PRESENTATION ON

Information Security Concepts

Ms.Pradnya Natekar

Lecturer, Computer Engineering,SBMP

Need for Computer Security

- **Protection of Sensitive Data**
  - Safeguards personal, financial, and organizational information from theft or misuse.
  - Prevents unauthorized access to confidential files.

- **Prevention of Cyber Threats**
  - Shields systems from cyberattacks such as viruses, ransomware, phishing, and hacking attempts.
  - Mitigates risks posed by malware and spyware.

- **Maintaining Data Integrity**
  - Ensures data is accurate, reliable, and unchanged during storage or transfer.
  - Prevents unauthorized modifications or tampering.

- **Ensuring System Availability**
  - Protects against disruptions caused by DoS (Denial of Service) attacks or hardware failures.
  - Keeps critical systems operational for users.

- **Compliance with Legal and Regulatory Standards**
  - Meets requirements of data protection laws and industry standards (e.g., GDPR, HIPAA, PCI-DSS).
  - Avoids legal consequences and fines for data breaches.

- **Protection Against Insider Threats**
  - Safeguards against employees or trusted individuals misusing access rights.
  - Enforces policies to monitor and control insider actions.

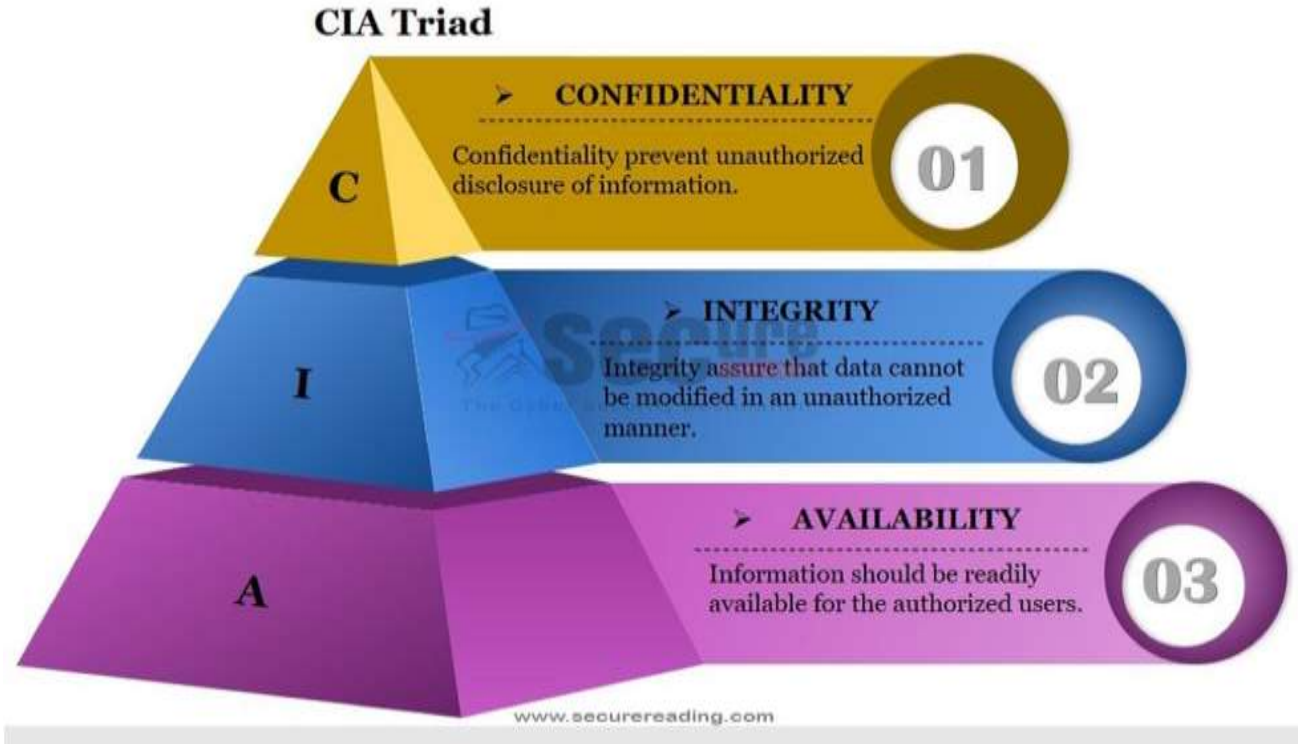
- **Economic and Reputational Impact**
  - Prevents financial losses due to data breaches, fraud, or system downtime.
  - Preserves trust and reputation by demonstrating commitment to security.

- **Support for Remote Work and Cloud Services**
  - Ensures secure access to corporate resources for remote employees.
  - Protects data stored in cloud environments from unauthorized access.

- **Defense Against Emerging Technologies**
  - Prepares for threats arising from advancements like AI, IoT, and quantum computing.
  - Adapts to new vulnerabilities in evolving tech ecosystems.

Key Concepts of Information Security

- The foundation of computer security is built on several core principles and concepts designed to protect computer systems, networks, and data from unauthorized access, misuse, and damage.
- By following these principles and implementing them effectively, organizations can build a strong foundation for computer security
- Below are the key elements of this foundation:



Information security concepts

- **1. Confidentiality**
- **Definition:** Ensures that information is accessible only to authorized users.
- **Methods:**
  - Encryption (e.g., AES, RSA)
  - Access Control Mechanisms (e.g., Role-Based Access Control)
  - Secure communication protocols (e.g., TLS/SSL)

- **2. Integrity**
- **Definition:** Ensures that data is accurate, consistent, and has not been tampered with.
- **Methods:**
  - Hash functions (e.g., SHA-256)
  - Digital Signatures
  - Checksums and Message Authentication Codes (MAC)

- **3. Availability**
- **Definition:** Ensures that authorized users have uninterrupted access to resources and systems.
- **Methods:**
  - Redundancy (e.g., backup systems)
  - Denial-of-Service (DoS) attack mitigation
  - Load balancing and disaster recovery plans

- **4. Authentication**
- **Definition:** Verifies the identity of users, devices, or systems before granting access.
- **Methods:**
  - Passwords and PINs
  - Multi-Factor Authentication (MFA)
  - Biometrics (e.g., fingerprint, facial recognition)

- **5. Authorization**
- **Definition:** Determines the permissions and access levels granted to authenticated users.
- **Methods:**
  - Access Control Lists (ACLs)
  - OAuth and Single Sign-On (SSO)
  - Privileged Access Management

6 .Non-Repudiation

- **Definition:** Ensures that a user cannot deny their actions or transactions.
- **Methods:**
  - Digital certificates
  - Audit trails and logging
  - Blockchain technology for tamper-evident records

7.Risk Management

- **Definition:** Identifies, evaluates, and mitigates potential security risks.
- **Steps:**
  - Threat Analysis
  - Vulnerability Assessment
  - Implementation of security policies and controls

Risk and Threat Analysis

Attack OR Attack Vector

- An attack vector is defined as the technique by which unauthorized access is gained inside the computer or network for a criminal purpose by exploiting the vulnerabilities in the system

Risk

- It can be defined as the probability of the loss from any particular threat from the threat landscape, which can exploit the system and gain the benefits from it such as loss of private and confidential information such as username and password, sensitive organization data, also the loss of the reputation which has occurred can be considered.
- Also, the loss occurred in terms of damage or destruction of hardware and software assets can be considered as Risk.

Threat

- Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

Vulnerability

- Weaknesses or gaps in a systems security program, design policies and implementation that can be exploited by different threats to gain unauthorized access of a computer system or network

Assets

- The term "asset" encompasses a wide range of valuable elements within an organization, categorized broadly into **people**, **property**, and **information**:
- **People**:
  - Includes employees, contractors, and customers.
  - Represents human capital crucial for operations, innovation, and service delivery.
- **Property**:
  - Comprises both **tangible assets**, such as buildings, machinery, equipment, and inventory.
  - Includes **intangible assets**, such as brand reputation, intellectual property, trademarks, and patents.
- **Information**:
  - Encompasses critical data like customer databases, proprietary software code, financial records, and sensitive company documents.
  - These are often intangible but have significant strategic and operational value.
- Each asset type plays a vital role in organizational success and requires appropriate measures for protection and management.

Countermeasure

- An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, or by minimizing the harm it can cause, or by discovering and reporting it so that corrective and proactive action can be taken
- Here in the below image, we will the relationship between all the different terminologies we have seen

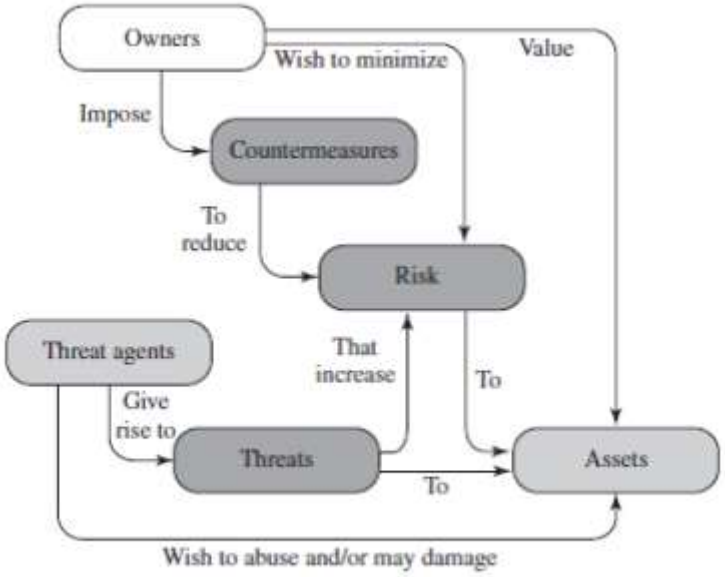
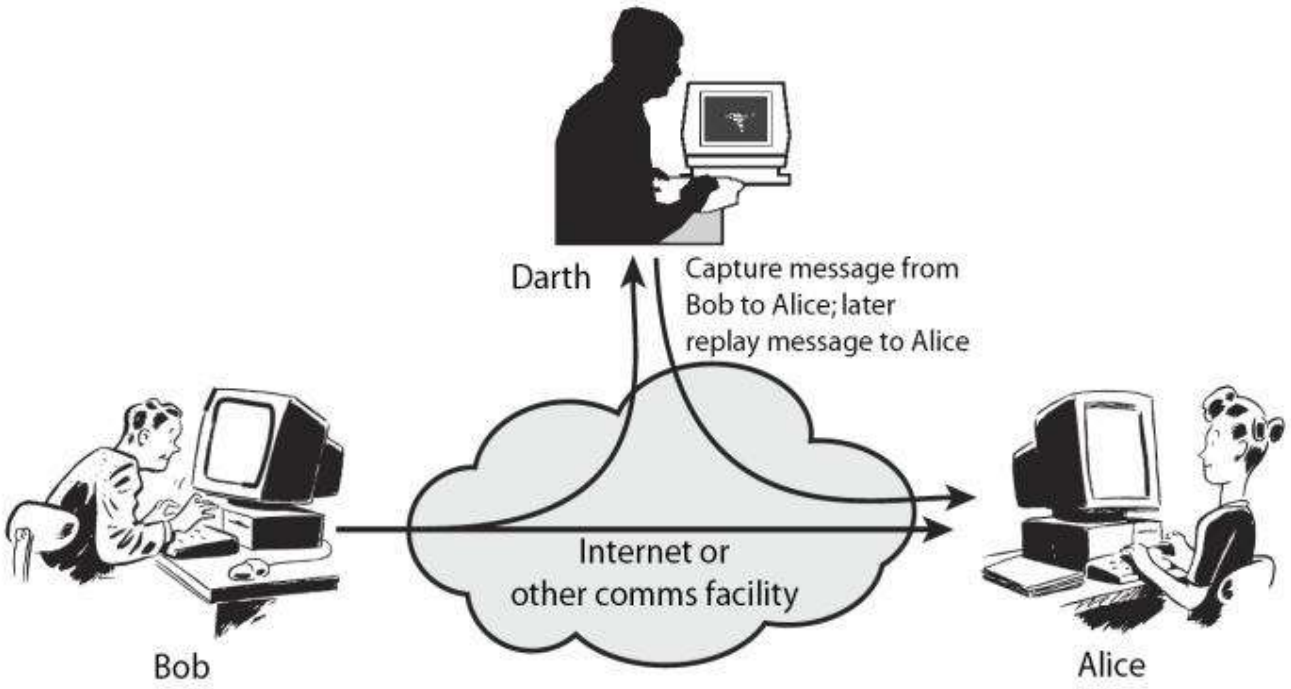


Figure 2.1 Security Concepts and Relationships

ATTACK

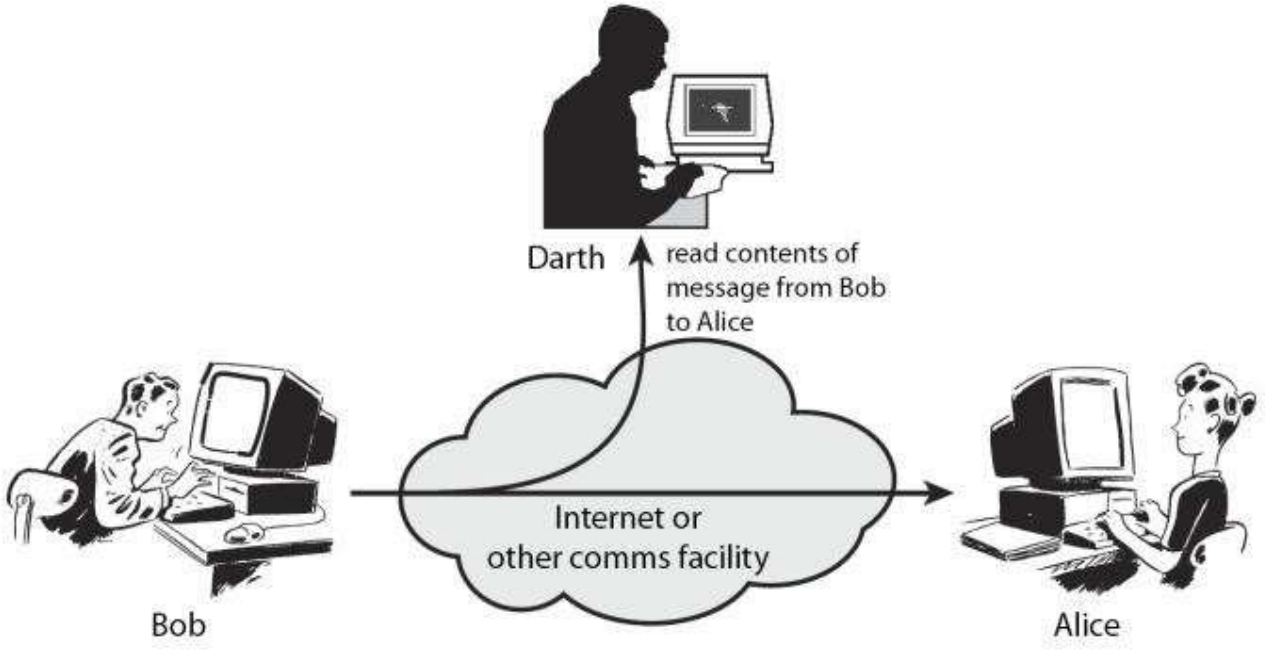
We have already seen the definition of the attack on the previous page,
we will look here the subtypes of attack and they are Active Attacks and Passive Attacks

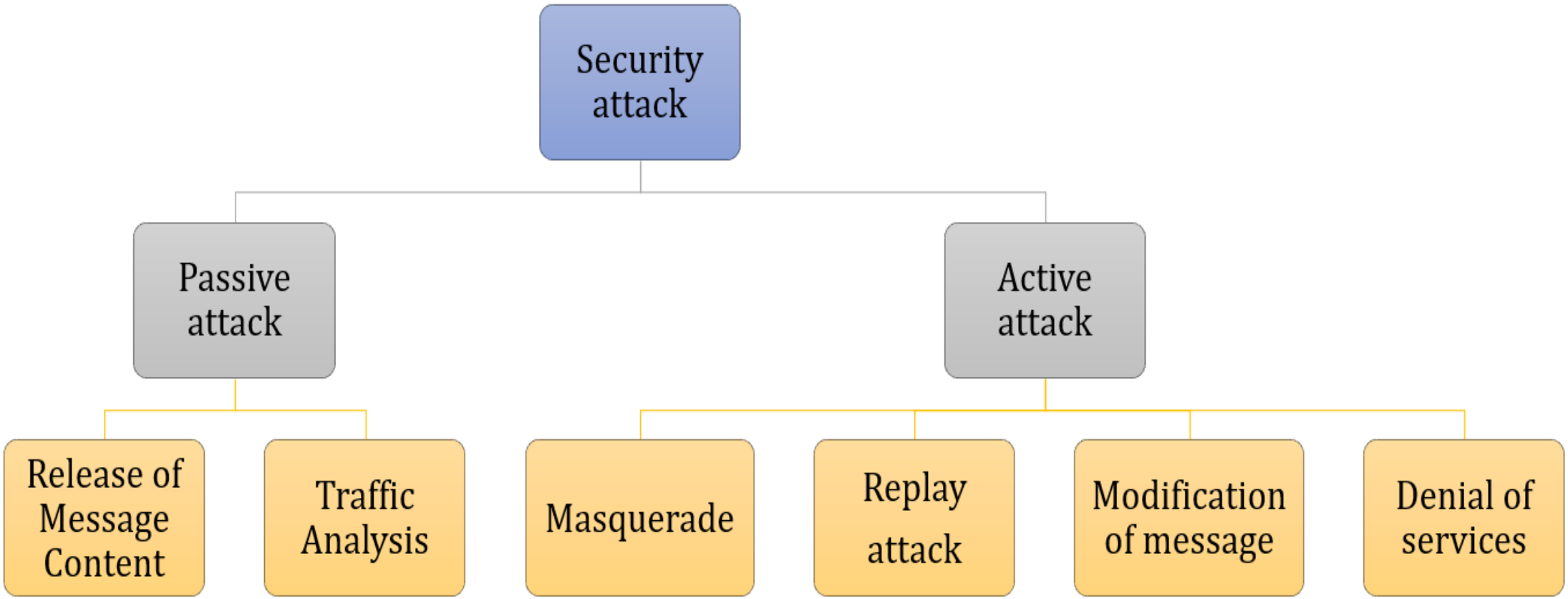
- Active Attacks: In an active attack, the attacker intercepts the connection and then modifies information.



An active attack can be divided further into Masquerade, Replay attack, Modification of messages.

Passive Attack: In a passive attack, the attacker intercepts the information but with the
intent of reading the information and not modifying it.
It can further be divided as Traffic Analysis and Release of Message content.





https://www.sanfoundry.com/difference-between-active-attack-and-passive-attack/

Message Content Release Attack

Message Content Release Attack is a passive attack in which confidential data of sender and receiver can be viewed by a third party.

The figure below explains the message content release attack.

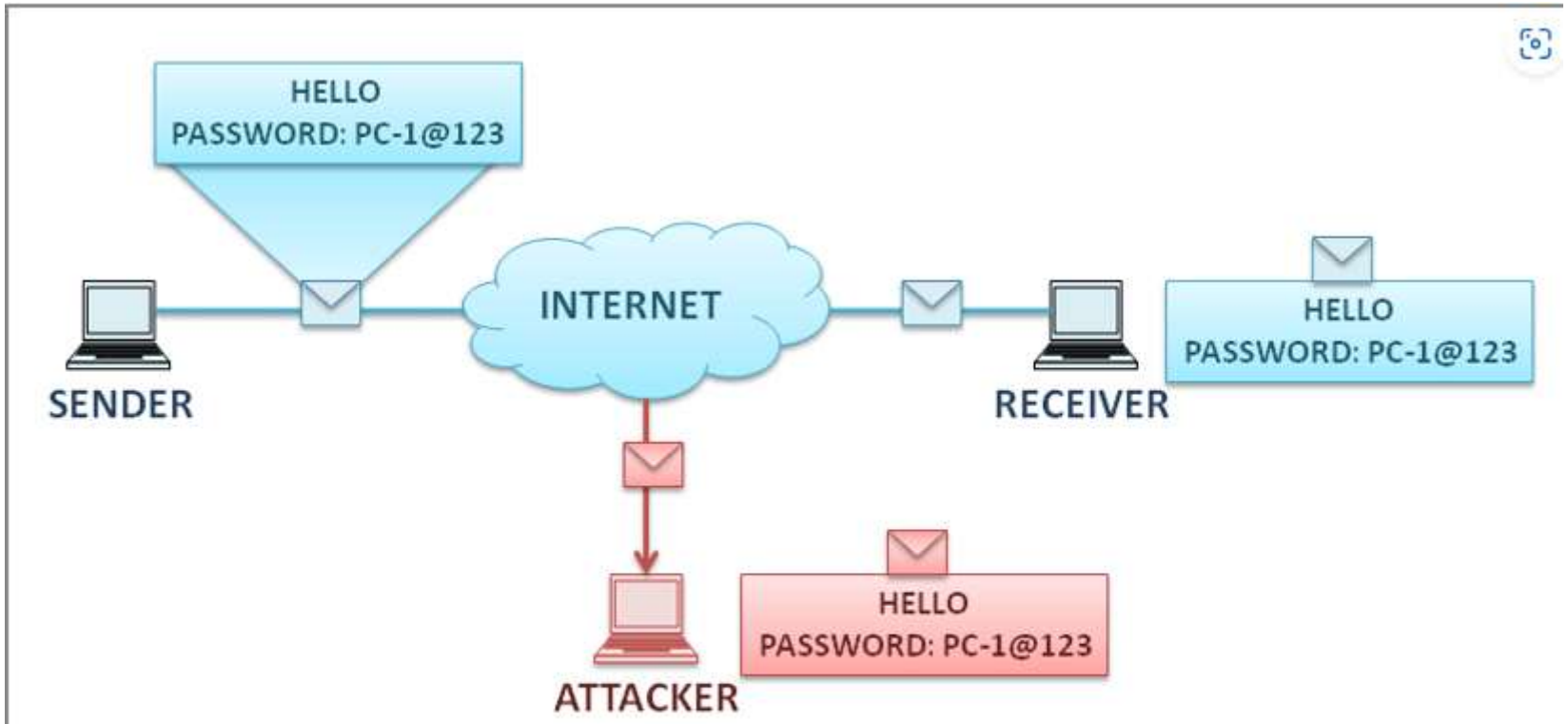


Figure 1: Release of Message Content

•The sender and receiver are communicating over a network.

•Data transmitted from sender to receiver is not encrypted. Now, in the middle of the communication, a third party, an attacker, comes to access and read the
confidential information of sender and receiver.

•The sender is sending the message to the receiver. The attacker connects across the range of the sender and receiver and accesses the channel.

•Once an attacker gains access to the channel, they can monitor the contents of the data transmitted by the sender and receiver.

•The attacker can use confidential data with malicious intent. For example, they may sell the sender and receiver passwords to another party to earn money.

•One way to prevent this attack is to encrypt the data with an encryption algorithm and key. Without encryption of the data, the attacker can easily access the channel. Therefore, it is necessary to encrypt the data.

Traffic Analysis

The attacker can use traffic analysis to identify hosts on the network that are communicating. The attacker runs a script and tries to analyze the number of packets transmitted.

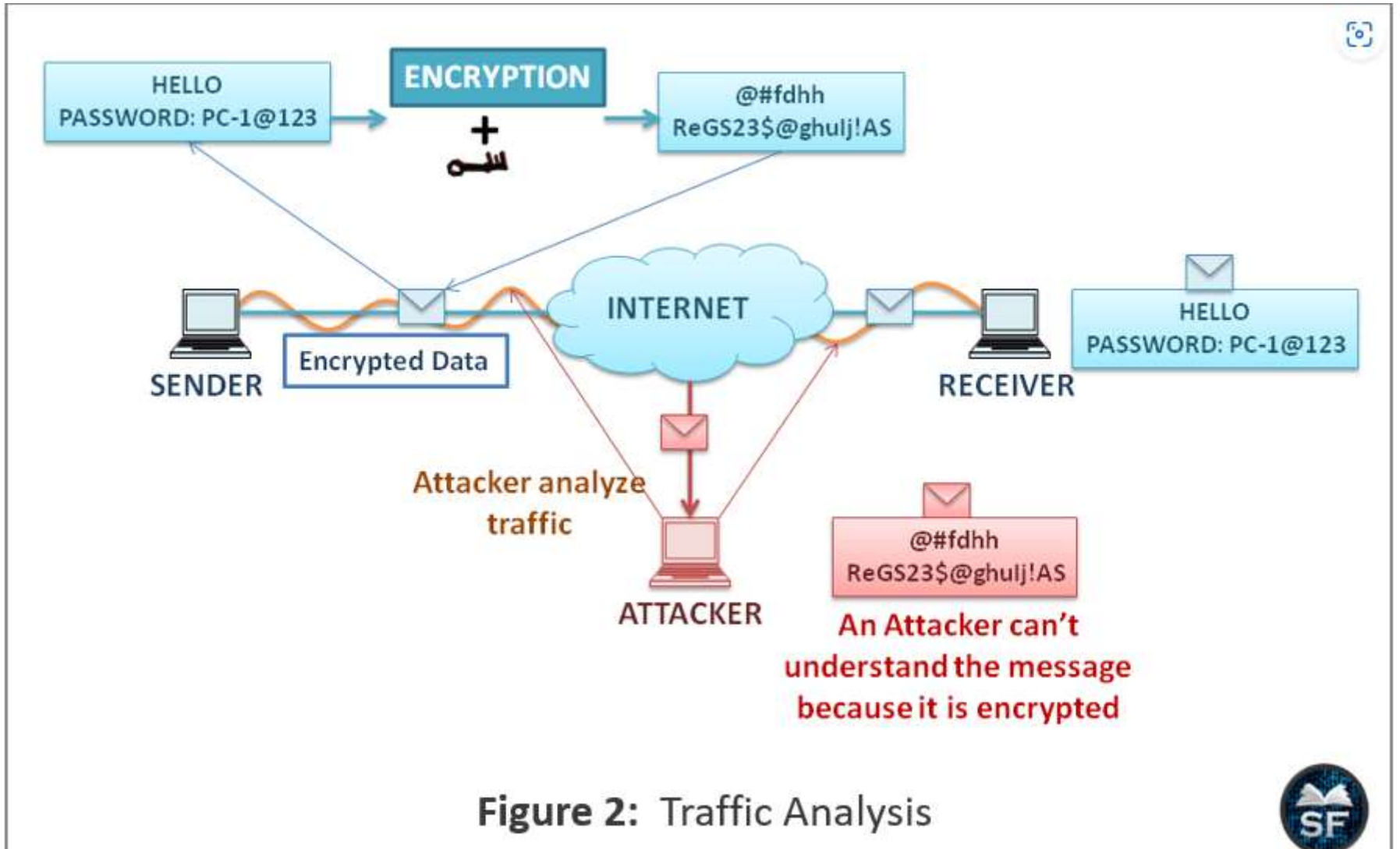


Figure 2: Traffic Analysis

•The attacker tries to find the pattern and behavior of the communication. It analyzes traffic, predicts transmission behavior, and decides whether hosts are exchanging confidential information or having a normal conversation

•The attacker learns about the incoming and outgoing traffic on a network, the frequency of sending messages, at what times the sender and receiver are most active, the length of packets exchanged between the sender and receiver, and what kind of communication is going on between them.

•Basically, the attacker performs traffic analysis if the sender and receiver are sending data in an encrypted format.

•The attacker has access to the channel over which the sender and receiver are communicating.

•The attacker receives the packet sent by the sender but cannot read it because the packet is encrypted. So, the attacker tries to find out the pattern of traffic, determining where the traffic is coming from and where it is going.

•Here, the attacker cannot modify the messages, but can make decisions based on the traffic regarding the type of communication between the sender and the receiver.

•The sender and receiver have no idea that someone is analyzing the traffic.

Replay Attack

A replay attack is an active attack that can be carried out on a network by an attacker with bad intentions.

•Confidential information is transmitting over a network, and attackers try to access that information to take advantage of it.

•The attacker can enable a replay attack by using ARP spoofing or by sending malicious code to the end device.

•When a host sends confidential data to a server, an attacker seated in the middle can access the data and replay it to appear as someone else. The attacker sends the same data of the sender to the receiver over and over again.

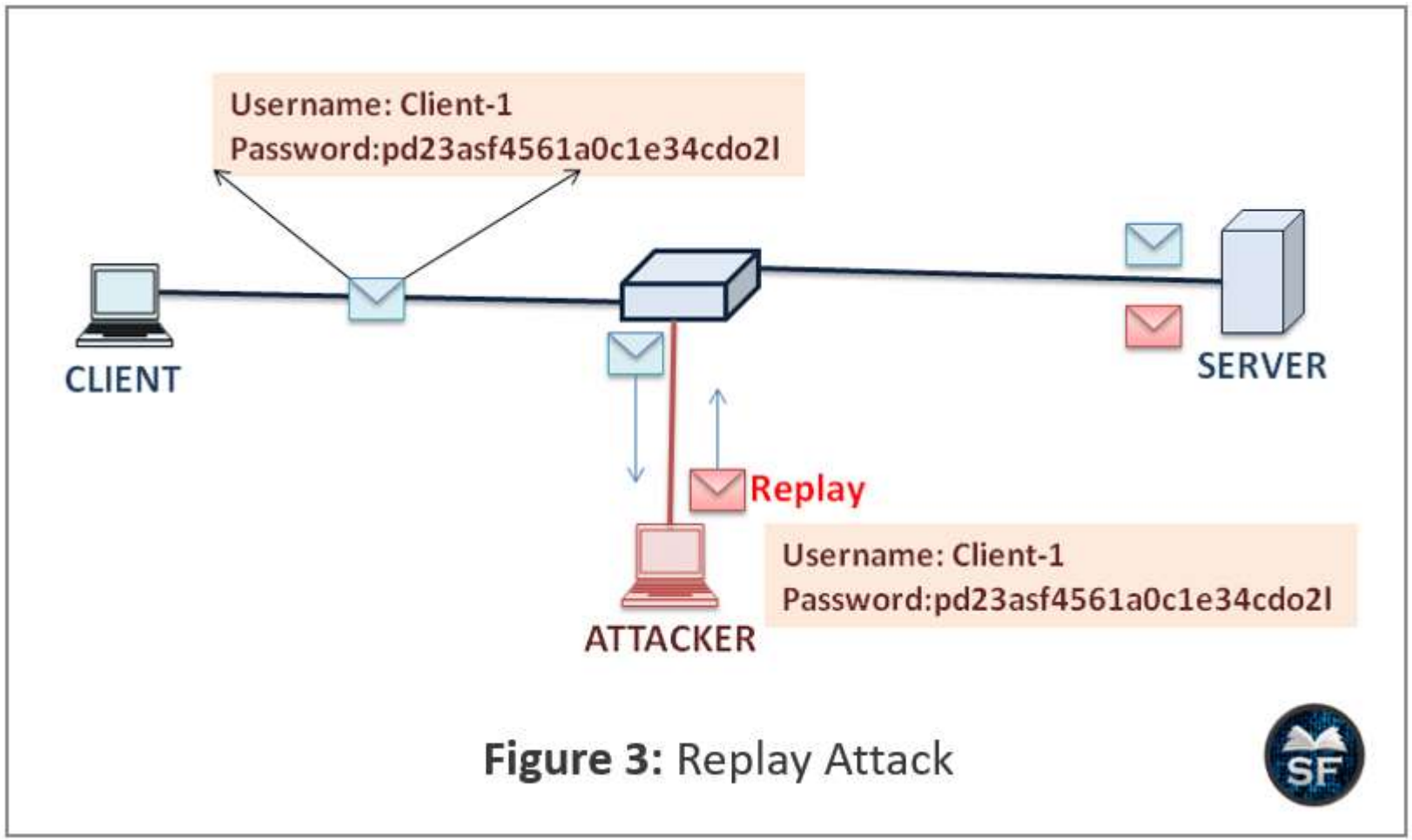


Figure 3: Replay Attack

•The client wants to access the server. The client is connected to the switch, and an attacker gains access to the switch.

•The client sends confidential data to the server for authentication. Now, the data will be transmitted through the switch.

•The switch transmits the data to the server and an attacker. The attacker gets the client's data.

•The client data contains a username and a hashed password for authentication. Also, the attacker gets a copy of the client's username and hashed password.

•So, the attacker will send an authentication request to the server with the client's username and hashed password. This is known as a replay.

•The server gives access to the attacker because the server thinks that the data came from the client itself, but it is actually coming from an attacker.

•To prevent replay attacks, session IDs are used. The server gives the client a temporary session ID for as long as the server and the client are communicating.

•When an attacker replays the data on the server, the server will not give access to the attacker.

Message Modification

When the sender sends a message to the receiver, the message reaches the third party sitting between the sender and the receiver and receives the message. The attacker modifies the message by flipping bits or adding malicious code or generating noise.
The figure below explains the message modification.

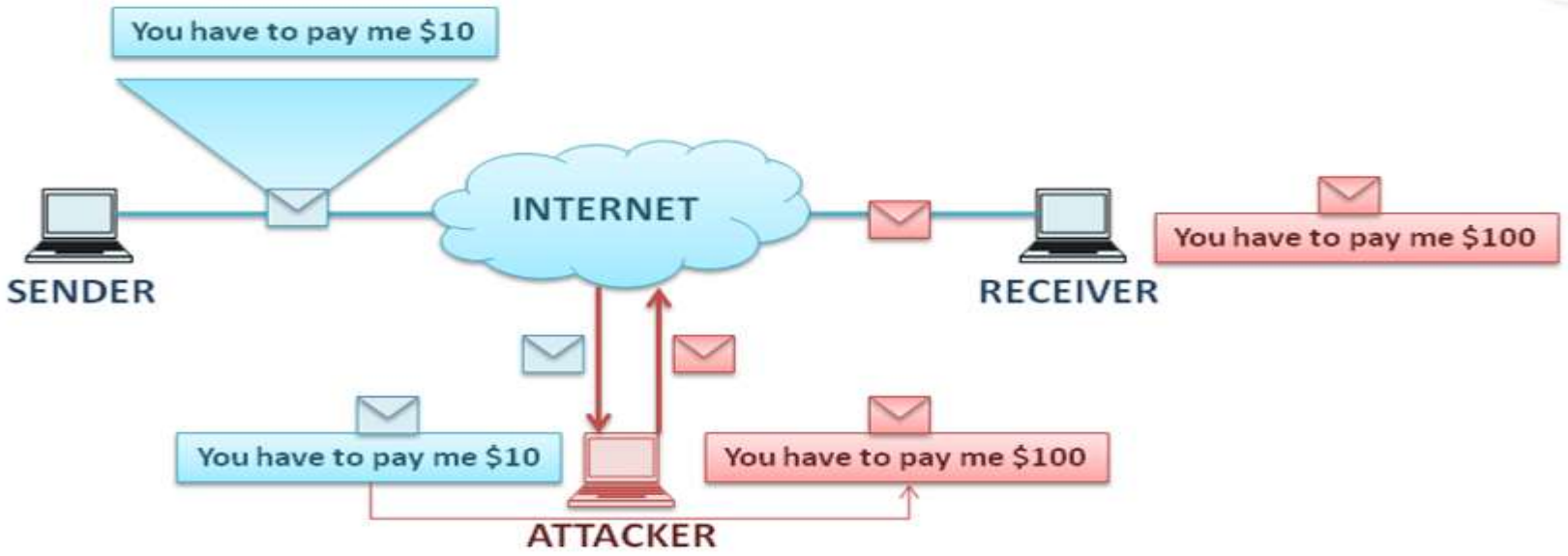


Figure 4: Message Modification

•As shown in the picture, the sender sends a message to the receiver that you have to pay me $10.

• The attacker intercepts the message and modifies it, you have to pay me $100 and send it to the receiver.

•When the receiver receives the message, it will receive the modified message, not the original message. This attack is also known as the man-in-the-middle (MITM) attack.

•Here, an attacker blocks the communication of sender and receiver using DNS hijacking or BGP redirection.

•Message modification compromises the confidentiality and integrity of the message.

•The message modified by the attacker can cause a delay in message delivery or loss of message

•To prevent message modification attacks, we can use symmetric-key and asymmetric-key cryptography algorithms to achieve message confidentiality, and document, fingerprint, and message digest to achieve message integrity.

Denial of Service (DoS)

Website resources are stored on the server. It means when the client requests services from a website, it communicates with the server and the server provides access to the resources to the client. The attacker floods the server with the fake IP addresses, gains access to all of the server's resources, and the server denies all other users access to the resources.

This attack is known as a Denial of Service (DoS) attack.

The diagram below explains the denial-of-service attack.

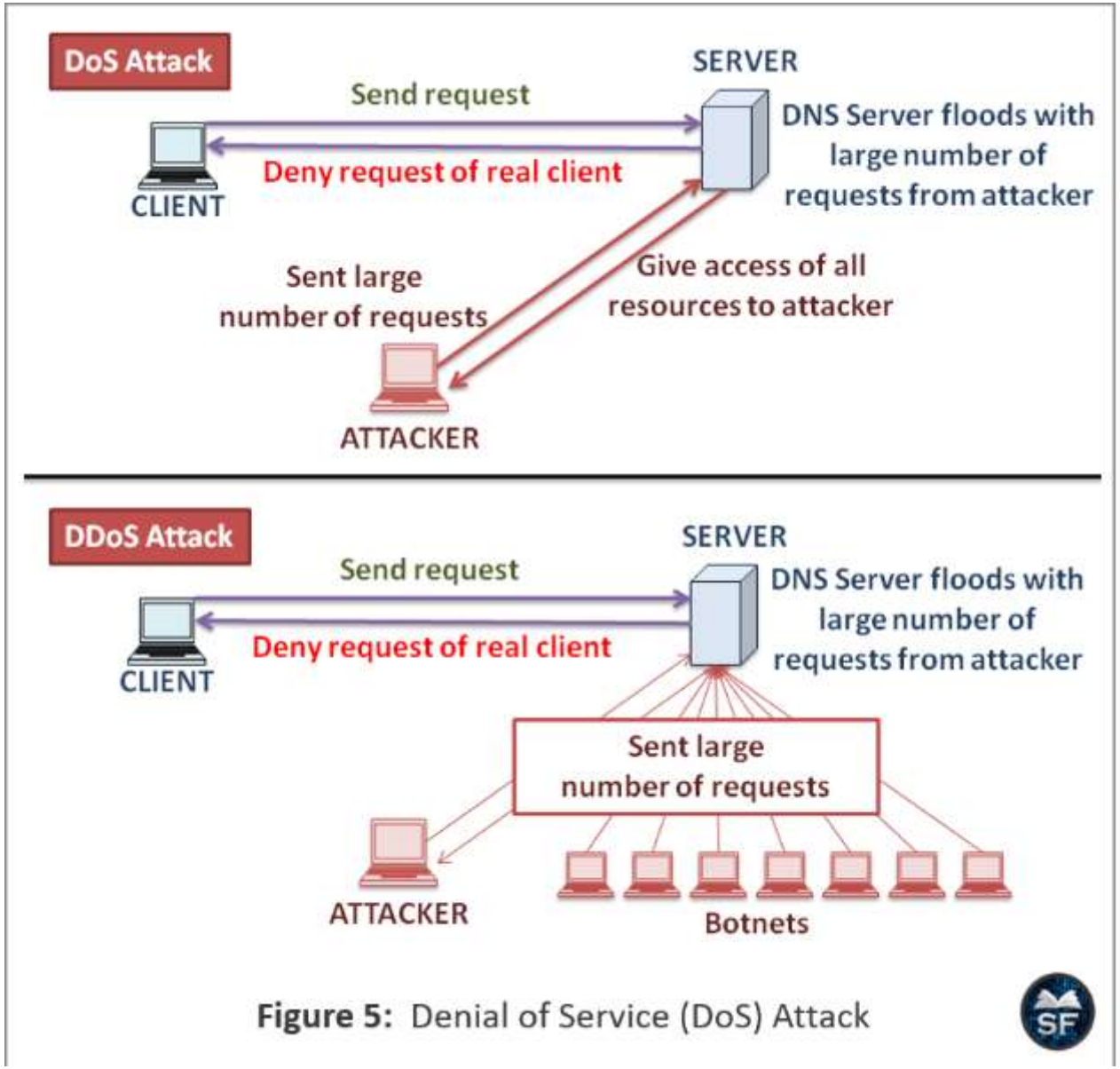


Figure 5: Denial of Service (DoS) Attack

•As shown in the figure, the client wants to access the website running on the server. So, the client sends a request to the server to access the resource, and the server gives the client access to the resource as a response. This is a common scenario.
•In the second figure, the attacker comes into play. As we know, the server can handle a limited number of requests at a time, as each website has a bandwidth that defines the capacity of the load that it can handle at a time.
•The attacker exploits the limited capacity of the server. An attacker creates fake users with fake IP addresses. Here fake users are also known as botnets..
•Botnets are not real users; they are fake users and an attacker sets a different IP address for each botnet.
•Now the hacker or attacker sends a large number of requests from the botnet to the server. In the end, the attacker ties up all the resources on the server.
•After that, if a real user sends a request to the server, the server denies access to the real user because it has already given all resources to the attacker.
•Here, the attacker attacks the server by creating several botnets. Hence, it is known as Distributed Denial of Service attack.
•Due to a DDoS attack, the webserver gets down and the actual users who actually want to access the website cannot access the website.
•If the site is frequently down, or if the site speed is reduced, or there are no resources on the server, a DDoS attack may have occurred.
•By using network monitoring tools, the network administrators can monitor the activity of the network. Firewalls can be used to prevent unauthorized access to webservers. Alerts can be set during threat detection. The last thing that helps prevent a DDoS attack is to regularly update the network and system to fix bugs and issues.

Masquerade Attack

Masquerade attack is one of the active attacks and in this attack, the attacker gains access to an authorized user and uses it to pretend that he is an authorized user.
The diagram below explains the masquerade attack.

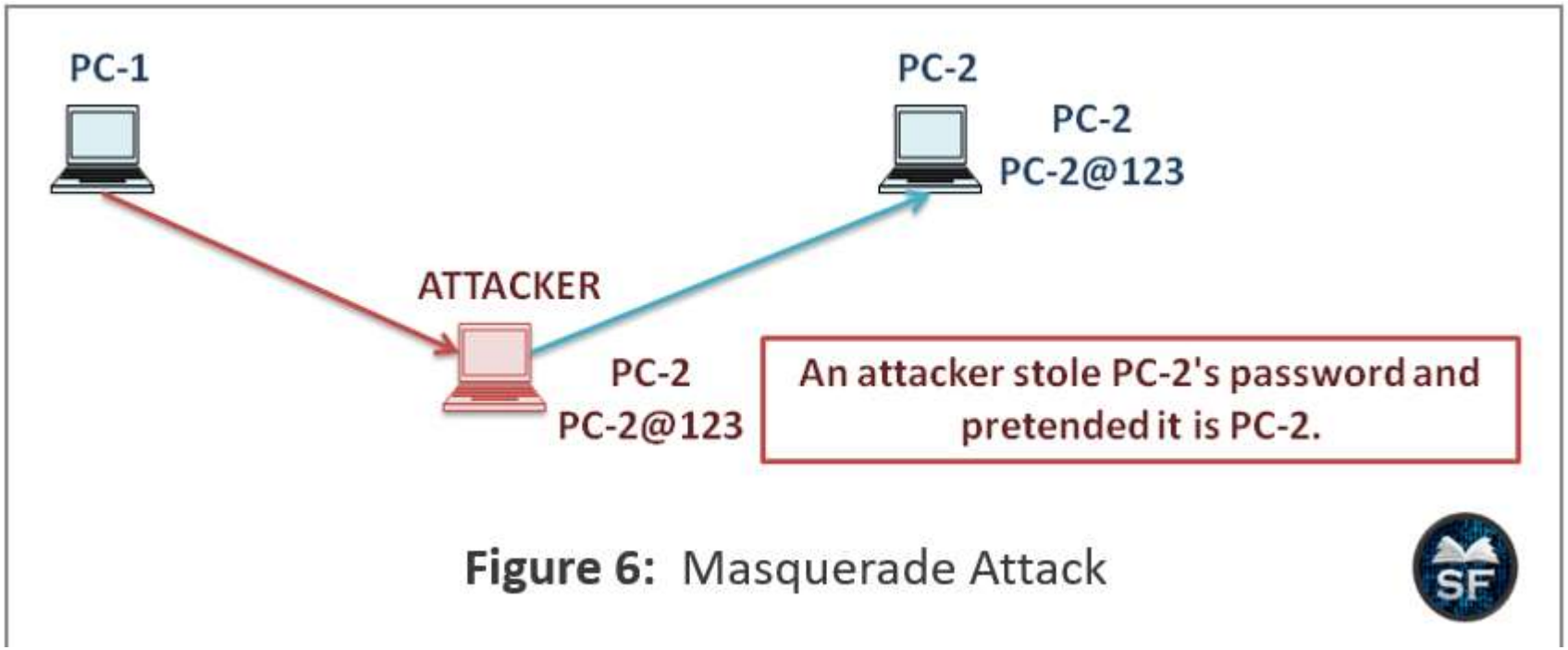


Figure 6: Masquerade Attack

•PC-1 and PC-2 are communicating with each other, and the attacker tries to steal the information.

•The attacker steals PC-2’s username and password and pretends to be PC-2.

•PC-1 thinks the attacker is PC-2, so it sends the message to the attacker instead of PC-2.

•Although each device has a unique IP address, the attacker obtains PC-2’s IP address using spoofing methods and builds trust with PC-1 that it is PC-2.

•Here, the attacker has used the legal information of another PC to compromise security.

•The attacker can get the username and password of the end-user using phishing attacks, brute-force attacks, or dictionary attacks.

•To prevent masquerade attacks, use long and strong passwords, enable two-factor authentication, and remember to log out after communication is complete.

We can also classify the attack based on its origin.

 Inside Attack: If the origin of the threat agent is from the inside the organization, which
may have the authorization and access granted to the resources, but uses it with the
criminal intent.

 Outside Attack: Origin or source of the attack is from the outside of the organization and
gains the unauthorized access to the system or resources with the criminal intent.

A Cyber attack can destroy the business overnight; a proper security defense is required to stop such attacks.

The main focus is to compromise the systems and gain access to sensitive data.

Let us see the top cyber security attack and what do they do

Phishing

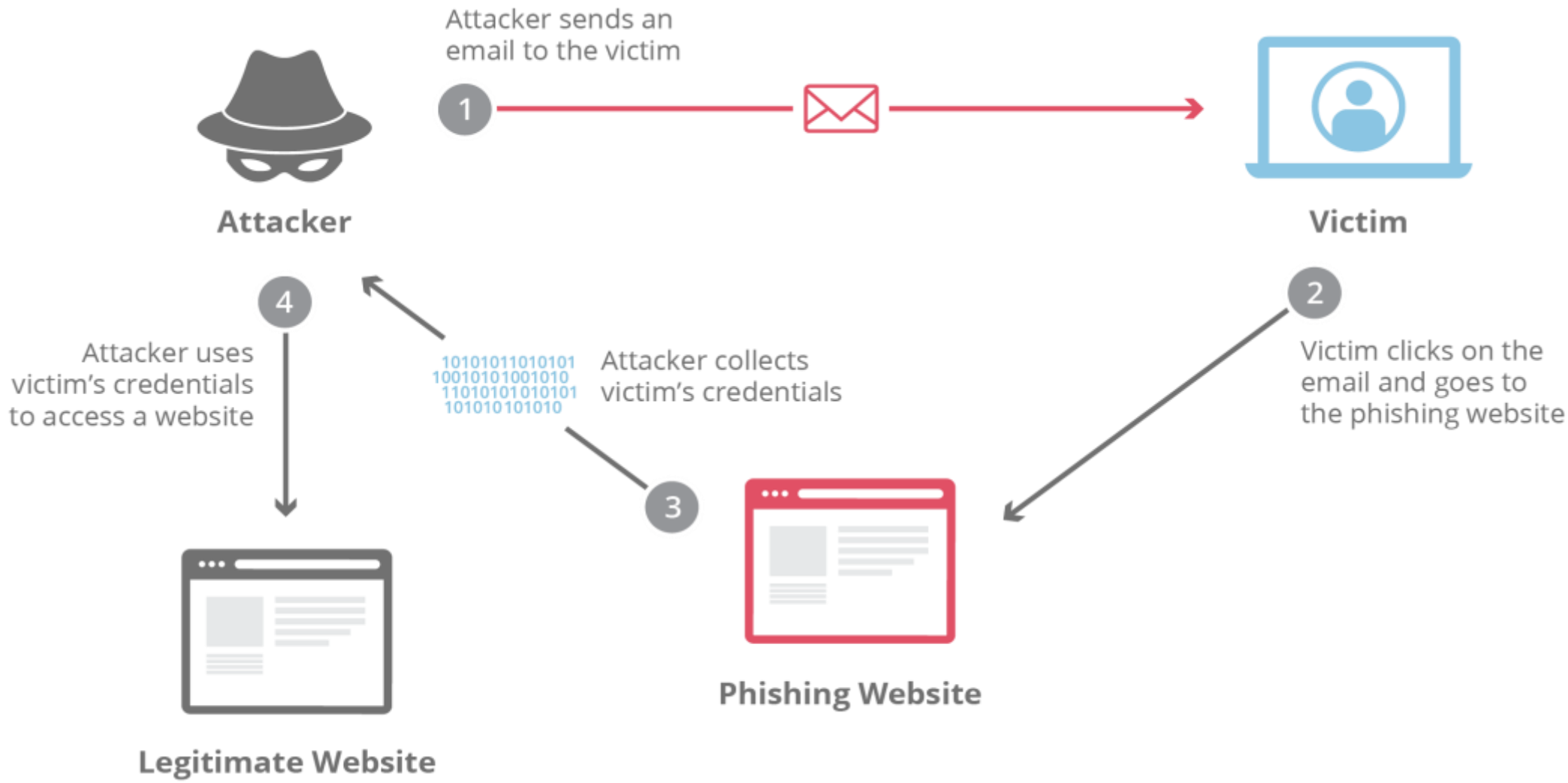
It is a type of security attack that tricks the user to divulge the sensitive and personal/confidential information which is sometimes referred to as “Phishing Scam” also.

- Definitely, every user will not click the links provided in the email id for providing the details, but the attackers are smart they will perform the social engineering and will send the emails to the users with the similar content which user is already looking or interested in it.

- The most targeted business sectors are Payment Platforms, Financial and Banking organizations, Webmail services and Cloud storage/hosting providers.

- Phishing attacks engage users with a specific message and very solicit way for the response from the user which is ideally to click on the link is known as “Call To Action”.

- Which means the attacker wants the user action on the link provided in the email to perform the action


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
3
Attacker collects victim's credentials
10101011010101
10010101001010
11010101010101
10101010101
4
Attacker uses victim's credentials to access a website
Phishing Website
Legitimate Website

Spear phishing

- When a phishing attack is targeted to the specific individuals of the organization, it is known as spear phishing.
- Attackers use the solicit company logo, footer and all other style information which is present in the legit email to trick the user.
- The content of the email mainly focuses on the password reset email or, account reset activity.

Example of spear phishing

An attacker tried to target an employee of NTL World, which is a part of the Virgin Media company, using spear phishing. The attacker claimed that the victim needed to sign a new employee handbook. This was designed to lure them into clicking a link where they would have been asked to submit private information.

For the prevention of the phishing, the user has to check clearly the from address and email content, along with the links present in the email body. Apart from this, employees awareness using various teaching method is the most important as major data breach occurs due to human error which cannot be ignored

Vishing

Vishing, which is short for "voice phishing," is when someone uses the phone to try to steal information. The attacker may pretend to be a trusted friend or relative or to represent them.

Example of vishing

In 2019, there was a vishing campaign that targeted members of the UK’s parliament and their staffers. The attack was part of an assault that involved at least 21 million spam emails targeting UK lawmakers.

Email phishing

In an email phishing scam, the attacker sends an email that looks legitimate, designed to trick the recipient into entering information in reply or on a site that the hacker can use to steal or sell their data.

Email phishing
In an email phishing scam, the attacker sends an email that looks legitimate, designed to trick the recipient into entering information in reply or on a site that the hacker can use to steal or sell their data.

HTTPS phishing

An HTTPS phishing attack is carried out by sending the victim an email with a link to a fake website. The site may then be used to fool the victim into entering their private information.

Example of HTTPS phishing

Hacker group Scarlet Widow searches for the employee emails of companies and then targets them with HTTPS phishing. When the user gets a mostly empty email, they click on the little link that is there, taking the first step into Scarlet Widow's web.

SQL Injection Attack

SQL which is pronounced as “squeal” stands for the structured query language. It’s a programming language used to communicate with databases.
It is used to store critical data of websites/users/services in their databases which can contain personal and sensitive information such as username and password, transaction details.

SQL Injection attack targets the database using specifically crafted SQL statements to trick the system into unexpected and undesired outputs.

SQL Injection attack can be carried out in different ways which can be decided after the attacker identifies system behavior.

If the web application is building a SQL query string dynamically with the account number the user will provide, it might look something like this:
“SELECT * FROM customers WHERE account = ‘“ +userProvidedAccountNumber +”’;”

While this works for users who are properly entering their account number, it leaves the door open for attackers. For example, if someone decided to provide an account number of “‘ or ‘1’ = ‘1”, that would result in a query string of:
“SELECT * FROM customers WHERE account = ‘’ or ‘1’ = ‘1’;”

Due to the ‘1’ = ‘1’ always evaluates to TRUE, sending this statement to the database will result in the data for all customers being returned instead of just a single customer.

The above query might not work for all the database, but it can work where there are less or no security measures taken to filter such SQL injection queries.

Other types of SQL injection attacks include Blind SQL Injection, Out of Bound SQL Injection.

SQL Injection attack can be prevented by avoiding the use of dynamic SQL, sanitize user inputs, don’t store data in plaintext, provide access control and privileges also use of web application firewall is a must

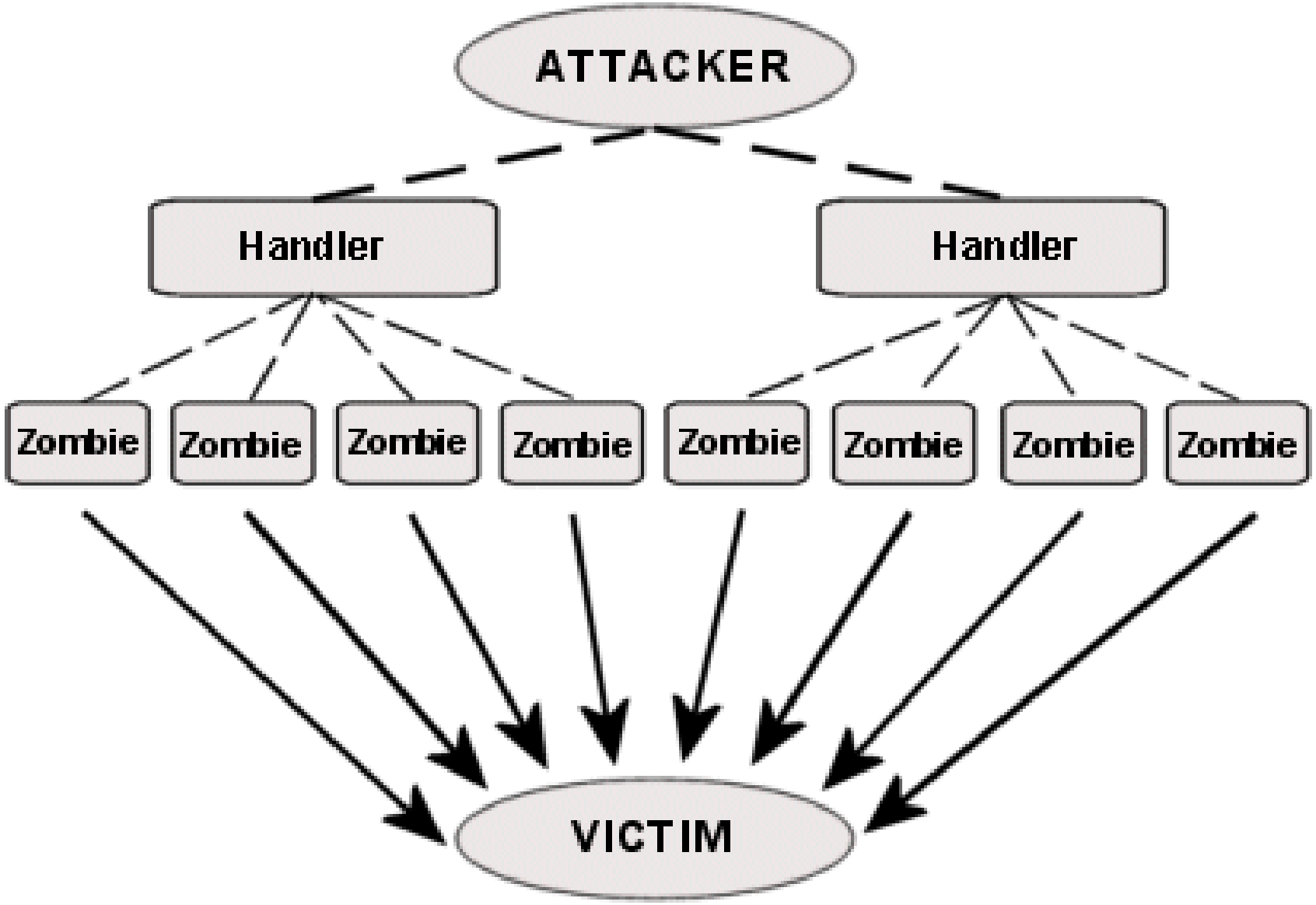
Denial-of-service(DOS) and Distributed Denial of Service(DDOS)

Denial-of-Service attack focus on disrupting or preventing legitimate users from accessing the websites or application or any other resources by sending flood of messages, packets, & connection requests, causing the target to slow down or “crash”, rendering it unavailable to its users.

Attacker mostly targets high-end value organizations such as media houses,banking, and financial organization, E-Commerce to disrupt their services.

When the majority of present-day DoS attacks involve a number of systems (even into the hundreds of thousands) under the attacker’s control which are installed with the bots, all simultaneously attacking the target. This coordination of attacking systems is referred to as a “Distributed Denial-of-Service” (DDoS).

Architecture of a DDoS Attack



Man-In-The-Middle Attack and Session Hijacking:

Man-in-the-middle attacks are a common type of cyber security attack that allows attackers to eavesdrop on the communication between two targets.

The attack takes place in between two legitimately communicating hosts, allowing the attacker to “listen” to a conversation they should normally not be able to listen.

When a user is using the internet and our computer performs a lot back and forth transaction, the application generates and uses a session ID which will be unique and to make the transactions private between user and application.

The attacker hijacks the session ID to eavesdrop the communication between user and application.

There are various types of Man-In-The-Middle Attack such as Rogue access points, ARP Spoofing, DNS Spoofing, Packet Injection, SSL Striping.

We can prevent such attacks by using strong WEP/WAP encryption on access points, using a virtual private network(VPN), enforce https and using a strong combination of the public key pair authentication.

A **Rogue Access Point (RAP)** is a wireless access point that is either installed on a secure network without authorization from the network administrator or is installed maliciously by an attacker to intercept sensitive information. Rogue access points are a significant security threat to wireless networks.

Types of Rogue Access Points:

1.Unauthorized Access Point:

1. Set up by employees for convenience without the knowledge or approval of IT administrators.
2. These devices often lack proper security configurations, making the network vulnerable to attacks.

2.Malicious Access Point:

1. Set up by attackers to mimic legitimate access points.
2. Used to perform **Man-in-the-Middle (MITM)** attacks, steal credentials, or inject malware into the network.

ARP Spoofing (also known as ARP Cache Poisoning) is a type of cyberattack where an attacker sends falsified Address Resolution Protocol (ARP) messages over a local area network (LAN).

This allows the attacker to link their MAC address to the IP address of another device, typically a gateway or a victim's device, enabling them to intercept, modify, or disrupt data being transmitted within the network.

ARP Spoofing Working:

ARP Basics:The ARP protocol maps IP addresses (logical addresses) to MAC addresses (physical addresses) within a network.

Devices store these mappings in an ARP table for faster communication.

Spoofing Process:

The attacker sends forged ARP replies to the network, associating their MAC address with the IP address of a target (e.g., a gateway or victim).As a result, traffic intended for the target device (e.g., the gateway) is redirected to the attacker's machine.

Brute Force Attack

- A Brute Force Attack is a trial-and-error method used by attackers to crack passwords, encryption keys, or login credentials. The attacker systematically tries every possible combination until the correct one is found. Although it's simple, brute force attacks can be highly effective, especially against weak passwords or improperly secured systems.

Brute Force Attacks Explained

In a brute force attack, a cybercriminal uses trial and error to try and break into a device, network, or website.

An attacker **utilizes a hacking tool.**

The hacking tool **attempts multiple logins.**

The system **returns a valid or invalid response.**

Types of Brute Force Attacks:

•**Simple Brute Force Attack**:
The attacker tries all possible combinations of passwords or keys without any optimization.
For example, attempting "0000", "0001", "0002", etc., for a 4-digit PIN.
•**Dictionary Attack**:
The attacker uses a precompiled list of commonly used passwords (a "dictionary") to guess credentials.
These lists often include weak or default passwords like "password123" or "admin".
•**Hybrid Brute Force Attack**:
A combination of dictionary and brute force techniques.
The attacker might append numbers or special characters to dictionary words
(e.g., "password123!", "admin2023").
•**Reverse Brute Force Attack**:
Instead of guessing passwords for a specific user, the attacker uses a common password (e.g., "123456")
and tries it on many user accounts.
•**Credential Stuffing**:
Reusing credentials from previous data breaches on other platforms, leveraging users' habit of reusing
passwords.
•**Rainbow Table Attack**:
Involves precomputed hash values of common passwords.
Instead of guessing passwords, the attacker matches hashes to crack the password.

Malware Attack

- Malware can be described as Malicious software that is installed in your system without your consent. It can attach itself to the legitimate process or replicate itself or can put itself to startup. The objective of the malware could be to exfiltrate information, disrupt business operations, demand payment

Types of Malware

- Macro Virus: These viruses infect applications such as Microsoft Word or Excel. Macro viruses attach to an application's initialization sequence. When the application is opened, the virus executes instructions before transferring control to the application. The virus replicates itself and attaches to other code in the computer system.

- **Example: MyDoom**
  - **Description**: MyDoom is one of the most well-known computer viruses that spreads through email attachments. When executed, it infects the system and replicates itself, sending infected emails to other users in the victim's address book.
  - **Impact**: It caused widespread email disruptions and was also used to launch a **denial-of-service (DDoS)** attack against websites, including the website of Microsoft.

- **Trojans:** A Trojan or a Trojan horse is a program that hides in a useful program and usually has a malicious function. A major difference between viruses and Trojans is that Trojans do not self-replicate. In addition to launching attacks on a system, a Trojan can establish a back door that can be exploited by attackers

- **Example: Emotet**
  - **Description**: Emotet started as a banking Trojan but evolved into a modular malware distribution platform. It is typically delivered via email attachments or links disguised as legitimate communications.

  - **Impact**: Emotet steals sensitive financial data and often installs other types of malware (such as ransomware). It is known for distributing payloads like **Ryuk** ransomware and **TrickBot**.

- Worms: Worms differ from viruses in that they do not attach to a host file, but are self-contained programs that propagate across networks and computers. A 22 typical worm exploit involves the worm sending a copy of itself to every contact in an infected computer's email address In addition to conducting malicious activities, a worm can result in denial-of-service attacks against nodes on the network.

- **Example: Conficker**
  - **Description**: Conficker is a worm that spreads through Microsoft Windows vulnerabilities, particularly an unpatched flaw in the **Windows SMB protocol**. It does not require human intervention to spread, as it exploits network connections to propagate.
  - **Impact**: Conficker infected millions of computers across the world and turned them into a botnet, which was used for spamming, spreading malware, and launching other attacks.

- Dropper: A dropper is a program used to install viruses on computers. In many instances, the dropper is not infected with malicious code and, therefore might not be detected by virus-scanning software. A dropper can also connect to the internet and download updates to virus software that is resident on a compromised system.

- Ransomware:Ransomware is a type of malware that blocks access to the victim’s data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion and asks for the payment in bitcoinWhich encrypts the victim’s files in a way that makes them nearly impossible to recover without the decryption key or using the decryptor if it is available.

- **Example: WannaCry**
  - **Description**: WannaCry was a massive ransomware attack in 2017 that exploited a zero-day vulnerability in **Microsoft Windows' SMB protocol**. Once executed, WannaCry encrypted files on the infected systems and demanded a ransom payment in Bitcoin.

  - **Impact**: It affected hundreds of thousands of computers worldwide, including critical infrastructure like hospitals, disrupting operations and causing significant financial losses.

- Adware: Adware is a software application used by companies for marketing purposes; advertising banners are displayed while any program is running. Adware can be automatically downloaded to your system while browsing any website and can be viewed through pop-up windows or through a bar that appears on the computer screen automatically.

- **Example:**
- **Fireball**
- **Description**: Fireball is a type of adware that takes control of the infected browser, hijacks search engines, and redirects web traffic to malicious websites to serve ads. It was typically bundled with legitimate software downloads, often without the user's knowledge.
- **Impact**: It generated revenue by driving traffic to malicious websites and injecting ads into browsing sessions, but could also track user behavior and invade privacy.

- Spyware: Spyware is a type of program that is installed to collect information about users, their computers or their browsing history. It tracks everything you do without your knowledge and sends the data to a remote user. It also can download and install other malicious programs from the internet. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware application.

  - **Example: Pegasus**
  - **Description**: Pegasus is a sophisticated spyware tool developed by the Israeli company **NSO Group**, primarily used for surveillance. It exploits zero-day vulnerabilities to infect devices (mainly smartphones) and can track calls, messages, emails, and even activate microphones and cameras.

  - **Impact**: It has been used in high-profile surveillance cases, targeting journalists, activists, and political figures across the globe.

- **Rootkits**: Malicious software that gains administrative control over a system while hiding its presence.

- **Example: Stuxnet**
  - **Description**: Stuxnet is a sophisticated **computer worm** that included rootkit functionality. It was designed to infect industrial control systems, particularly those used in Iran's nuclear facilities. It hid its presence by using rootkit techniques and altered the functioning of the targeted systems.

  - **Impact**: Stuxnet caused physical damage to industrial equipment, such as centrifuges used in uranium enrichment, marking one of the first known cyberattacks that targeted critical infrastructure.

- **Bots**: Automated programs used for malicious activities, often forming a botnet.

- **Example: Mirai**
- **Description**: Mirai is a malware that turns IoT (Internet of Things) devices into bots, forming a botnet. It was initially spread through weak default passwords on IoT devices like cameras, routers, and DVRs.
- **Impact**: The **Mirai botnet** was used to launch massive **DDoS (Distributed Denial of Service) attacks**, including the attack on **Dyn**, a major DNS provider, which disrupted services for websites like Twitter, Netflix, and Reddit.

- **Keyloggers**: Software that tracks and records keystrokes to capture sensitive data like passwords.
- **Example: Revealer Keylogger**
  - **Description**: Revealer Keylogger is a type of malware that records all keystrokes on a compromised system. It operates covertly in the background, capturing everything typed by the user, including passwords, credit card numbers, and personal messages.
  - **Impact**: It can be used for identity theft, banking fraud, or espionage by capturing sensitive personal information without the victim's knowledge.

Zero-Day Exploit

- A **zero-day exploit** refers to a security vulnerability in software or hardware that is unknown to the vendor or developer, or that has not yet been patched or fixed. These exploits are called "zero-day" because they are discovered and leveraged by attackers before the vendor or security community has had "zero days" to address and patch the vulnerability.

Common Uses of Zero-Day Exploits

- **Targeted Attacks**
- Zero-day exploits are commonly used in targeted attacks, such as **advanced persistent threats (APTs)**, where attackers are focusing on a specific organization or individual.
- Example: State-sponsored groups using zero-day exploits to breach governments, military organizations, or critical infrastructure.
- **Cybercrime and Ransomware**
- Cybercriminals may use zero-day exploits to gain access to systems and deploy ransomware, steal data, or disable systems for financial gain.
- Example: A ransomware attack using an unpatched vulnerability to encrypt files before the victim can even recognize the threat.

- **Espionage and Surveillance**
- Zero-day exploits can be used for espionage, allowing attackers to silently monitor and steal sensitive information from a target.
- Example: **Stuxnet** used multiple zero-day vulnerabilities to target and sabotage Iran's nuclear program.

- **Widespread Worms and Malware**
- Zero-day exploits are often leveraged to create worms or malware that spread rapidly across networks, infecting multiple systems before defenses can be updated.
- Example: **Conficker worm** used zero-day vulnerabilities to spread in 2008 and became one of the most widespread computer worms in history.

Malware Infection Vectors

- **Email Attachments**: Malware often spreads through phishing emails with malicious attachments.
- **Websites and Downloads**: Malicious websites or infected downloads (via exploit kits or Trojans).
- **Removable Media**: USB drives or other external storage can carry and spread malware.
- **Exploiting Vulnerabilities**: Malware can exploit unpatched software or system vulnerabilities to enter a device.
- **Social Engineering**: Trick users into clicking on links, opening files, or executing harmful commands.