**UNIT 1 :Introduction to security and threat:**

**LIST OF TOPICS:**
Basic concepts of security: Security, Need of Security, Attack, Threat, The OSI Security Architecture, Security Services, Security Attacks, A model for Network Security.

**********

## Basic concepts of security:

Computer security refers to protecting and securing computers and their related data, networks, software, hardware from unauthorized access, misuse, theft, information loss, and other security issues. The Internet has made our lives easier and has provided us with lots of advantages but it has also put our system's security at risk of being infected by a virus, of being hacked, information theft, damage to the system, and much more.

Technology is growing day by day and the entire world is in its grasp. We cannot imagine even a day without electronic devices around us. With the use of this growing technology, invaders, hackers and thieves are trying to harm our computer's security for monetary gains, recognition purposes, ransom demands, bullying others, invading into other businesses, organizations, etc. In order to protect our system from all these risks, computer security is important.

## Definition of Computer Security

## Types of computer security

Computer security can be classified into four types:

**1. Cyber Security:** Cyber security means securing our computers, electronic devices, networks , programs, systems from cyber attacks. Cyber attacks are those attacks that happen when our system is connected to the Internet.

**2. Information Security:** Information security means protecting our system's information from theft, illegal use and piracy from unauthorized use. Information security has mainly three objectives: confidentiality, integrity, and availability of information.

**3. Application Security:** Application security means securing our applications and data so that they don't get hacked and also the databases of the applications remain safe and private to the owner itself so that user's data remains confidential.

**4. Network Security:** Network security means securing a network and protecting the user's information about who is connected through that network. Over the network hackers steal, the packets of data through sniffing and spoofing attacks, man in the middle attack, war driving, etc, and misuse the data for their benefits.

## Types of cyber attack

**1. Denial of service attack or DOS:** A denial of service attack is a kind of cyber attack in which the attackers disrupt the services of the particular network by sending infinite requests and temporary or permanently making the network or machine resources unavailable to the intended audience.

**2. Backdoor:** In a backdoor attack, malware, trojan horse or virus gets installed in our system and start affecting it's security along with the main file. Consider an example: suppose you are installing free software from a certain website on the Internet. Now, unknowingly, along with this software, a malicious file also gets installed, and as soon as you execute the installed software that file's malware gets affected and starts affecting your computer security. This is known as a backdoor.

**3.Eavesdropping:** Eavesdropping refers to secretly listening to someone's talk without their permission or knowledge. Attackers try to steal, manipulate, modify, hack information or systems by passively listening to network communication, knowing passwords etc. A physical example would be, suppose if you are talking to another person of your organization and if a third person listens to your private talks then he/ she is said to eavesdrop on your conversation. Similarly, your conversation on the internet maybe eavesdropped by attackers listening to your private conversation by connecting to your network if it is insecure.

**4. Phishing:** Phishing is pronounced as "fishing" and working functioning is also similar. While fishing, we catch fish by luring them with bait. Similarly, in phishing, a user is tricked by the attacker who gains the trust of the user or acts as if he is a genuine person and then steals the information by ditching. Not only attackers but some certain websites that seem to be genuine, but actually they are fraud sites. These sites trick the users and they end up giving their personal information such as login details or bank details or card number etc. Phishing is of many types: Voice phishing, text phishing etc.

**5. Spoofing:** Spoofing is the act of masquerading as a valid entity through falsification of data(such as an IP address or username), in order to gain access to information or resources that one is otherwise unauthorized to obtain. Spoofing is of several types- email spoofing, IP address spoofing, MAC spoofing , biometric spoofing etc.

**6. Malware:** Malware is made up of two terms: Malicious + Software = Malware. Malware intrudes into the system and is designed to damage our computers. Different types of malware are adware, spyware, ransomware, Trojan horse, etc.

**7. Social engineering:** Social engineering attack involves manipulating users psychologically and extracting confidential or sensitive data from them by gaining their trust. The attacker generally exploits the trust of people or users by relying on their cognitive basis.

**8. Polymorphic Attacks:** Poly means "many" and morph means "form", polymorphic attacks are those in which attacker adopts multiple forms and changes them so that they are not recognized easily. These kinds of attacks are difficult to detect due to their changing forms.

## Steps to ensure computer security

In order to protect our system from the above-mentioned attacks, users should take certain steps to ensure system security:

1. Always keep your Operating System up to date. Keeping it up to date reduces the risk of their getting attacked by malware, viruses, etc.

2. Always use a secure network connection. One should always connect to a secure network. Public wi-fi's and unsecured networks should be avoided as they are at risk of being attacked by the attacker.

3. Always install an Antivirus and keep it up to date. An antivirus is software that scans your PC against viruses and isolates the infected file from other system files so that they don't get affected. Also, we should try to go for paid anti-viruses as they are more secure.

4. Enable firewall. A firewall is a system designed to prevent unauthorized access to/from a computer or even to a private network of computers. A firewall can be either in hardware, software or a combination of both.

5. Use strong passwords. Always make strong passwords and different passwords for all social media accounts so that they cannot be key logged, brute forced or detected easily using dictionary attacks. A strong password is one that has 16 characters which are a combination of upper case and lower case alphabets, numbers and special characters. Also, keep changing your passwords regularly.

6. Don't trust someone easily. You never know someone's intention, so don't trust someone easily and end up giving your personal information to them. You don't know how they are going to use your information.

7. Keep your personal information hidden. Don't post all your personal information on social media. You never know who is spying on you. As in the real world, we try to avoid talking to strangers and sharing anything with them. Similarly, social media also have people whom you don't know and if you share all your information on it you may end up troubling yourself.

8. Don't download attachments that come along with e-mails unless and until you know that e-mail is from a genuine source. Mostly, these attachments contain malware which, upon execution infect or harms your system.

9. Don't purchase things online from anywhere. Make sure whenever you are shopping online you are doing so from a well-known website. There are multiple fraud websites that may steal your card information as soon as you checkout and you may get bankrupt by them.

10. Learn about computer security and ethics. You should be well aware of the safe computing and ethics of the computing world. Gaining appropriate knowledge is always helpful in reducing cyber-crime.

11. If you are attacked, immediately inform the cyber cell so that they may take appropriate action and also protect others from getting attacked by the same person. Don't hesitate to complain just because you think people may make your fun.

12. Don't use pirated content. Often, people try to download pirated movies, videos or web series in order to get them for free. These pirated content are at major risk of being infected with viruses, worms, or malware, and when you download them you end up compromising your system security.

## Computer Security Threats

Computer security threats are potential threats to your computer's efficient operation and performance. These could be harmless adware or dangerous trojan infection. As the world becomes more digital, computer security concerns are always developing. A threat in a computer system is a potential danger that could jeopardize your data security. At times, the damage is irreversible.

**Types of Threats:**

A security threat is a threat that has the potential to harm computer systems and organizations. The cause could be physical, such as a computer containing sensitive information being stolen. It's also possible that the cause isn't physical, such as a viral attack.

**1. Physical Threats:** A physical danger to computer systems is a potential cause of an occurrence/event that could result in data loss or physical damage. It can be classified as:

- **Internal:** Short circuit, fire, non-stable supply of power, hardware failure due to excess humidity, etc. cause it.
- **External:** Disasters such as floods, earthquakes, landscapes, etc. cause it.
- **Human:** Destroying of infrastructure and/or hardware, thefts, disruption, and unintentional/intentional errors are among the threats.

**2. Non-physical threats:** A non-physical threat is a potential source of an incident that could result in:

- Hampering of the business operations that depend on computer systems.
- Sensitive – data or information loss
- Keeping track of other's computer system activities illegally.
- Hacking id & passwords of the users, etc.

The non-physical threads can be commonly caused by:

**(i) Malware:** Malware ("malicious software") is a type of computer program that infiltrates and damages systems without the users' knowledge. Malware tries to go unnoticed by either hiding or not letting the user know about its presence on the system. You may notice that your system is processing at a slower rate than usual.

**(ii) Virus:** It is a program that replicates itself and infects your computer's files and programs, rendering them inoperable. It is a type of malware that spreads by inserting a copy of itself into and becoming part of another program. It spreads with the help of software or documents. They are embedded with software and documents and then transferred from one computer to another using the network, a disk, file sharing, or infected e-mail. They usually appear as an executable file.

**(iii) Spyware:** Spyware is a type of computer program that tracks, records, and reports a user's activity (offline and online) without their permission for the purpose of profit or data theft. Spyware can be acquired from a variety of sources, including websites, instant chats, and emails. A user may also unwittingly obtain spyware by adopting a software program's End User License Agreement.
Adware is a sort of spyware that is primarily utilized by advertising. When you go online, it keeps track of your web browsing patterns in order to compile data on the types of websites you visit.

**(iv) Worms:** Computer worms are similar to viruses in that they replicate themselves and can inflict similar damage. Unlike viruses, which spread by infecting a host file, worms are freestanding programs that do not require a host program or human assistance to proliferate. Worms don't change programs; instead, they replicate themselves over and over. They just eat resources to make the system down.

**(v) Trojan:** A Trojan horse is malicious software that is disguised as a useful host program. When the host program is run, the Trojan performs a harmful/unwanted action. A Trojan horse, often known as a Trojan, is malicious malware or software that appears to be legal yet has the ability to take control of your computer. A Trojan is a computer program that is designed to disrupt, steal, or otherwise harm your data or network.

**(vi) Denial Of Service Attacks:** A Denial of Service attack is one in which an attacker tries to prohibit legitimate users from obtaining information or services. An attacker tries to make a system or network resource unavailable to its intended users in this attack. The web servers of large organizations such as banking, commerce, trading organizations, etc. are the victims.

**(vii) Phishing:** Phishing is a type of attack that is frequently used to obtain sensitive information from users, such as login credentials and credit card details. They deceive users into giving critical information, such as bank and credit card information, or access to personal accounts, by sending spam, malicious Web sites, email messages, and instant chats.

**(viii) Key-Loggers**: Keyloggers can monitor a user's computer activity in real-time. Keylogger is a program that runs in the background and records every keystroke made by a user, then sends the data to a hacker with the intent of stealing passwords and financial information.

**How to make your system secure:**

In order to keep your system data secure and safe, you should take the following measures:

1. Always keep a backup of your data.

2. Install firewall software and keep it updated every time.

3. Make use of strong and difficult to crack passwords (having capital & small alphabets, numbers, and special characters).

4. Install antivirus/ anti-spyware and keep it updated every time.

5. Timely scan your complete system.

6. Before installing any program, check whether it is safe to install it (using Antivirus Software).

7. Take extra caution when reading emails that contain attachments.

8. Always keep your system updated.

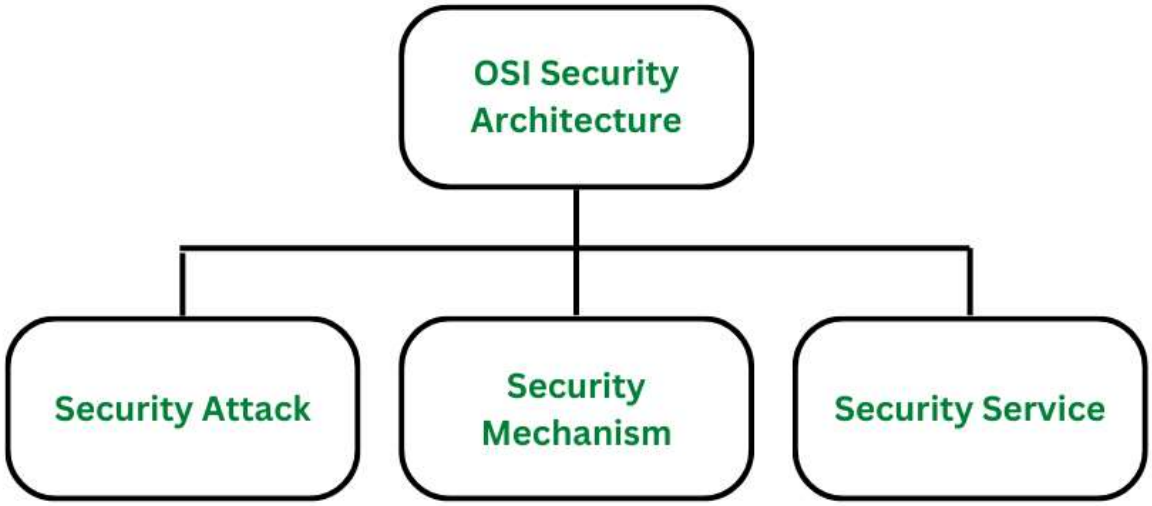
## OSI Security Architecture

The security of an organization is the greatest concern of the people working at the organization. Safety and security are the pillars of cyber technology. It is hard to imagine the cyber world without thinking about security. The architecture of security is thus a very important aspect of the organization. The OSI (Open Systems Interconnection) Security Architecture defines a systematic approach to providing security at each layer. It defines security services and security mechanisms that can be used at each of the seven layers of the OSI model to provide security for data transmitted over a network. These security services and mechanisms help to ensure the confidentiality, integrity, and availability of the data. OSI architecture is internationally acceptable as it lays the flow of providing safety in an organization.

OSI Security Architecture focuses on these concepts:

- Security Attack:
- Security mechanism: A security mechanism is a means of protecting a system, network, or device against unauthorized access, tampering, or other security threats.
- Security Service:

Classification of OSI Security Architecture




Classification of OSI Security Architecture

OSI Security Architecture is categorized into three broad categories namely **Security Attacks, Security mechanisms**, **and Security Services**. We will discuss each in detail:

## 1. Security Attacks:

A security attack is an attempt by a person or entity to gain unauthorized access to disrupt or compromise the security of a system, network, or device. These are defined as the actions that put at risk an organization's safety. They are further classified into 2 sub-categories:

A. Passive Attack:

Attacks in which a third-party intruder tries to access the message/ content/ data being shared by the sender and receiver by keeping a close watch on the transmission or eave-dropping the transmission is called Passive Attacks. These types of attacks involve the attacker observing or monitoring system, network, or device activity without actively disrupting or altering it. Passive attacks are typically focused on gathering information or intelligence, rather than causing damage or disruption.

Here, both the sender and receiver have no clue that their message/ data is accessible to some third-party intruder. The message/ data transmitted remains in its usual form without any deviation from its usual behavior. This makes passive attacks very risky as there is no information provided about the attack happening in the communication process. One way to prevent passive attacks is to encrypt the message/data that needs to be transmitted, this will prevent third-party intruders to use the information though it would be accessible to them.

Passive attacks are further divided into two parts based on their behavior:

- **Eavesdropping:** This involves the attacker intercepting and listening to communications between two or more parties without their knowledge or consent. Eavesdropping can be performed using a variety of techniques, such as packet sniffing, or man-in-the-middle attacks.

- **Traffic analysis:** This involves the attacker analyzing network traffic patterns and metadata to gather information about the system, network, or device. Here the intruder can't read the message but only understand the pattern and length of encryption. Traffic analysis can be performed using a variety of techniques, such as network flow analysis, or protocol analysis.

B. Active Attacks:

Active attacks refer to types of attacks that involve the attacker actively disrupting or altering system, network, or device activity. Active attacks are typically focused on causing damage or disruption, rather than gathering information or intelligence. Here, both the sender and receiver have no clue that their message/ data is modified by some third-party intruder. The message/ data transmitted doesn't remain in its usual form and shows deviation from its usual behavior. This makes active attacks dangerous as there is no information provided of the attack happening in the communication process and the receiver is not aware that the data/ message received is not from the sender.

Active attacks are further divided into four parts based on their behavior:

- **Masquerade** is a type of attack in which the attacker pretends to be an authentic sender in order to gain unauthorized access to a system. This type of attack can involve the attacker using stolen or forged credentials, or manipulating authentication or authorization controls in some other way.
- **Replay** is a type of active attack in which the attacker intercepts a transmitted message through a passive channel and then maliciously or fraudulently replays or delays it at a later time.
- **Modification of Message** involves the attacker modifying the transmitted message and making the final message received by the receiver look like it's not safe or non-meaningful. This type of attack can be used to manipulate the content of the message or to disrupt the communication process.
- **Denial of service** (DoS) attacks involve the attacker sending a large volume of traffic to a system, network, or device in an attempt to overwhelm it and make it unavailable to legitimate users.

## 2. Security Mechanism

The mechanism that is built to identify any breach of security or attack on the organization, is called a security mechanism. Security Mechanisms are also responsible for protecting a system, network, or device against unauthorized access, tampering, or other security threats. Security mechanisms can be implemented at various levels within a system or network and can be used to provide different types of security, such as confidentiality, integrity, or availability.

Some examples of security mechanisms include:

- **Encipherment (Encryption)** involves the use of algorithms to transform data into a form that can only be read by someone with the appropriate decryption key. Encryption can be used to protect data it is transmitted over a network, or to protect data when it is stored on a device.
- **Digital signature** is a security mechanism that involves the use of cryptographic techniques to create a unique, verifiable identifier for a digital document or message, which can be used to ensure the authenticity and integrity of the document or message.
- **Traffic padding** is a technique used to add extra data to a network traffic stream in an attempt to obscure the true content of the traffic and make it more difficult to analyze.
- **Routing control** allows the selection of specific physically secure routes for specific data transmission and enables routing changes, particularly when a gap in security is suspected.

## 3. Security Services:

Security services refer to the different services available for maintaining the security and safety of an organization. They help in preventing any potential risks to security. Security services are divided into 5 types:

- **Authentication** is the process of verifying the identity of a user or device in order to grant or deny access to a system or device.
- **Access control** involves the use of policies and procedures to determine who is allowed to access specific resources within a system.
- **Data Confidentiality** is responsible for the protection of information from being accessed or disclosed to unauthorized parties.
- **Data integrity** is a security mechanism that involves the use of techniques to ensure that data has not been tampered with or altered in any way during transmission or storage.
- **Non- repudiation** involves the use of techniques to create a verifiable record of the origin and transmission of a message, which can be used to prevent the sender from denying that they sent the message.

## Benefits of OSI Architecture:

Below listed are the benefits of OSI Architecture in an organization:

1. Providing Security:

- OSI Architecture in an organization provides the needed security and safety, preventing potential threats and risks.
- Managers can easily take care of the security and there is hassle-free security maintenance done through OSI Architecture.

2. Organising Task:

- The OSI architecture makes it easy for managers to build a security model for the organization based on strong security principles.
- Managers get the opportunity to organize tasks in an organization effectively.

3. Meets International Standards:

- Security services are defined and recognized internationally meeting international standards.
- The standard definition of requirements defined using OSI Architecture is globally accepted.

**A Model for Network Security**

A model for much of what we will be discussing is captured, in very general terms, in Figure 2.

A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination

and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

● A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

● Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

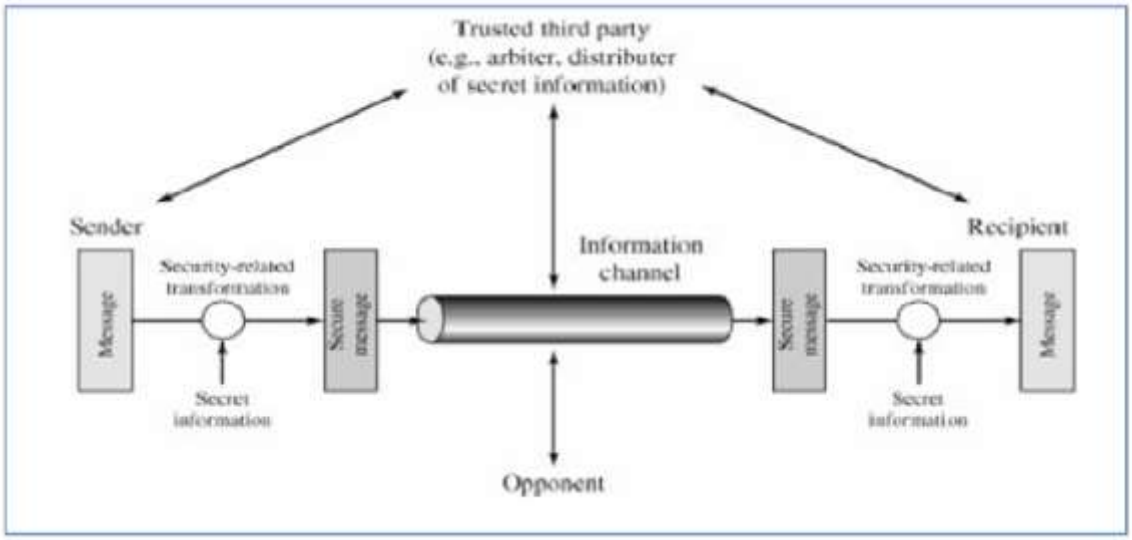



Figure 2: Model for network security

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.

2. Generate the secret information to be used with the algorithm.

3. Develop methods for the distribution and sharing of the secret information.

4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system. Or, the intruder can be a disgruntled employee who wishes to do damage, or a criminal who seeks to exploit computer assets for financial gain (e.g., obtaining credit card numbers or performing illegal money transfers). Another type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compilers. Programs can present two kinds of threats:

● Information access threats intercept or modify data on behalf of users who should not have access to that data.

● Service threats exploit service flaws in computers to inhibit use by legitimate users.

Viruses and worms are two examples of software attacks. Such attacks can be introduced into a system by means of a disk that contains the unwanted logic concealed in otherwise useful software. They can also be inserted into a system across a network; this latter mechanism is of more concern in network security.

The security mechanisms needed to cope with unwanted access fall into two broad categories. The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or unwanted software gains access, the second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders

**Assignment 1**

1. What are the types of computer security?
2. What is the difference between a security threat and a security attack?
3. Why is security important in the digital world?
4. What is Cyber security?
5. What is information security?
6. What is application security?
7. What is network security?
8. What is social engineering?
9. Enlist types of cyber-attack.
10. Explain dos.
11. What is backdoor?
12. What is eavesdropping?
13. Define fishing.
14. Define spoofing.
15. Define malwares.
16. what is polymorphic attacks:
17. What steps can be taken to ensure computer security?
18. What is an antivirus? Name some antivirus software.
19. Enlist and explain types of threats.
20. Define following term: malware, virus, Spyware, Worms, Trojan, Denial of services attack, Phishing, keyloggers.
21. How to make your system secure.
22. Explain OSI Security Architecture.
23. Enlist and Explain Security mechanism.
24. Enlist and explain types of security services.
25. Benefits of OSI architecture.
26. Drow and explain model for network security.
27. Compare and contrast Worms and Viruses.
28. What is the difference between an attack and a threat in the context of cybersecurity?
29. What are some common sources of threats
30. Describe the various types of cyber attacks
31. What is the OSI model and how does it relate to network security
32. Describe the different layers of the OSI model and their role in security
33. How can security mechanisms be implemented at different layers of the OSI model?
34. What are some common types of security attacks and how do they exploit vulnerabilities?
35. Describe a basic model for network security and its components.