International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Network Security Threats and Vulnerabilities

**Dr. Manish Kumar[1], Mr. Prabhat Kumar[2]**

[1,2]Assistant Professor, University Department of Computer Applications, Vinoba Bhave University, Hazaribag, Jharkhand, India

**Abstract:**
The communication of confidential data over the Internet increases every day. Individuals and organizations submit their sensitive data electronically. It is also common for hackers to target these networks. Nowadays, protecting your data, software, and hardware from viruses is more of a necessity than ever, not just a concern.
Cyber security is traditionally defined by the three attributes of confidentiality, integrity and availability. Confidentiality is the prevention of unauthorized disclosure of information. Integrity is the prevention of unauthorized modification of information, and availability is the prevention of unauthorized retention of information or resources.
This article studies the different types of security threats, resources and vulnerabilities of computer systems.

**Keyword:** Computer & Network Security, Types of Threats, Computer System Assets.

## I. Introduction

Computers and the Internet have transformed almost every aspect of our personal and professional lives. Computers are vital to most modern businesses, but their indispensability comes with risk. Protecting corporate data is an important consideration for any organization that prioritizes cyber security. Sensitive information is often valuable and computer systems are a target for thieves and hackers.
Cyber security refers to measures and controls that guarantee the confidentiality, integrity and availability of information processed and stored by a computer. This includes everything from the protection of physical information assets to data security and cyber security practices. Cyber security ensures that a company's data and computer systems are safe from breaches and unauthorized access. [1]
System security can mean many things. To have security in the system, we must protect it from corruption and we must protect the data in the system.
There are many reasons why these need not be secure.

- A system may no longer work because a user fills the entire disk with junk.
- A power outage can cause system failure.
- Malicious users may try to hack the system to destroy it.
- We can classify security attacks into two types as mentioned below:
- **Direct:** This is any direct attack on your specific systems, whether by external hackers or disgruntled insiders.
- **Indirect:** This is a general random attack, most commonly computer viruses, computer worms or computer trojans.

## II. Objectives

- Learn computer and network level security.
- Identify security threats and objectives.
- Mention the role of information system resources in security.
- How to handle vulnerabilities in network security.

## III. Types of Threats

The types of attacks on the security of a computer system or network are best characterized by considering the function of the computer system as an information provider. In general, information flows from a source, such as a file or a region of main memory, to a destination, such as another file or a user.[2]

### 1) Normal Flow:

This normal flow is depicted in figure.


1) Normal Flow

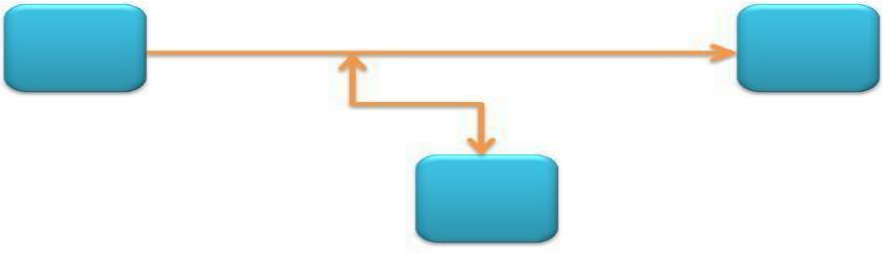
### 2) Interruption:

A system resource is destroyed or becomes unavailable or unusable. This is attack **availability.**
Examples include destroying a hardware component such as a hard drive, cutting a communications line, or disabling the file management system.

2) Interruption

### 3) Interception:

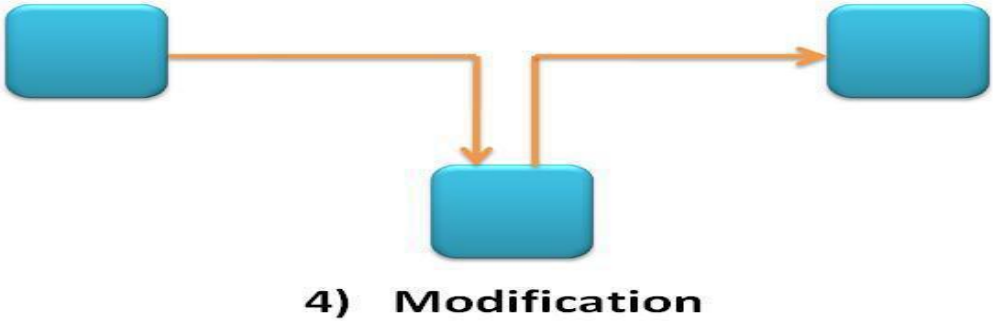
An unauthorized party gains access to an asset. This is an attack on **confidentiality**. The unauthorized party could be a person, a program or a computer.
Examples include wire tapping to capture data in a network and the illicit copying of files or programs.



3) Interception

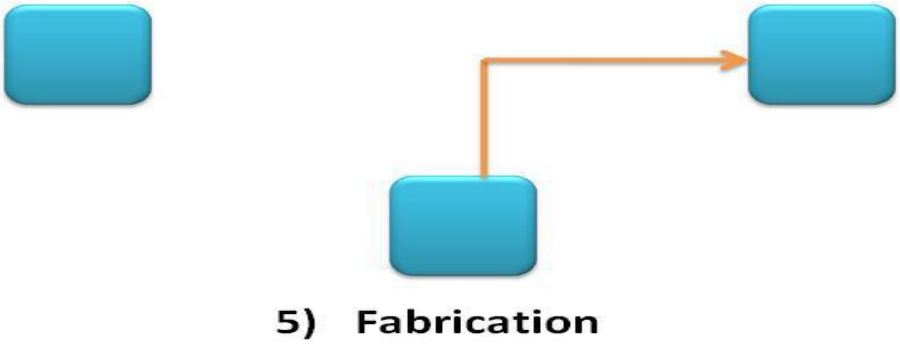
**4) Modification:**

An unauthorized party not only gains access to but tampers with the asset. This is an attack on **integrity.** Examples include changing values in a data file, altering a program so that it performs differently and modifying the content of messages being transmitted on a network.




**5) Fabrication:**

An unauthorized party inserts counterfeit objects into the system. This is an attack on **authenticity**. Examples include the insertion of spurious messages in a network or the addition of records to a file.




**Active and passive network security threats:**

## IV. Computer System Assets

Computer system resources can be classified into hardware, software, data and communication lines. [3]
Hardware: The biggest threat to computer systems hardware is in the area of availability. Hardware is the least susceptible to attacks and autopilots. Hazards include unintentional and intentional damage to equipment and theft. Physical and administrative security measures are required to combat these threats.
Software: Software, including operating systems, utilities and application programs can be useful for individuals and businesses. Computer system hardware is also beneficial for businesses or individuals.
Data: Hardware and software security is a common concern of computer center professionals or computer users. Data security is a much broader issue of keeping data and other types of information managed by individuals, groups and business organizations.
Communication Lines: Passive attacks involve interception or monitoring of transmission. The goal of the opponent is to obtain information that is being transmitted.

## V. Network security threats and strategies to minimize vulnerabilities

Network security threats can pose serious risks to the confidentiality, integrity, and availability of information within a network. Minimizing vulnerabilities is crucial to building a robust defense against these threats. Here are some common network security threats and strategies to minimize vulnerabilities: [4]

### Common Network Security Threats:

1. **Malware:**

**Minimize Vulnerability:** Keep antivirus software up-to-date, regularly scan for malware, and educate users about safe online behavior.

1. **Phishing Attacks:**

**Minimize Vulnerability:** Train employees to recognize phishing emails, use email filtering solutions, and implement multi-factor authentication (MFA).

2. **Denial of Service (DoS) Attacks:**

**Minimize Vulnerability:** Use firewalls and intrusion prevention systems (IPS), implement rate limiting, and use content delivery networks (CDNs) to distribute traffic.

3. **Man-in-the-Middle (MitM) Attacks:**

**Minimize Vulnerability:** Encrypt communication using protocols like HTTPS, use VPNs for remote access, and monitor network traffic for suspicious activities.

4. **Insider Threats:**

**Minimize Vulnerability:** Implement access controls, conduct regular employee training on security policies, and monitor user activities for unusual behavior.

5. **Password Attacks:**

**Minimize Vulnerability:** Enforce strong password policies, use password hashing, and implement MFA.

6. **Zero-Day Exploits:**

**Minimize Vulnerability:** Keep software and systems updated with the latest patches, use intrusion detection systems, and implement network segmentation.

**Strategies to Minimize Vulnerabilities:**

1. **Regular Security Audits:**

Conduct regular security audits to identify and address vulnerabilities in the network.

2. **Patch Management:**

Keep all software, operating systems, and firmware up-to-date with the latest security patches.

3. **Network Segmentation:**

Divide the network into segments to contain potential threats and limit lateral movement in case of a security breach.

4. **Firewalls and Intrusion Prevention Systems:**

Use firewalls to filter incoming and outgoing traffic, and intrusion prevention systems to detect and prevent potential threats.

5. **Encryption:**

Implement encryption for sensitive data in transit and at rest to protect it from unauthorized access.

6. **User Education and Training:**

Educate users about security best practices, such as recognizing phishing attempts and creating strong passwords.

7. **Access Controls:**

Implement the principle of least privilege to ensure users have only the necessary access rights for their roles.

8. **Incident Response Plan:**

Develop and regularly update an incident response plan to quickly and effectively respond to security incidents.

9. **Security Monitoring:**

Use security monitoring tools to detect and respond to suspicious activities in real-time.

10. **Backup and Recovery:**

Regularly back up critical data and test the restoration process to ensure business continuity in case of a security incident.

By adopting a multi-layered approach to security and staying proactive in identifying and addressing vulnerabilities, organizations can significantly enhance their network security posture. Regularly reassessing and updating security measures are crucial in the ever-evolving landscape of cyber security threats.

## VI. Conclusion

In this research, we explored the concept of security and the various threats associated with it. The result of this research is that the increasing dependence of companies on the use of data processing systems and the increasing use of network and communication devices in the construction of distributed systems lead to strong information security requirements.

Security requirements are best assessed by looking at the various security threats a business faces. Service outages threaten availability. Interception of information threatens secrecy. Finally, integrity is threatened by both alteration of legitimate information and unauthorized fabrication of information.

**References:**

1. EC-Council, Network Defense: Security Policy and Threats – 1st Edition (Apr 2010) Cengage Learning.
2. James Michael Stewart, Network Security, Firewalls and VPN – 4th Edition (2011) Jones & Bartlett Learning Canada.
3. Willing Stallings. Operating System Internals and Design Principles – 3rd Edition New Jersey: Prentice-Hall International.
4. Avi Silberschatz, Peter Baer Galvin, Greg Gagne – Operating System Concept – 9th Edition John Wiley & Sons.

**Web sites:**

1. Network security available at: http://en.wikipedia.org/wiki/Network_security