

CYBER SECURITY

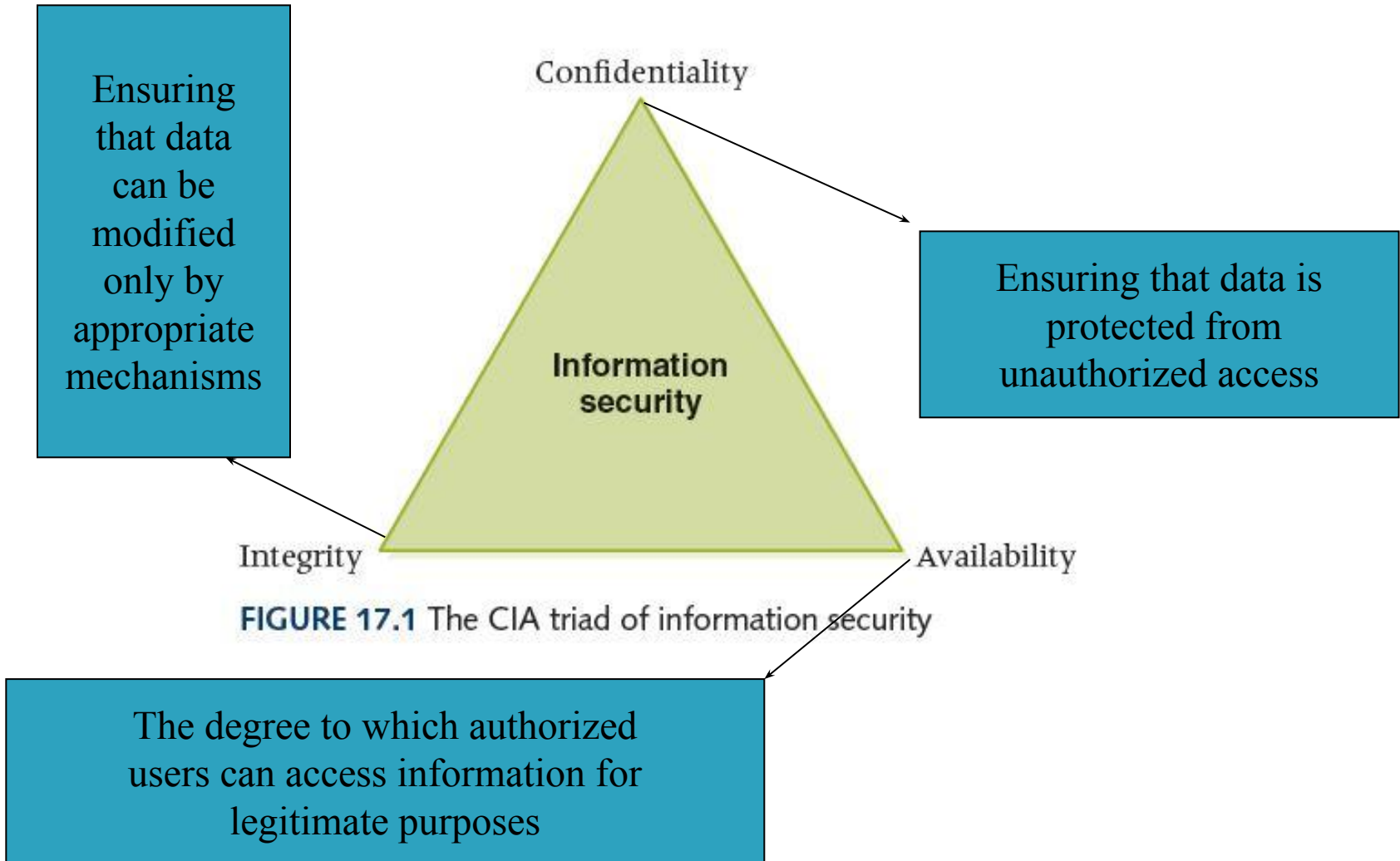
INTRODUCTION TO COMPUTER SECURITY

Foundations of Computer Security

Computer security, Cyber security or Information technology security (IT security) is the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.

Security basics / Goals of Security:

CIA model of computer Security



CIA Model

- A simple but widely-applicable security model is the CIA triad standing for:
 - ❖ Confidentiality
 - ❖ Integrity
 - ❖ Availability
- These are the three key principles which should be guaranteed in any kind of secure system.
- This principle is applicable across the whole subject
- If any one of the three can be breached it can have serious consequences for the parties concerned.

Confidentiality

- Confidentiality is the ability to hide information from those people who are unauthorized to view it.
- It is perhaps the most obvious aspect of the CIA triad when it comes to security; but correspondingly, it is also the one which is attacked most often.
- Example:- Cryptography and Encryption methods are an example of an attempt to ensure confidentiality of data transferred from one computer to another.

Integrity

- The ability to ensure that data is an accurate and unchanged representation of the original secure information.
- The assurance that data and systems are trustworthy and free from unauthorized modification or corruption
- Example:- Using checksum or hashing to ensure data is not tampered.

Availability

- It is important to ensure that the information concerned is readily accessible to the authorized viewer at all times.
- ensuring that authorized users have timely and reliable access to information and resources when needed
- Example:- Creating backup servers or proxy servers to make sure that data is available to clients at any time.

Security Basics

- Accountability
- Nonrepudiation
- Reliability
- Authentication

Accountability

- It offers **administrators**, the ability to **track the activities** that users performed at a certain situation.
- It is a primary method to view what services were utilized and how much resources were used up by users.
- Example:- Logging and monitoring user activities.

Non-Repudiation

- ❑ Non repudiation is the assurance that someone cannot deny something.
- ❑ Typically, non repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
- ❑ Example:- Digital Signature

Reliability

- Ability of a system or organization's security measures to consistently and effectively prevent, detect, and respond to cyber threats.
- Example:- Gmail, Quick heal antivirus.

Authentication

- The process of verifying the identity of a user, device, or system before granting access to resources or information
- Identity verification is implemented in three general ways:
 - ❖ Knowledge: Something You Know – based on user knowledge
 - ❖ Ownership: Something You Have - based on user ownership
 - ❖ Characteristics: Something You Are – based on user characteristics

Example:- Fingerprint, Adhar, password

Threat to Security:

Malware, short for malicious software, refers to any software designed to harm or exploit computer systems, networks, or devices.

- ❑ Viruses
- ❑ Worms
- ❑ Trojan horse
- ❑ Intruders
- ❑ Insiders
- ❑ Ransomware

Virus

- Self-replicating code, attaches itself to another program and executes secretly when the host program is executed.



Phases of a Virus (Life cycle)

- **Dormant** - The virus enters the system, often hidden within another program or file, and remains inactive, waiting for a specific trigger.
- **Propagation** - The virus replicates itself, creating copies that can infect other programs, files, or even other computers on a network
- **Trigger** - A specific event, such as a date, time, or user action, activates the virus and initiates its malicious behavior.
- **Execution** - The virus carries out its intended harmful actions, which could involve deleting files, corrupting data, slowing down the system, or even stealing information.

Types of Viruses



- On the basis of target
- **Boot Sector Infector:** Infects master boot record / boot record (boot sector) of a disk and spreads when a system is booted with an infected disk (original DOS viruses). They are **Memory--resident Virus**.
- **File Infector :** Infects executable files, they are also called **Parasitic Virus** as they attach their self to executable files as part of their code. Runs whenever the host program is executed.
- **Macro Virus** –Infects files with macro code that is interpreted by the relevant application, such as doc or excel files.

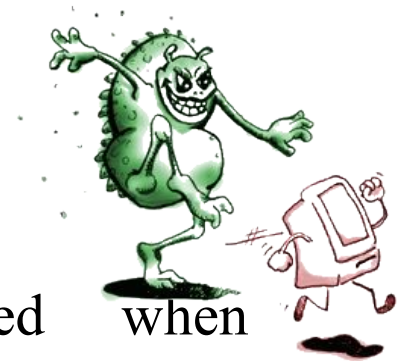
Types of Viruses



- On the basis of concealment strategy
- **Encrypted Virus** – A portion of virus creates a random encryption key and encrypts the remainder of the virus. The key is stored with the virus. When the virus replicates, a different random key is generated.
- **Stealth Virus** -- explicitly designed to hide from Virus Scanning programs.
- **Polymorphic Virus** -- mutates with every new host to prevent signature detection, signature detection is useless.
- **Metamorphic Virus** – Rewrites itself completely with every new host, may change their behavior and appearance.

Email Virus

- Moves around in e-mail messages, triggered when user opens attachment
- Do local damages on the user's system
- Propagates very quickly
- Replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book



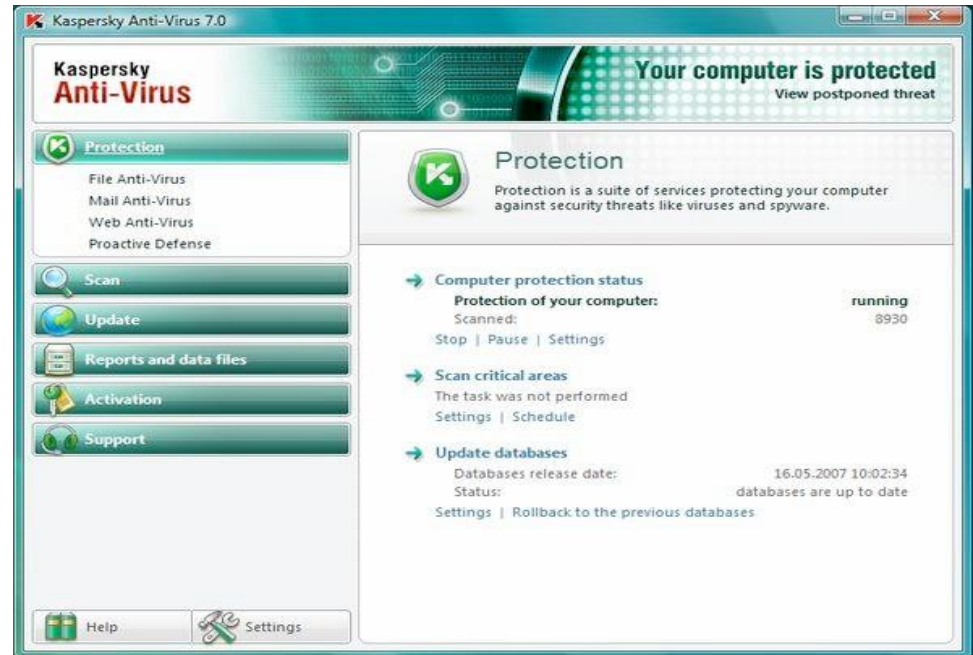
Examples of risky file types

- The following file types should never be opened if...
 - .EXE
 - .PIF
 - .BAT
 - .VBS
 - .COM

Anti-virus



- It is not possible to build a perfect virus/malware detector.
- Analyze system behavior
- Analyze code to decide if it a virus
- Type :
 - Scanner
 - Real time monitor



Worm

A computer worm is a self-replicating computer virus. It uses a network to send copies of itself to other nodes and do so without any user intervention.



Worm



- Runs independently
 - Does not require a host program
- Propagates a fully working version of itself to other machines

History

- Morris worm was one of the first worms distributed over Internet

Two examples

- Morris – 1998,
- Slammer – 2003

Feature	Virus	Worm
Spreading Mechanism	Requires a host program to run and spread; attaches to executable files	Self-replicating and spreads independently across networks
Replication	Relies on user action to spread (e.g., opening an infected file)	Does not require user interaction to replicate and spread
Impact	Can modify, corrupt, or delete files; may cause system instability	Primarily consumes system resources (bandwidth, memory) and can cause network congestion
Speed of Spread	Generally slower than worms	Can spread rapidly across networks, often exploiting vulnerabilities
Examples	File infectors, boot sector viruses, macro viruses	Internet worms, email worms, file-sharing network worms
Detection and Removal	Antivirus software can detect and remove viruses after they have spread	Can be more challenging to detect due to autonomous spreading and may require robust network security measures

Intruders

- An Intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system.
- In summary, this person attempts to violate Security by interfering with system Availability, data Integrity or data Confidentiality.

Insiders :

- ❑ An Insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.
- ❑ The threat may involve fraud, the theft of confidential or commercially valuable information.
- ❑ Example:-In 2023, insider threat examples from household company names continue to make headlines – and that includes electric vehicle giant Tesla. Tesla suffered a major data breach that was orchestrated by two former employees, who leaked sensitive personal data to a foreign media outlet. The leaked information included names, addresses, phone numbers, employment records, and social security numbers of over 75,000 current and former employees.

Insiders are more dangerous than outside intruders.

- They have the access and knowledge necessary to cause immediate damage to an organization.
- Most security is designed to protect against outside intruders and thus lies at the boundary between the organization and the rest of the world.
- Besides employees, insiders also include a number of other individuals who have physical access to facilities.

Comparison:

Feature	Insider	Intruder
Access	Authorized	Unauthorized
Origin	Internal to the organization	External to the organization
Motivation	malicious intent, negligence	financial gain
Knowledge	In-depth knowledge of the system and its security	Limited knowledge of the system initially
Examples	Employee stealing data, disgruntled contractor sabotaging a system	Hacker exploiting a vulnerability, phishing attack
Detection Difficulty	Can be difficult to detect, as they may not trigger typical security alerts	Easier to detect, as their actions often trigger alarms

Trojan Horse:

- ❑ A Trojan horse, or Trojan, is a type of malicious software (malware) that disguises itself as a legitimate program to trick users into installing it.
- ❑ Unlike viruses, Trojans cannot replicate themselves. They are designed to harm, disrupt, steal, or cause other damage to data or systems.
- ❑ Example: The Zeus Trojan is one of the oldest malware programs used to steal targeted victims' banking details. The creator sold the Zeus code to a competitor, but several variants were released over the years

Ransomware:

- ❑ Ransomware is a type of malicious software (malware) that restricts access to a computer system or the files on it, typically by encrypting them. Attackers then demand a ransom payment from the victim in exchange for restoring access or decryption.
- ❑ Example-Telangana and Andhra Pradesh, two southern states in India, got hit by a ransomware attack on their power utility systems last year. The malicious virus took down all the servers until the glitch was resolved. Since the computer systems of the two states were interlinked, the virus spread quickly, leading to a complete shutdown of all systems.

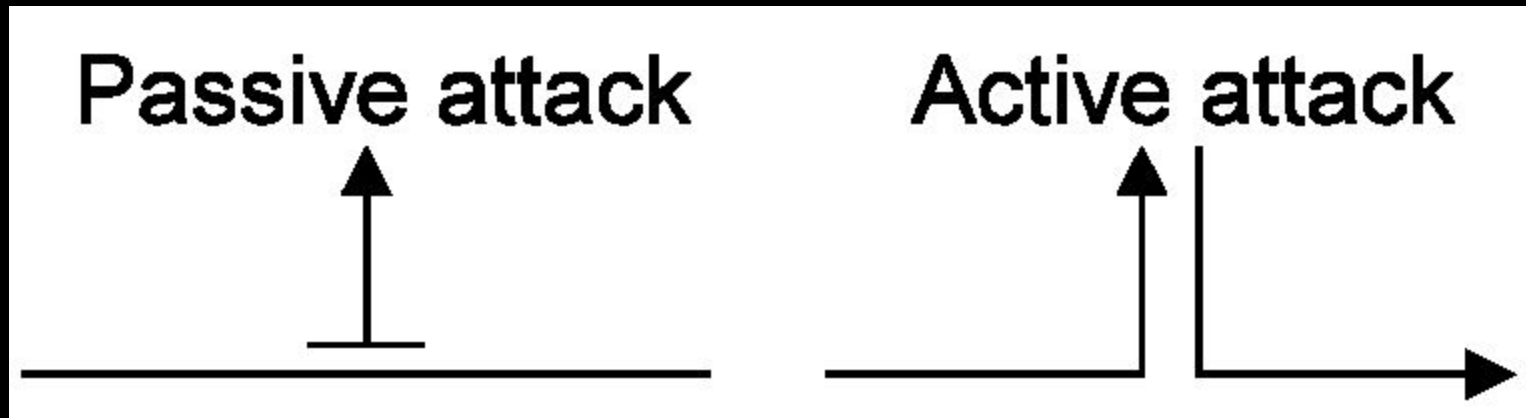
Types of Attacks

- Computer Security attacks can be classified into two broad categories:

Passive Attacks can only observe communications or data.

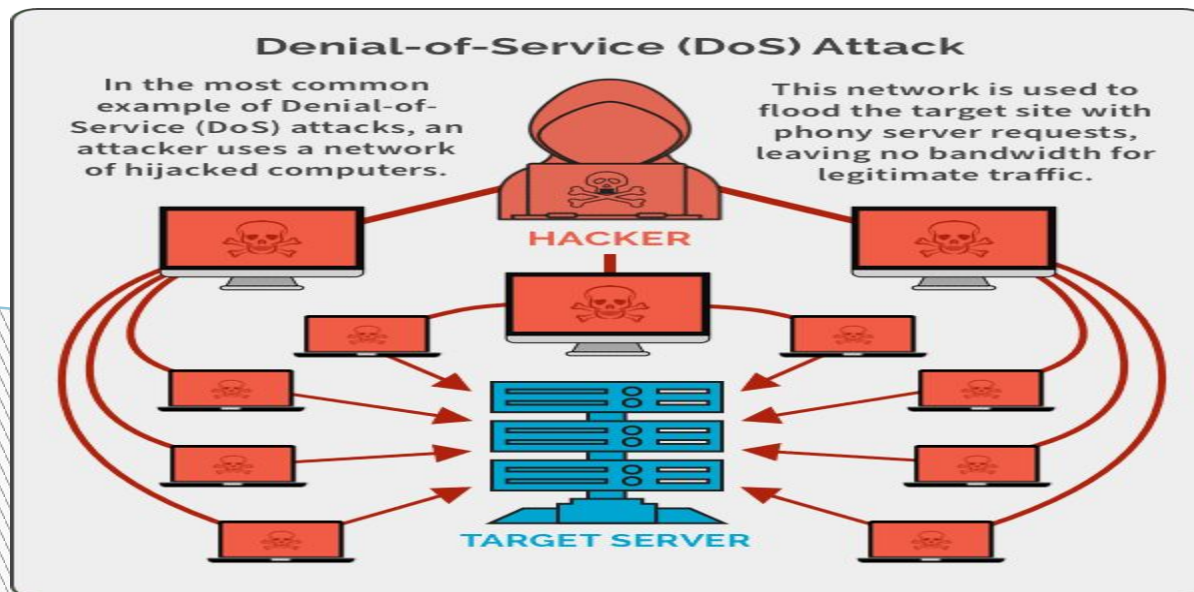
Active Attacks can actively modify communications or data. Often difficult to perform, but very powerful.

Passive Attacks and Active Attacks



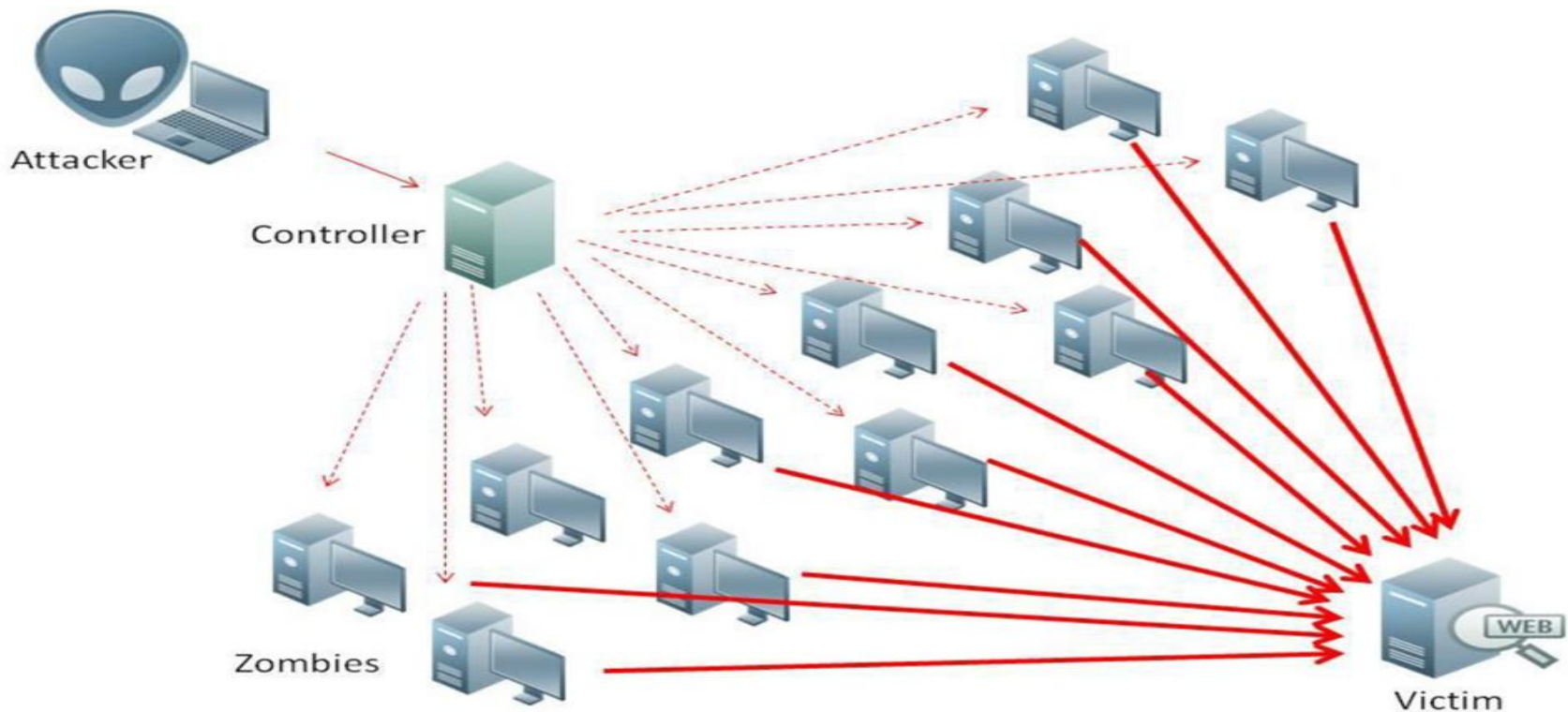
Denial of service

A **Denial of Service (DoS)** attack is a type of **cyberattack** in which an attacker attempts to make a machine, network, or service **unavailable** to its intended users by **overwhelming it with traffic** or sending information that triggers a **crash**.



DDOS - Distributed Denial of Service attack

A **type of cyberattack** where multiple systems (often part of a **botnet**) flood a target—like a website, server, or network—with massive amounts of traffic to **overwhelm** and **shut it down**.

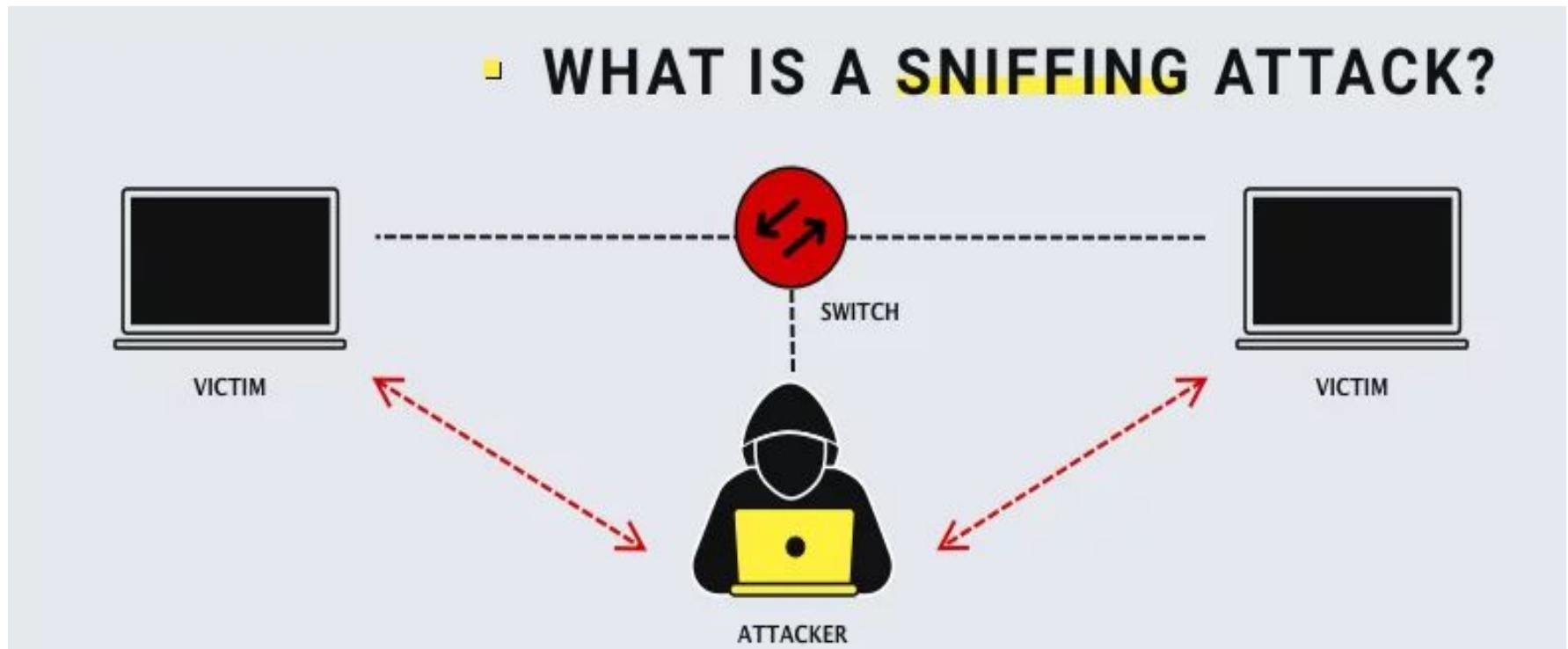


Backdoors and Trapdoors






- Both **backdoors** and **trapdoors** are ways to bypass normal authentication or security mechanisms in a system, but they differ slightly in how and why they are used.
- A **backdoor** is a **hidden method** of accessing a system or software, typically **without the user's knowledge**. It allows attackers (or sometimes developers) to **bypass normal authentication or security checks**.
- A **trapdoor** (also called a **trap backdoor**) is a **type of backdoor**, typically inserted **during software development**. It activates only under **specific conditions**.

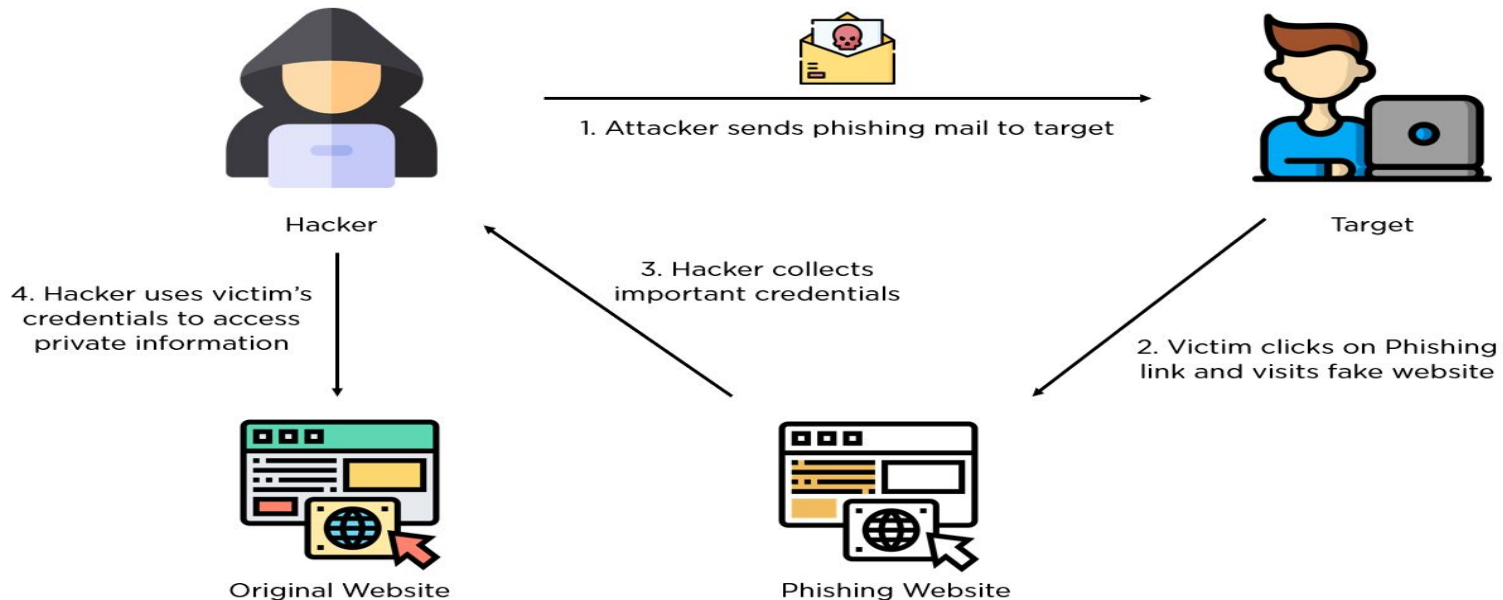
Sniffing

- **Sniffing** is the act of **monitoring and capturing data packets** that travel across a network. It can be used for **legitimate network troubleshooting**, but it's also a common technique used by **attackers** to steal sensitive data.



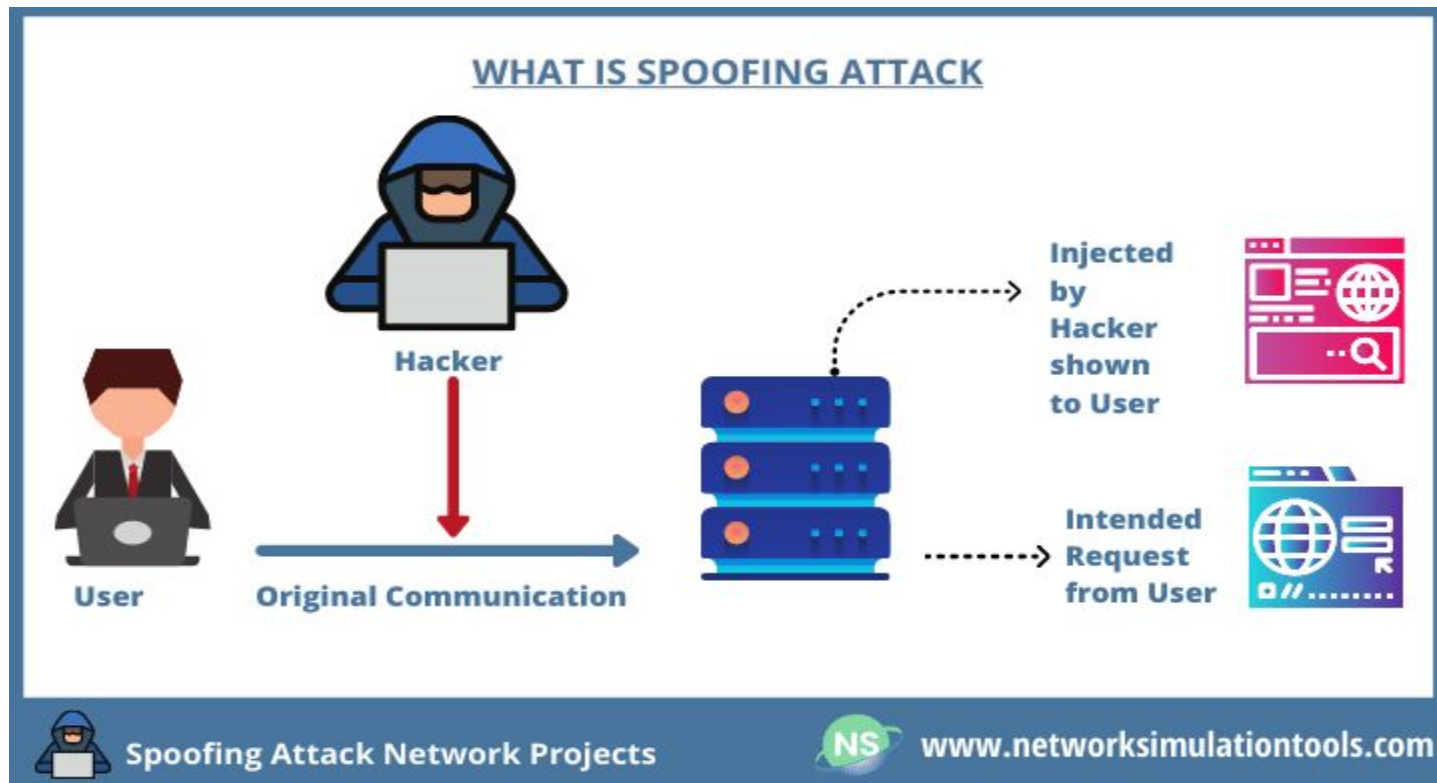
Phishing

- ❑ **Phishing** is a type of **social engineering attack** where an attacker **pretends to be a trustworthy entity** (like a bank, government agency, or company) to **trick users into revealing sensitive information**, such as:
 - ❑  Email addresses
 - ❑  Passwords
 - ❑  Credit card numbers
 - ❑  Social security numbers
 - ❑  Login credentials



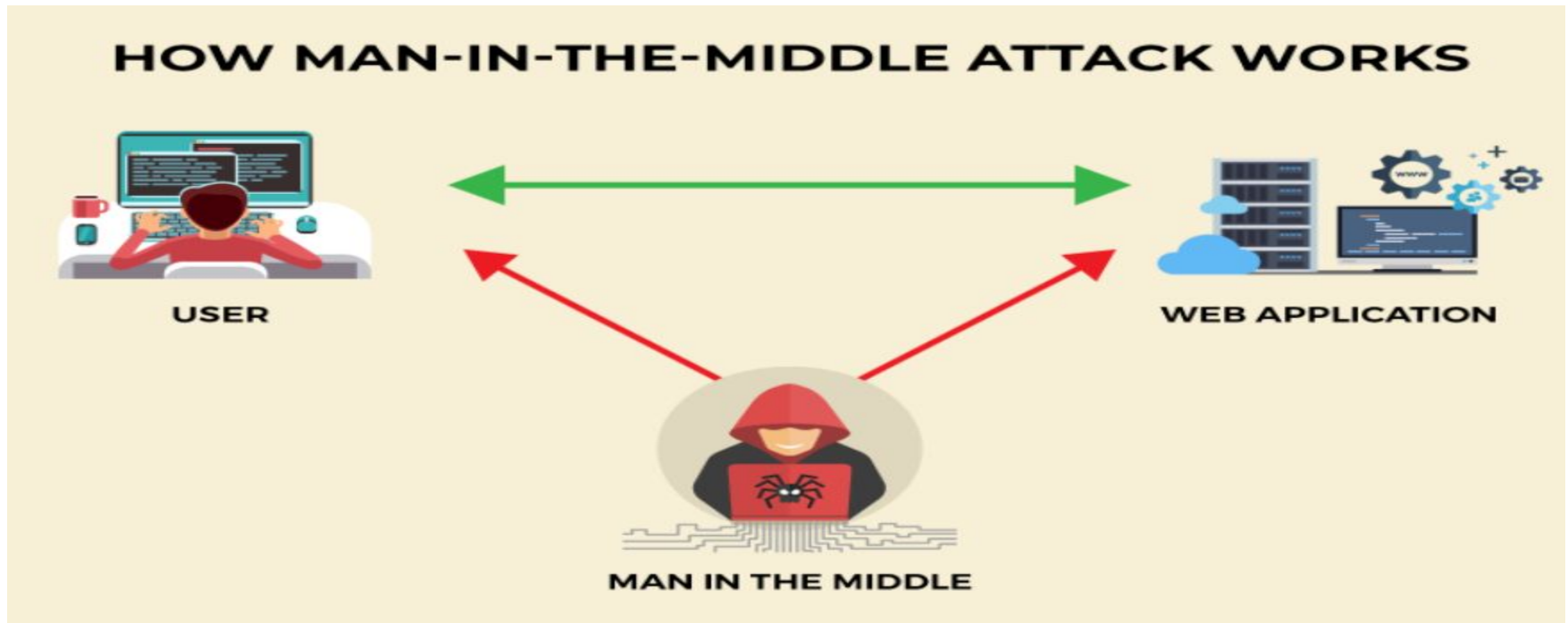
Spoofting

- ❑ **Spoofting** is a type of cyberattack where an attacker **pretends to be someone or something else** to gain access, trick users, or steal data. The goal is to **deceive** a system or user into **trusting a fake identity**.



Man in the middle

- A **Man-in-the-Middle (MITM) attack** is a type of cyberattack where an attacker **secretly intercepts, alters, or relays communication** between two parties who believe they are communicating directly with each other.

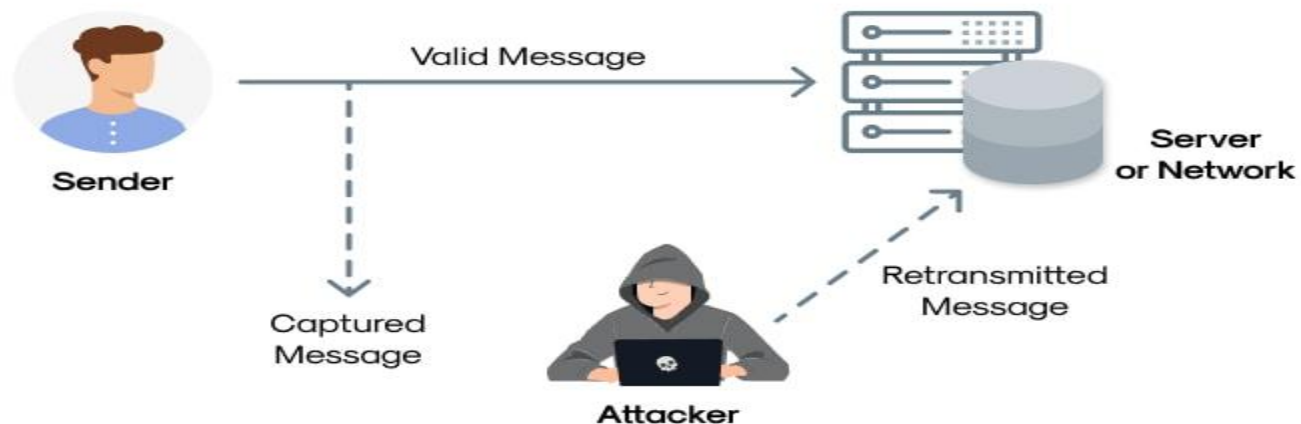


Replay

- A **Replay Attack** is a type of **network attack** where a **valid data transmission is maliciously captured and resent (replayed)** by an attacker to trick the recipient into **unauthorized actions or access**.

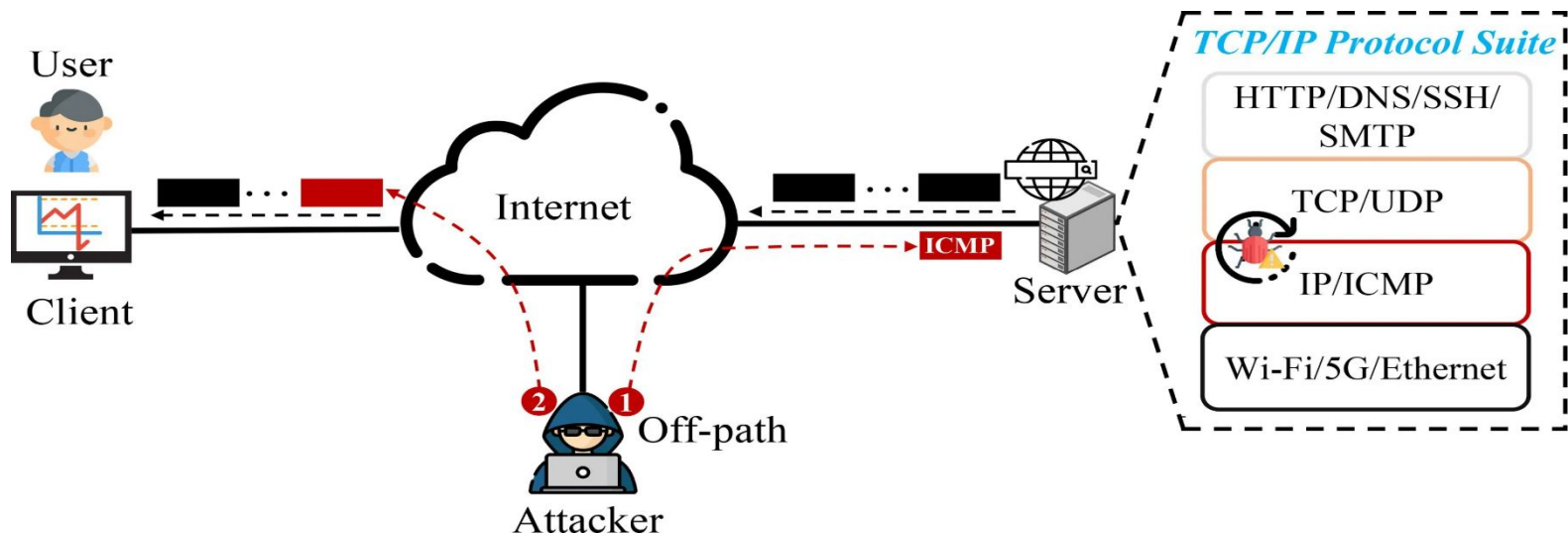


The Anatomy of a Replay Attack



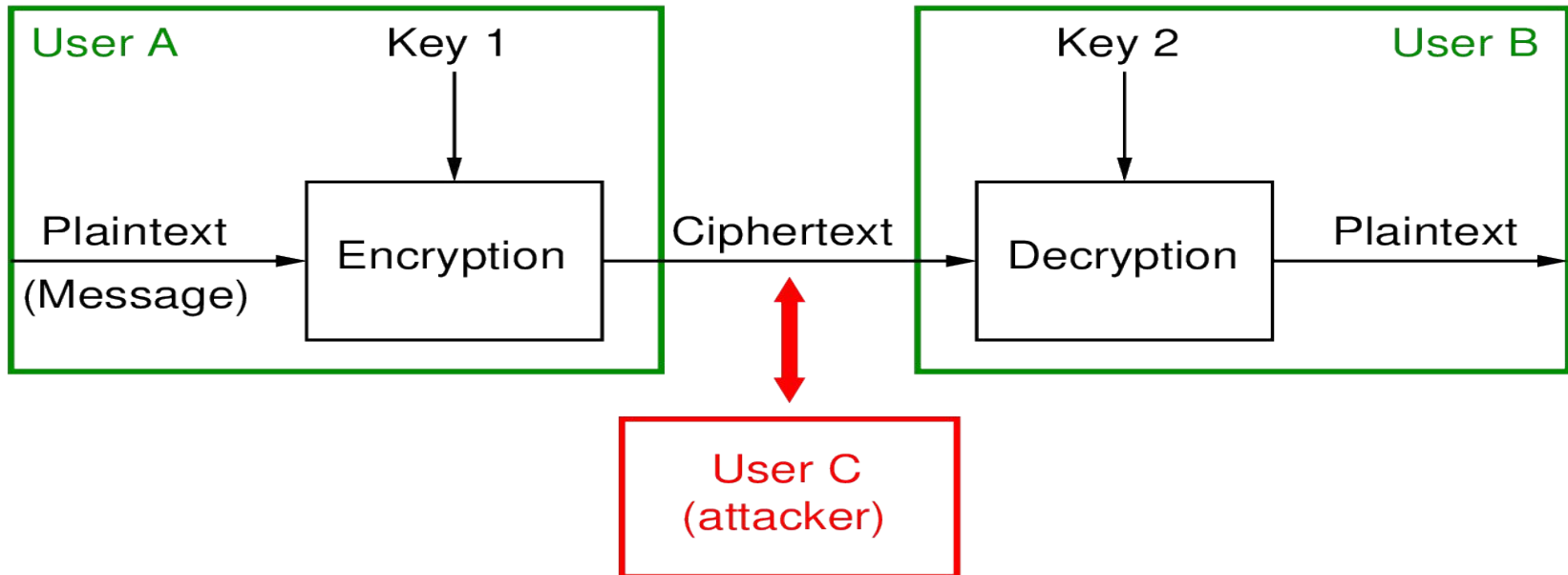
TCP/IP Hacking

- This is a attack where an authorized user can gain access to another user's or client's authorized network connection. After hijacking a TCP/IP session, an attacker is able to easily read and modify the transferred packets and the hacker is also able to send its own requests to the user.



Encryption attacks

- ❑ **Encryption attacks** are techniques used by cybercriminals to **break, bypass, or exploit weaknesses** in encryption algorithms or systems. The goal is to **access protected information** without the decryption key.



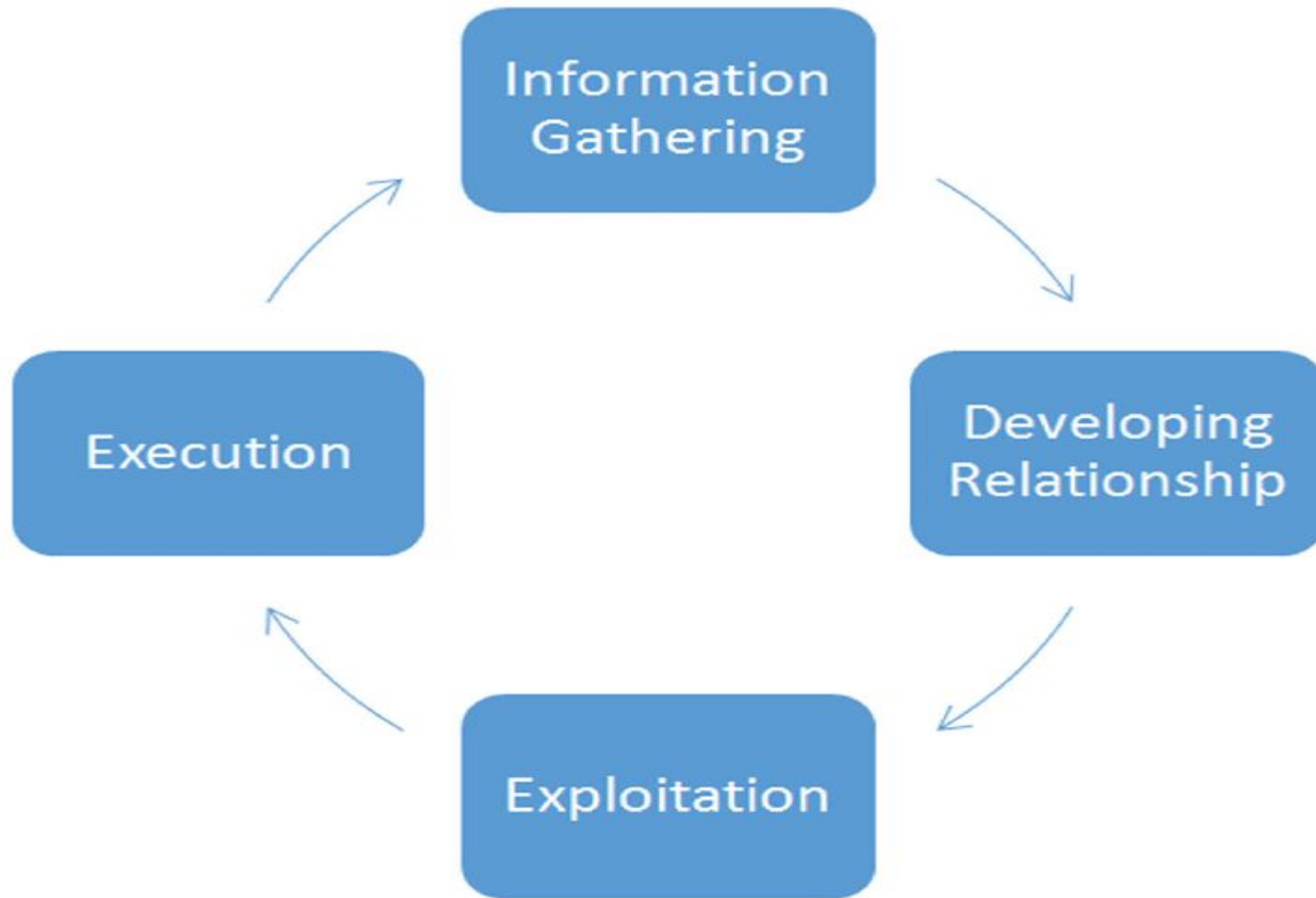
Attack Name	Type of Attack	Description
Denial of Service (DoS)	Active	Overloads a system to make it unavailable to users.
Distributed Denial of Service (DDoS)	Active	Multiple systems flood a target with traffic to crash it.
Backdoors and Trapdoors	Active	Hidden access points used to bypass normal authentication.
Sniffing	Passive	Captures data packets on a network to steal information.
Phishing	Active	Tricks users into revealing sensitive data using fake messages or websites.
Spoofing	Active	Fakes an identity (e.g., IP, email) to trick or gain access.
Man-in-the-Middle (MITM)	Both	Intercepts communication; passive when only listening, active when modifying.
Replay Attack	Active	Reuses captured data to trick a system into unauthorized actions.
TCP/IP Hacking	Both	Exploits flaws in the protocol; can be passive (sniffing) or active (session hijacking).
Encryption Attacks	Both	Brute-force, MITM, or cryptanalysis to break encryption; can be passive (eavesdropping) or active (altering messages).

Social Engineering

Attackers use psychology and manipulation to trick users into performing actions that could compromise with their security including **downloading malicious files, revealing sensitive information, clicking on malicious links, make transactions to illegal sources**

Social engineering is the art of **tricking or deceiving people** into giving up confidential information or access, usually through **trust, fear, urgency, or manipulation.**

Social Engineering Life cycle



Types of Social Engineering

1. Phishing

Phishing is a type of social engineering attack that involves sending an email or message that appears to be from a legitimate source, such as a bank, in an attempt to trick the recipient into revealing their login credentials or other sensitive information.

2. Baiting

Baiting is a type of social engineering attack that involves leaving a tempting item, such as a USB drive, in a public place in the hope that someone will pick it up and plug it into their computer. The USB drive is then used to infect the computer with malware.

3. Tailgating

Tailgating is a type of social engineering attack that involves following an authorized individual into a secure area, such as a building or data center, without proper authorization.

4. Pretexting

Pretexting is a type of social engineering attack that involves creating a false identity or situation in order to trick an individual into revealing sensitive information. For example, an attacker might pretend to be a customer service representative in order to trick an individual into giving them their login credentials.

5. Scareware

Scareware is when the victim is sent false messages claiming their system is infected with a malware, or outdated, suggesting them to download softwares to resolve the issue. Downloading the software would lead to the attackers gaining access to the system.