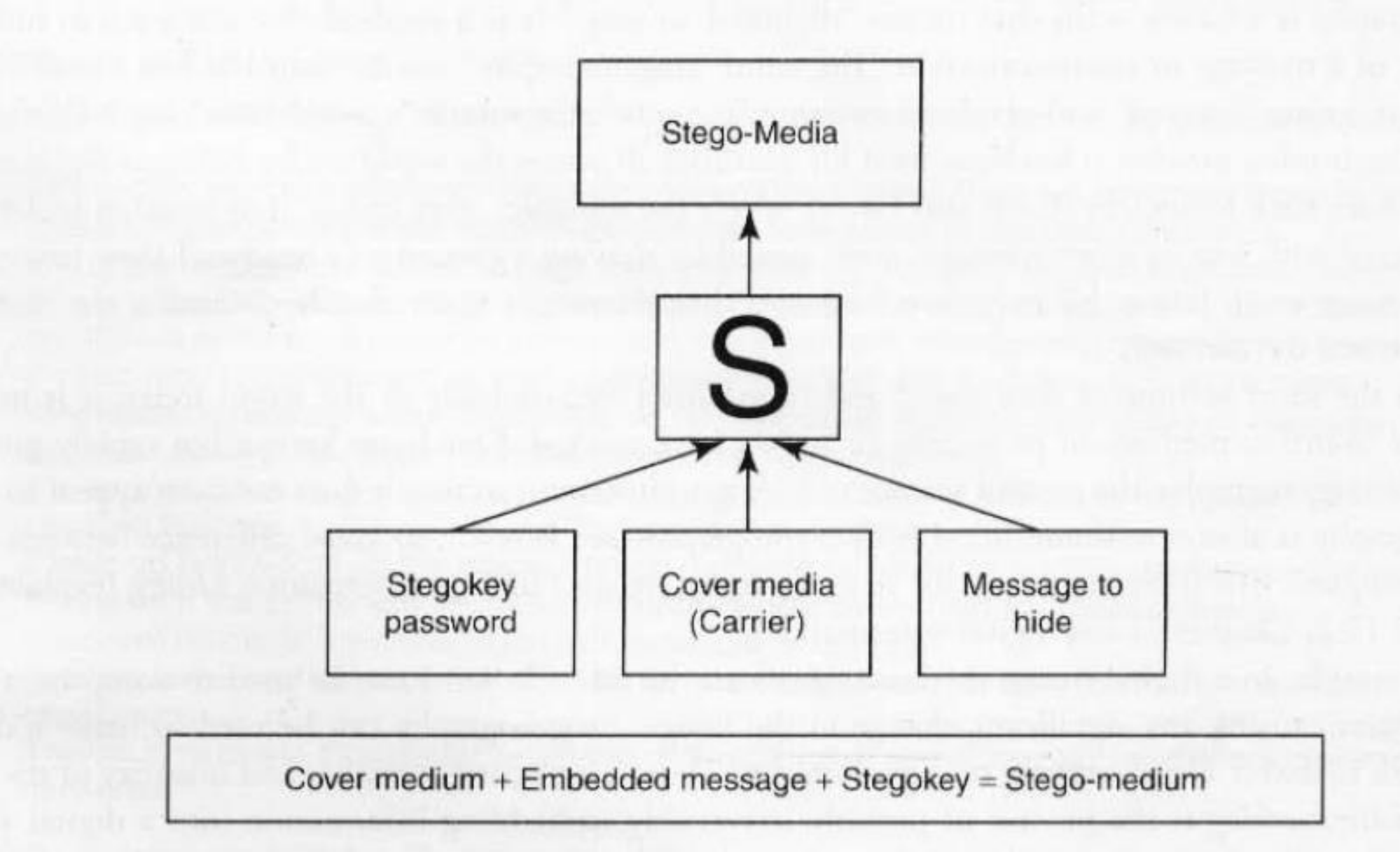
- **Stegosuite**: It is a Java-based, free steganography tool. Stegosuite makes it simple to obfuscate data in pictures for covert purposes.

- **OpenPuff**: It is a high-quality steganographic tool that allows you to conceal data in other media types like images, videos, and Flash animations.

- **Xiao Steganography**: To conceal information in BMP images or WAV files, use the free Xiao Steganography tool.

- **SSuite Picsel**: The free portable program SSuite Picsel is yet another option for hiding text within an image file; however, it uses a somewhat different method than other programs.

# How Steganography Works



# Advantages of Steganography

- Steganography is a form of encryption that protects the information within a message and the connections between sender and receiver.
- Hiding communications.
- Security, capacity, and robustness
- You can store an encrypted copy of a file containing sensitive information on the server without fear of unauthorized parties gaining access to the data.
- Government and law enforcement agencies can communicate secretly with the help of steganography corporations.

# Steganography Tools

- **DiSi-Steganography**

  It is a very small, DoS-based steganography program that embeds data in PCX images.

- **Invisible Folders**

  It can make any file or folder invisible to anyone using your PC even on a network.

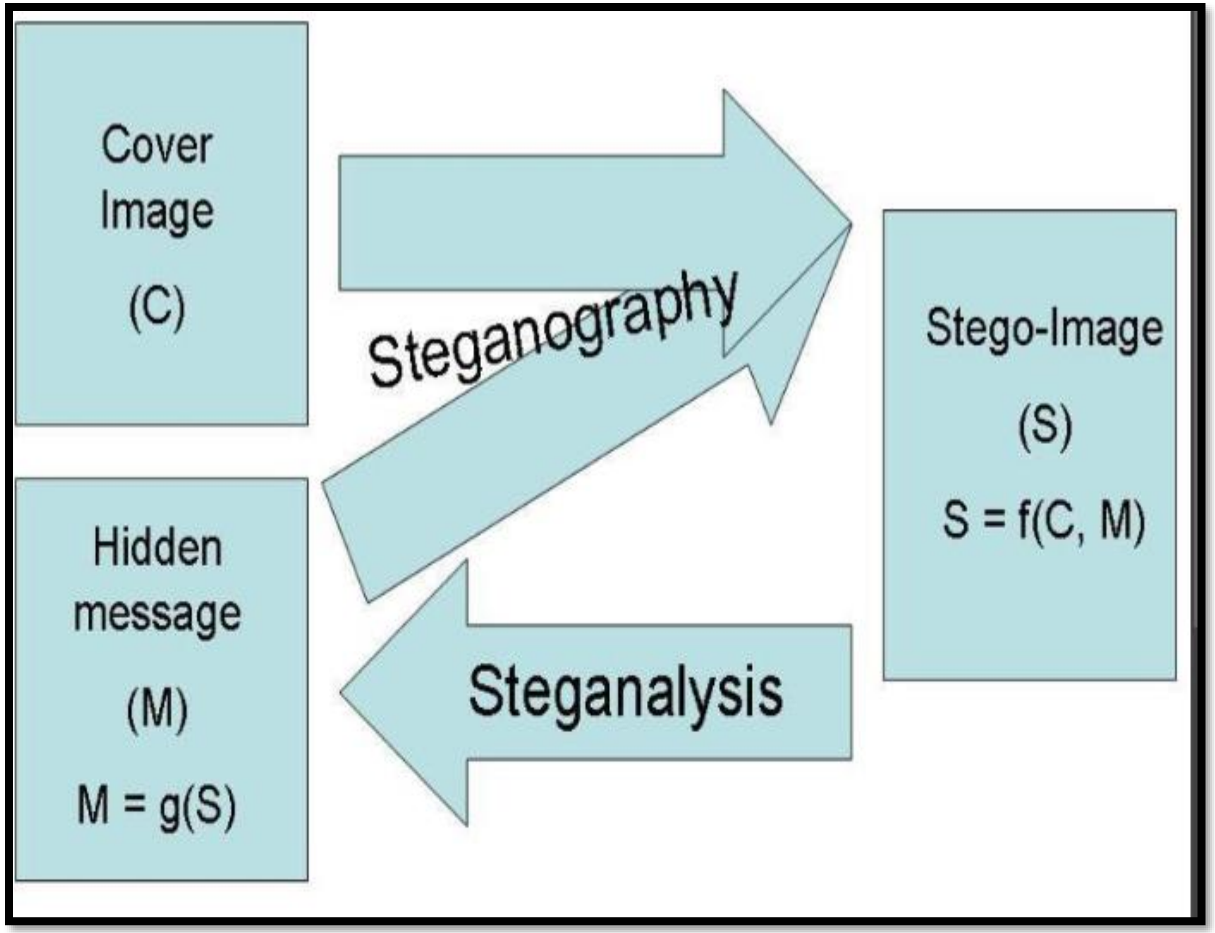
- **Invisible Secrets:-**

  It not only encrypts the data and files for safe-keeping or for secure transfer across the Net but also hides them in places.

- **Hermetic Stego:-** Steganography program that allows encrypting and hide contents of any data file in another file so that the addition of the data to the container file will not noticeably change the appearance of that file.

- **DCPP(DriveCrypt Plus):-** Secure hiding of an entire OS inside the free space of another OS. Full disk encryption, preboot authentication

# Steganography and Steganalysis



- Steganalysis is the art and science of detecting messages that are hidden in images, audio/video files using steganography.

- Automated tools are used to detect such steganographed data/information hidden in the image and audio and/or video files.

# Steganography Tools

- **StegAlyzerAS**

  It is a very small, DoS-based steganography program that embeds data in PCX images.

- **StegAlzyerSS**

  It can make any file or folder invisible to anyone using your PC even on a network.

- **StegSpy:-**

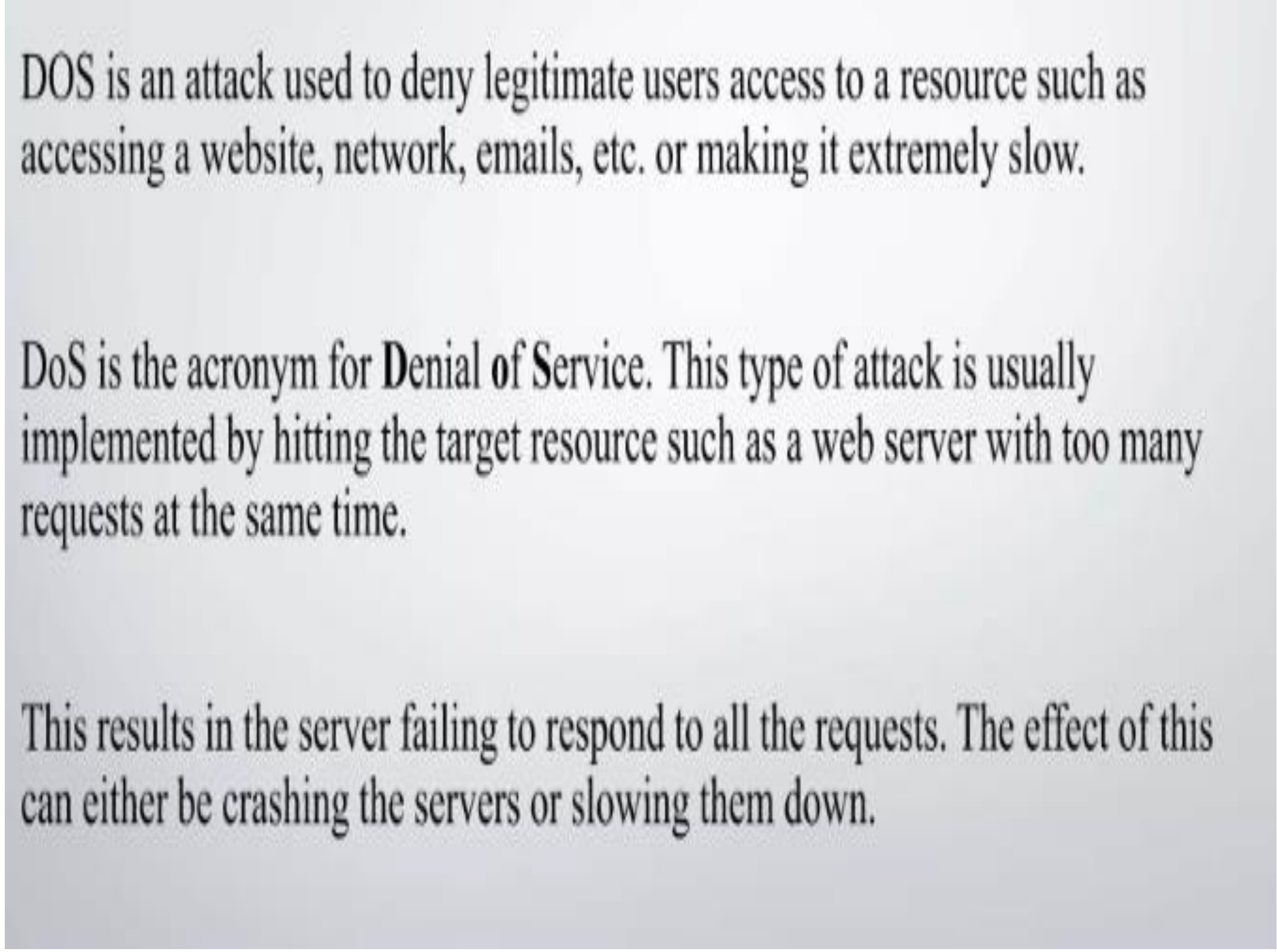
  It not only encrypts the data and files for safe-keeping or for secure transfer across the Net but also hides them in places.

- **Stegdetect**

- **Stegsecret**

- **VSL(Virtual Steganographic laboratory)**

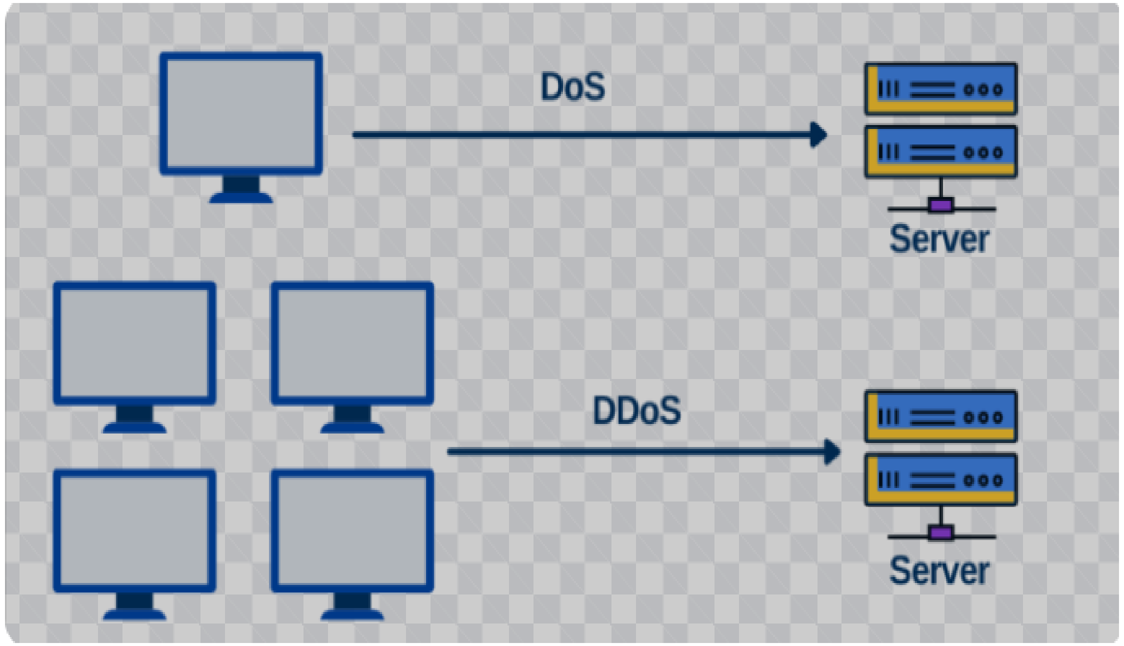
# DOS (Denial Of Service) Attacks



DOS is an attack used to deny legitimate users access to a resource such as accessing a website, network, emails, etc. or making it extremely slow.

DoS is the acronym for **Denial of Service**. This type of attack is usually implemented by hitting the target resource such as a web server with too many requests at the same time.

This results in the server failing to respond to all the requests. The effect of this can either be crashing the servers or slowing them down.



# DOS (Denial Of Service) and DDOS(Distributed DOS) Attacks

- A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.

**DOS Attacks:-**

- The attacker floods the bandwidth of the victim's network or fills his E-Mail box with Spam mail depriving him of the services he is entitled to access or provide.
- The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e., legitimate users) of a service from using it.

  1. Flood a network with traffic, thereby preventing legitimate network traffic.
  2. Disrupt connections between two systems, thereby preventing access to a service.
  3. Prevent a particular individual from accessing a service.
  4. Disrupt service to a specific system or person.

# DOS (Denial Of Service)

**Symptoms of DOS Attacks:-**

Usually slow network performance(opening files or accessing websites)—Such as long load times for files or websites.

Unavailability of a particular website

Inability to access any website

A sudden loss of connectivity across devices on same network.

Increase in the number of Spam E-mails received(E-Mail Bomb)

# DOS (Denial Of Service) Attacks

**Buffer Overflow Technique**

- ✓ It is the most common form of DOS attack.
- ✓ The adversary drives more traffic to a network address than the system is capable of handling.
- ✓ Buffer Overflow technique is used to commit Spoofing(IP address Spoofing).

**IP address Spoofing**

- ✓ Creation of IP packets with forged source IP address(To Conceal ID of Sender)
- ✓ The attacker spoofs the IP address and floods the network of the victim with repeated requests.
- ✓ As the IP address is fake, the Victim machine keeps on waiting for the response from the attacker’s machine(a lot of Bandwidth of the network will be consumed…failed to serve legitimate requests.)

# Classification of DOS Attacks

- Bandwidth Attacks: target the Network’s bandwidth, available computing resources

- Logic Attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack.

- Protocol Attacks exploit a specific feature or implementation bug of some protocol installed at the victim’s system to consume excess amounts of its resources.

- Unintentional DOS attack– Due to a sudden spike in popularity

# Types or levels of DOS Attacks

**Flood attack(ping flood)**

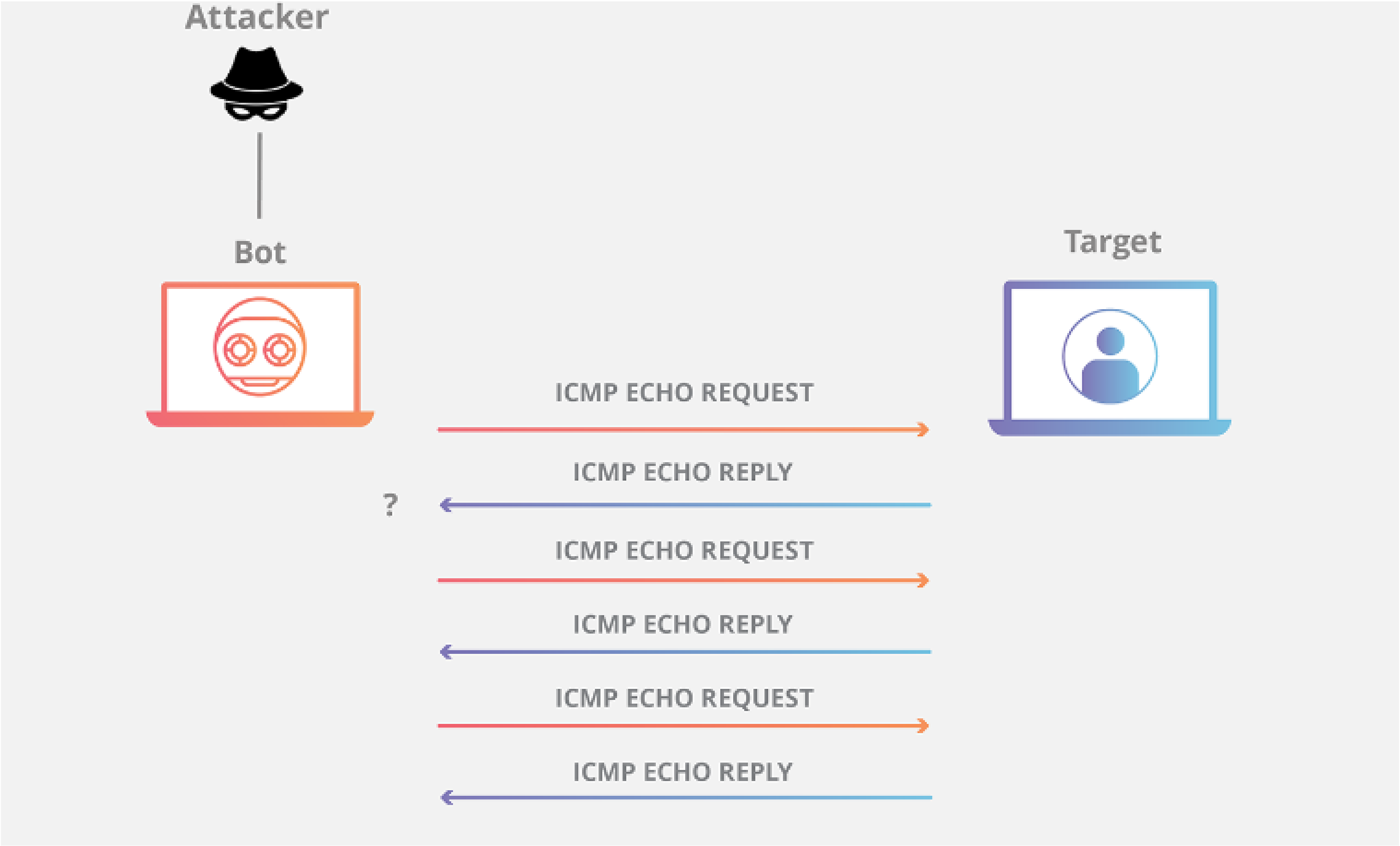
✓ The attacker sends the victim an overwhelming number of ping packets using ping commands.

✓ The attacker requires a faster network connection than the victim.

✓ Simply to launch, however difficult to prevent.

✓ For Example: an ICMP flood attack occurs when a system receives too many ICMP ping commands and must use all its resources to send reply commands.

# Ping Flood


Attacker
Bot
Target
ICMP ECHO REQUEST
ICMP ECHO REPLY
?
ICMP ECHO REQUEST
ICMP ECHO REPLY
ICMP ECHO REQUEST
ICMP ECHO REPLY

# Types or levels of DOS Attacks

## Ping of death attack

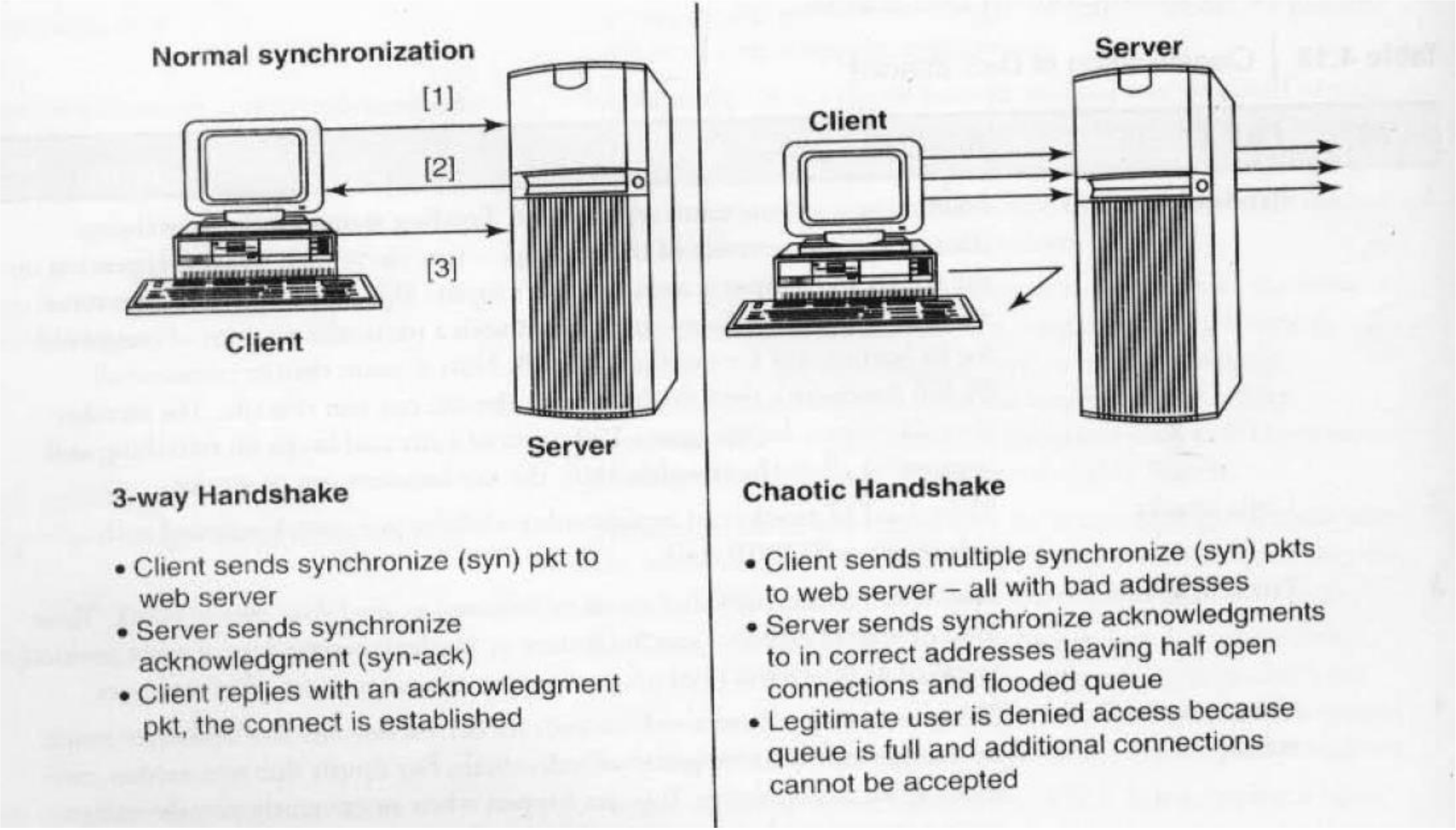
- ✓ The ping of death attack sends oversized ICMP packets.
- ✓ The maximum packet size allowed is 65,536 octets.
- ✓ Some systems upon receiving the oversized packet, will crash, freeze or reboot, resulting in DOS.

# Types or levels of DOS Attacks

**SYN  attack(TCP SYN Flooding)**

- ✓ In the TCP, handshaking is done with SYN and ACK messages.
- ✓ An attacker initiates a TCP connection to the server with an SYN(using spoof source address).
- ✓ The Server replies with a SYN-ACK. The client does not send back ACK, causing the server to allocate memory for pending connection and wait.
- ✓ This fills buffer space for SYN messages in the target system and prevents other systems from communicating.

# Denial of Service (DOS) Attack



### 3-way Handshake

- Client sends synchronize (syn) pkt to web server
- Server sends synchronize acknowledgment (syn-ack)
- Client replies with an acknowledgment pkt, the connect is established

### Chaotic Handshake

- Client sends multiple synchronize (syn) pkts to web server – all with bad addresses
- Server sends synchronize acknowledgments to in correct addresses leaving half open connections and flooded queue
- Legitimate user is denied access because queue is full and additional connections cannot be accepted

# Levels of Denial of Service (DOS) Attack

**Teardrop attack**

- ✓ Fragmented IP packets are forged to overlap each other when receiving host tries to reassemble them.
- ✓ IP’s packet fragmentation algorithm is used to send corrupted packets to confuse the victim and will hang the system.

**Smurf attack**

- ✓ Floods the target system via spoofed ping messages.
- ✓ Deals with ICMP echo request and ICMP echo response.

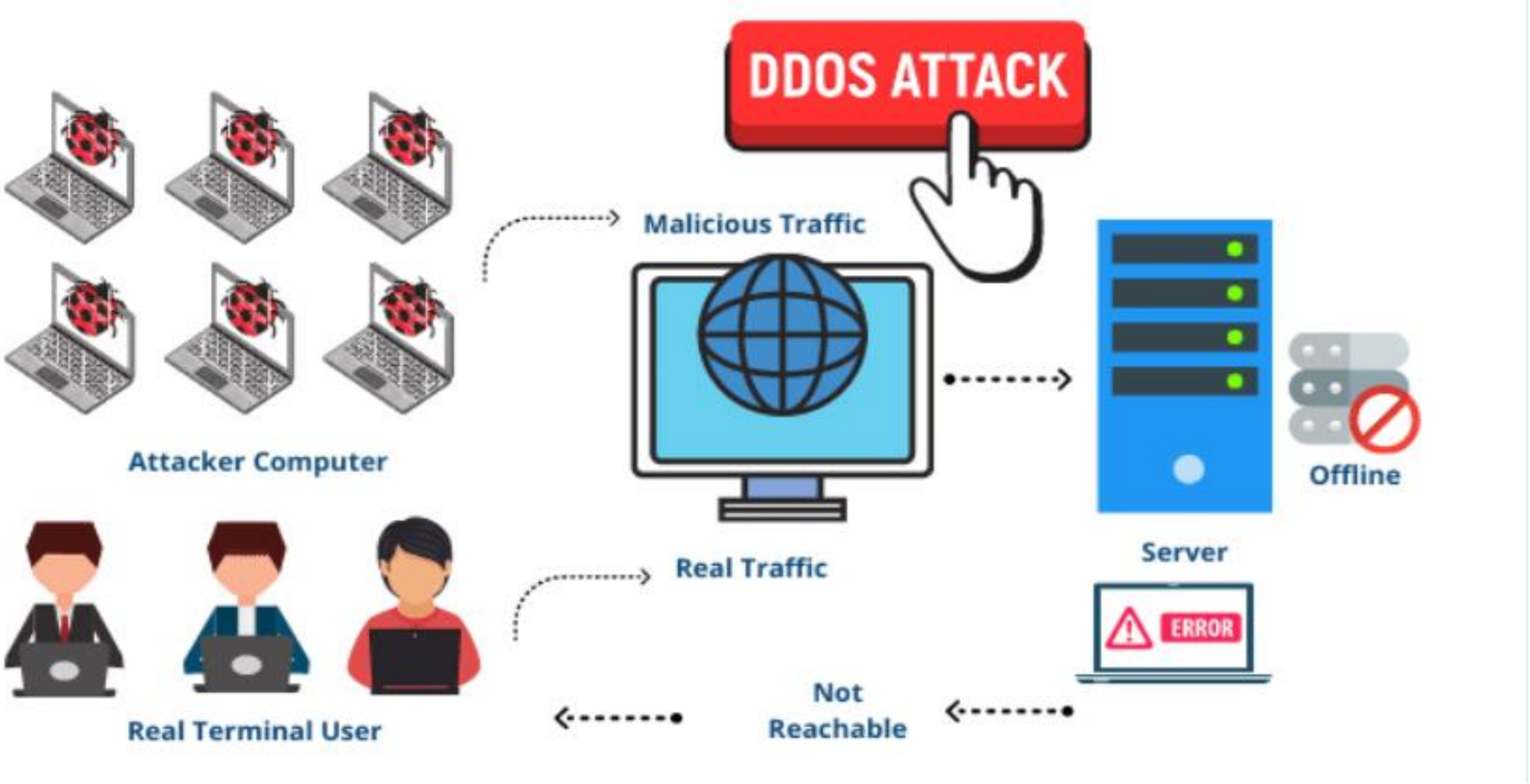
**Nuke attack**

- ✓ Old DOS attack.
- ✓ Invalid ICMP packets sent to the target.

# DDOS Attack

- In a DDoS attack, an attacker may use your computer to attack another computer.
- By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer.
- He/she could then force your computer to send huge amounts of data to a website or send Spam to particular E-Mail addresses.
- A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system. The zombie systems are called "secondary victims" and the main target is called "primary victim."
- DDoS attacks involves hardcoding the target IP address prior to release of the malware, hence no further interaction is necessary to launch the attack.
- A system may also be compromised with a Trojan, allowing the attacker to download a zombie agent.

# DDOS Attack


DDOS ATTACK
Malicious Traffic
Attacker Computer
Offline
Server
ERROR
Real Traffic
Real Terminal User
Not Reachable

# How to protect from DDOS/DOS Attack

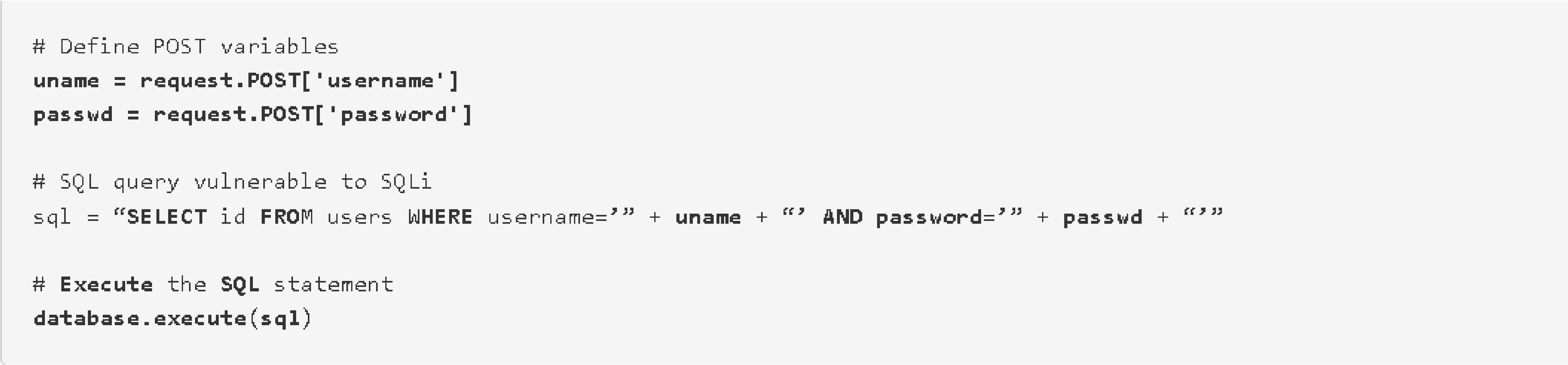
.

1. Implement router filters.
2. If such filters are available for your system, install patches to guard against TCP SYN flooding.
3. Disable any unused or inessential network service.
4. Enable quota systems on your OS if they are available.
5. Observe your system’s performance and establish baselines for ordinary activity
6. Routinely examine your physical security with regard to your current needs.
7. Use Tripwire or a similar tool to detect changes in configuration information or other files.
8. Invest in and maintain “hot spares” – machines that can be placed into service quickly if a similar machine is disabled.
9. Invest in redundant and fault-tolerant network configurations.
10. Establish and maintain regular backup schedules and policies, particularly for important configuration information.
11. Establish and maintain appropriate password policies, especially access to highly privileged accounts such as Unix root or Microsoft Windows NT Administrator.

# SQL Injection Attack

- SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.
- The vulnerability is present when user input is either filtered incorrectly for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.
- Attackers target the SQL servers – common database servers used by many organisations to store confidential data.
- During an SQL injection attack, Malicious Code is inserted into a web form field or the website’s code to make a system execute a command shell or other arbitrary commands.
- Just as a legitimate user enters queries and additions to the SQL database via a web form, the attacker can insert commands to the SQL server through the same web form field.
- Attackers can use SQL injection vulnerabilities to bypass application security measures.

# Simple SQL Injection Attack example

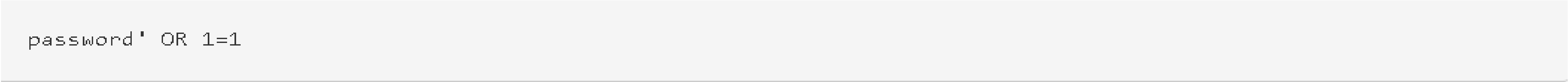


```
# Define POST variables
uname = request.POST['username']
passwd = request.POST['password']

# SQL query vulnerable to SQLi
sql = “SELECT id FROM users WHERE username=’” + uname + “’ AND password=’” + passwd + “’”

# Execute the SQL statement
database.execute(sql)
```

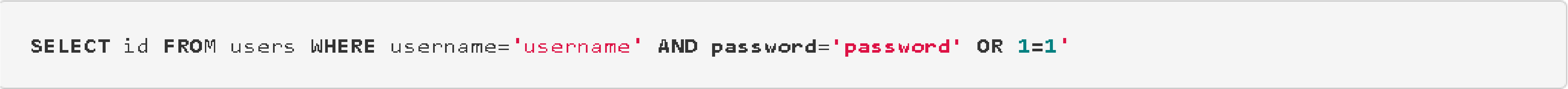
These input fields are vulnerable to SQL Injection. An attacker could use SQL commands in the input in a way that would alter the SQL statement executed by the database server. For example, they could use a trick involving a single quote and set the passwd field to:



```
password' OR 1=1
```

# Simple SQL Injection Attack example

As a result, the database server runs the following SQL query:



```
SELECT id FROM users WHERE username='username' AND password='password' OR 1=1'
```

Because of the OR 1=1 statement, the WHERE clause returns the first ID from the user table no matter what the username and password are:

# Blind SQL Injection

***Blind SQL Injection***

- Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker.

- The page with the vulnerability may not be the one that displays data; however, it will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page.

# How to prevent SQL Injection Attacks

SQL injection attacks occur due to poor website administration and coding. The following steps can be taken to prevent SQL injection.

1. **Input validation**

   **--Replace all single quotes with two single quotes.**
   **--Sanitize the input**
   **--Numeric value must be checked.**
   **--Keep all the boxes and form fields as short as possible to limit the length of user input.**

2. **Modify error reports**

   **-- handle error reports carefully—It must not be displayed to outside users.**

3. **Other preventions**

   **--Isolate data base server and web server.**

# Attacks on Wireless Networks

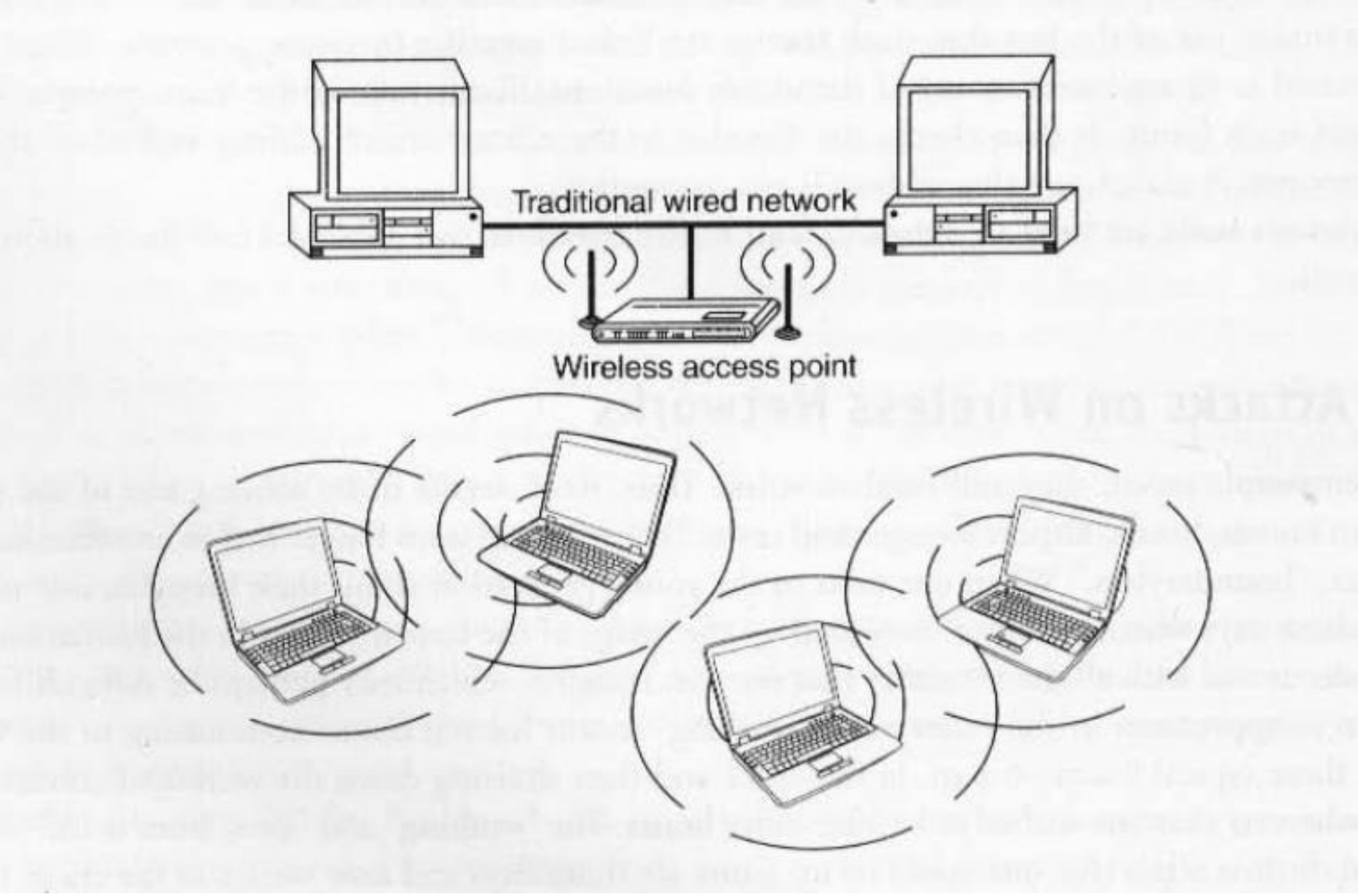
The following are different types of “mobile workers”:

1. Tethered/remote worker
2. Roaming user
3. Nomad
4. Road warrior

- Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wireless-enabled devices such as laptops and PDAs.

- Wireless networks are generally composed of two basic elements:
  (a) Access points (APs)
  (b) Other wireless-enabled devices, such as laptops radio transmitters and receivers to communicate or “connect” with each other.

# Wireless Networks



# Important Terminologies

- 802.11 networking standards.
- Access Points
- Wifi hotspots
- Service set identifier(SSID)
- Wired equivalence privacy(WEP)
- WIFI protected access(WPA and WPA2)
- Media Access Control(MAC)

# Traditional Techniques of Attacks on Wireless Networks

- Penetration of a wireless network through unauthorized access is termed as wireless cracking.

  - **Sniffing**

    --Intercepting wireless data

  - **Spoofing**

    --MAC address spoofing

    --IP spoofing

    --Frame spoofing

  - **Denial of service (DoS)**

  - **Man-in-the-middle attack (MITM)**

  - **Encryption cracking**

# How to Secure Wireless Networks

1. Change the default settings of all the equipments/components of the wireless network (e.g., IP address/ user IDs/administrator passwords, etc.).

2. Enable WPA/WEP encryption.

   WEP stands for Wired Equivalent Privacy, and WPA stands for Wireless Protected Access, Change the default SSID.

4. Enable MAC address filtering.

5. Disable remote login.

6. Disable SSID broadcast.

7. Avoid providing the network a name that can be easily identified (e.g., My_Home_Wifi ).

8. Connect only to a secured wireless network (i.e., do not auto-connect to open Wi-Fi hotspots).

9. Upgrade the router’s firmware periodically.