**Unit 1 introduction of information security**

**information security:-**

* The term 'information security' means protecting information and information systems from unauthorized access or use.
* Effective information security requires the successful integration of
* Security products such as firewalls, instruction detection system and vulnerability scanners
* Technologies such as authentication and encryption
* Security policies and procedures.

**Need of information security:-**

Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure.

Information security is needed because some organizations can be damaged by hostile application or intruders. There can be multiple forms of damage which are interrelated. These includes −

* Today all technology are depend on their information system.
* Information is the oxygen of the modern age. It keeps through the walls topped by barded wire, it wafts across the electrified borders.
* Protecting the functionality of organization.
* Enabling the safe operation of application
* Protecting the data that the organization collect and use.
* Safeguarding technology assets in organization.

**Security services**

* Security service is a service which provide a security to the system or of data transfer.
* It is divided into 5 categories:

1. **Authentication**

Authentication is the process of determining whether someone or something is, in fact, who or what it says it is. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

1. **Access control**

Access control is a security technique that regulates who or what can view or use resources in a computing environment.

1. **Data confidentiality**

Data confidentiality is the protection of transmitted data from passive attack.

With respect to the content of a data transmission, several levels of protection can be identified.

1. **Data integrity**

Data integrity is the overall accuracy, completeness, and consistency of data.

1. **Nonrepudiation**

* Non repudiation prevents either sender or receiver from denying a transmitted message.
* When a message is sent, the receiver can prove that the alleged sender in fact sent the message.
* Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

**Security mechanism**

Security mechanisms are technical tools and techniques that are used to implement security services. A mechanism might operate by itself, or with others, to provide a particular service. Examples of common security mechanisms are as follows: Cryptography. Message digests and digital signatures.

1. **Encipherment**

This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form.

It achieved by two famous techniques named cryptography and encipherment. Level of data encryption is dependent on the algorithm used for encipherment.

1. **Digital signature**

A digital signature—this security mechanism is achieved by adding digital data that is not visible to eyes. It if form of electronic signature which is added by senders which is checked by receiver electronically.t

1. **Access control**

This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.

1. **Data integrity**
2. **Traffic padding**

The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

1. **Routing control**

**Security attacks**

An attempt to gain unauthorized access to information resource or services, or to cause harm or damage to information systems.

There are two type of security attacks

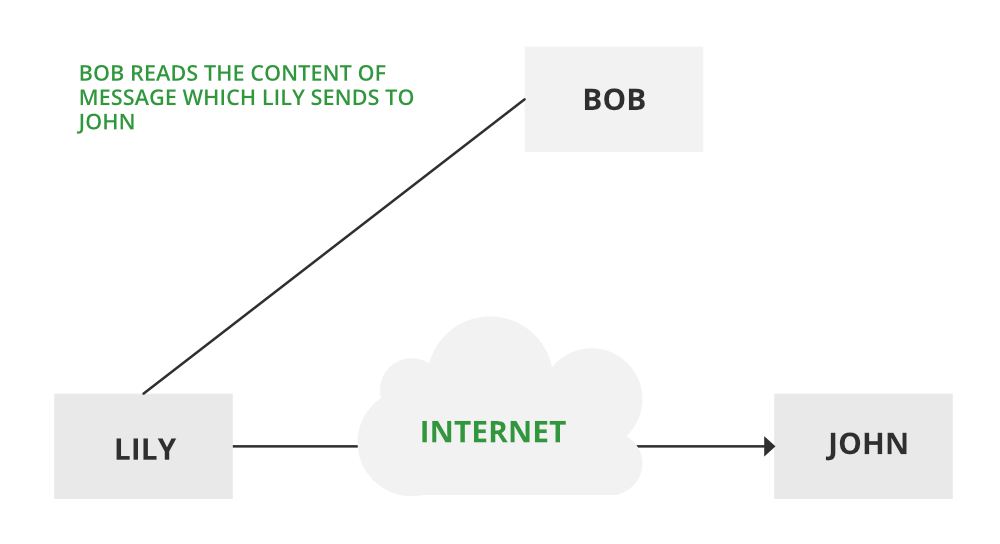
1. **Passive attack**

A Passive attack attempts to learn or make use of information from the system but does not affect system resources.

**list of passive attack are (the release attacks of message content, and traffic analysis).**

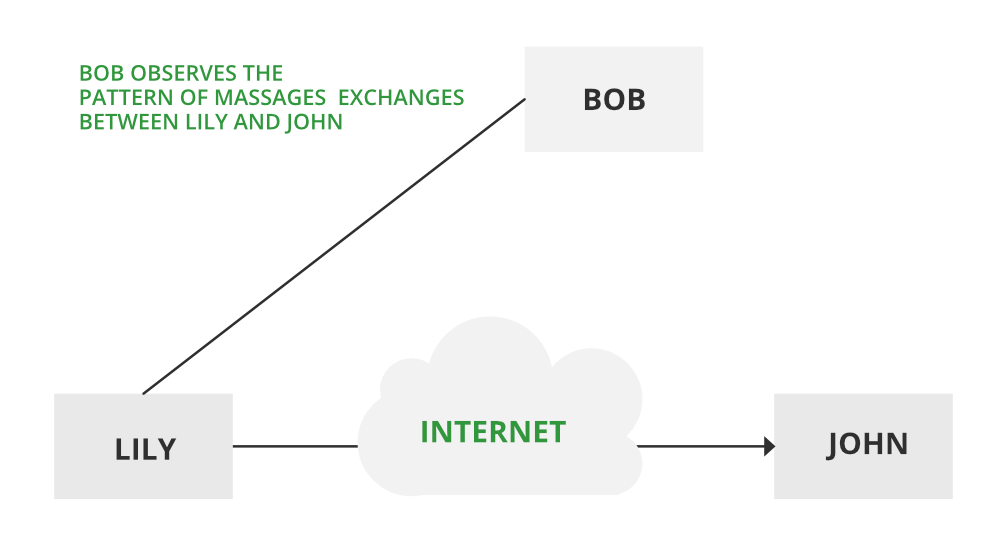
**The release of message content:**

* Telephonic conversation, an electronic mail message, or transferred file may contain sensitive or confidential information.
* We would like to prevent an enemy from learning the content of these information.

****

**Traffic analysis:**

* Suppose that we had a way of masking information, so that the attacker even if captured the message could not extract any information from the message.
* The technique for masking contents is encryption.
* Passive attacks are very difficult to detect, because they do not involve any alteration of the data.
* Encryption is a better way to prevent the passive attacks.

****

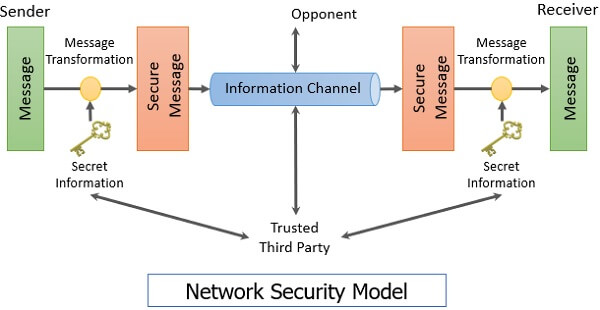
1. **Active attacks**

Active attacks involve some modification of the data stream or the creation of a false statements.

Types of active attacks are as follows:

* **Masquerade**
* **Modification of messages**
* **Repudiation**
* **Replay**
* **Denial of Service**

**Draw network security model.**



**Define computer security:-**

computer security, also called cybersecurity, the protection of computer systems and information from harm, theft, and unauthorized use. Computer hardware is typically protected by the same means used to protect other valuable or sensitive equipment—namely, serial numbers, doors and locks, and alarms.

Some examples of application security tools are antivirus software, firewalls, web application firewalls, encryption, etc.

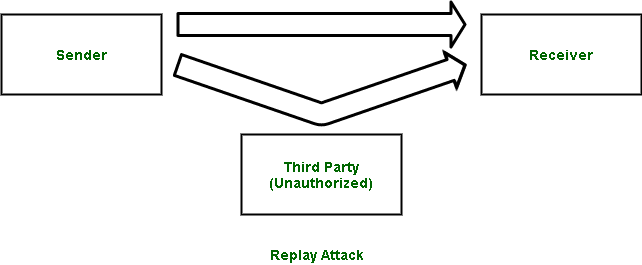
**Define internet security:-**

Internet security is a term that describes security for activities and transactions made over the internet. It's a particular component of the larger ideas of cybersecurity and computer security, involving topics including browser security, online behavior and network security.

**Explain the replaying attack:**

Replay Attack is a type of security attack to the data sent over a network.

In this attack, the hacker or any person with unauthorized access, captures the traffic and sends communication to its original destination, acting as the original sender. The receiver feels that it is an authenticated message but it is actually the message sent by the attacker. The main feature of the Replay Attack is that the client would receive the message twice, hence the name, Replay Attack.



**Define traffic padding:-**

Traffic padding produces ciphertext output continuously, even in the absence of plaintext. A continuous random data stream is generated. When plaintext is available, it is encrypted and transmitted. When input plaintext is not present, random data are encrypted and transmitted

.

**Unit-2 system security**

**Symmetric cipher model**

A symmetric encryption scheme has five parts:-

* 1. **Plaintext**

This is the original message or data that is fed into the algorithm as input

* 1. **Encryption algorithm**

The encryption algorithm performs various substitutions and transformation on the plain text. This help us to convert plaintext into ciphertext.

* 1. **Secret key**
  2. **Cipher key**

Ciphertext is encrypted text transformed from plaintext using an encryption algorithm. Ciphertext can't be read until it has been converted into plaintext (decrypted) with a key. The decryption cipher is an algorithm that transforms the ciphertext back into plaintext.

* 1. **Decryption key**

Decryption is a process in which ciphertext is converted into plaintext with the help of key

**Cryptography**

cryptography is a technique for data encryption and decryption. Method of encrypting messages include the symmetric key encryption and asymmetric key encryption.

• Encryption means convert plaintext to ciphertext and decryption mean convert ciphertext to plaintext.

• Symmetric key also known as secret key cryptography and asymmetric key is also known as public key cryptography, single key is used for both encryption and decryption.

cryptography is broadly classified into two categories:

1. **Symmetric key**

* Symmetric key cryptography also known as secret key cryptography. With secret key cryptography, a single key is used for both encryption and decryption.
* Here the sender uses the key and encryption algorithm to encrypt the plaintext and sends the ciphertext to the receiver.
* The receiver applies the same key and decryption algorithm to decrypt the message and remove the plaintext.
* Key is nothing but just number, alphabet or alphanumber word. Because a single key is used for both function, secret key cryptography is also called symmetric encryption.

1. **Asymmetric key**

* Asymmetric key cryptography is also known as public key cryptography.
* The advantage of public key is, it removes the restriction of a shared symmetric key between two person who need to communicate with each other. The key is shared by the two parties and cannot be used when one of them wants communicate with third party.
* In their concept, each person gets a pair of keys, one called the public key and other called the private key.
* Each person public key is published while the private key is kept secret.
* Anyone can send a message by just using public information, but the message can only be decrypted with a private key.
* For example: it is like a locker in the bank system, you keep your jewelries or other things in bank locker and if you ant to open it you must required two keys, your key and bank coordinators key.

**Cryptanalysis**

* **The process of discover the plaintext or**

**List of Substitution technique:-**

**Caesar cipher**

**Monoalphabetic cipher**

**Polyalphabetic cipher**

**Playfair cipher**

**Hill cipher**

**Problem with symmetric cipher algorithms**

**Diffie-hellman key exchange algorithm**

**Steganography (page 48)**

* The art and science of hiding information by embedding messages within seemingly harmless messages.
* Steganography work by replacing bits of useless or unused data in regular computer files such as graphics, sound, text etc.
* This hidden information can be plain text, cipher text or images.

**Brute force attack**

**Unit-3 basic arithmetic’s in encryption**

**Divisibility rules**

**Division algorithm**

**The Euclidean algorithm**

**Modular arithmetic**

**Random number**

**Group, ring, fields**

**Unit-4 symmetric encryption algorithm**