Unit VI : Network Security & Cryptography

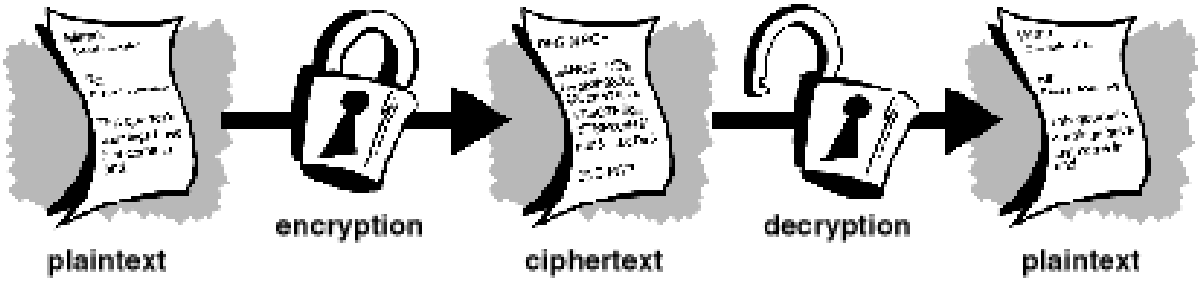
Introduction to Security & Cryptography,
Security concepts- Computer Security
Network Security
Information Security
Firewall
Working of Firewalls
Conventional Cryptography
Caesar's Cipher
public key Cryptography.

The Basics of Cryptography:

- When Julius Caesar sent messages to his generals, he didn't trust his messengers.
- So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet.
- Only someone who knew the "shift by 3" rule could decipher his messages.

Encryption and decryption

- Data that can be read and understood without any special measures is called *plaintext* or *cleartext.*
- The method of disguising plaintext in such a way as to hide its substance is called *encryption.*
- Encrypting plaintext results in unreadable gibberish called *ciphertext.*
- You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data.
- The process of reverting ciphertext to its original plaintext is called *decryption*.
- *Following Figure* illustrates this process.



What is cryptography?

- *Cryptography* is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.
- While cryptography is the science of securing data, *cryptanalysis* is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called *attackers.*

Introduction to Security:

- COMPUTER SECURITY:- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability** and **confidentiality** of information system resources which includes hardware, software, firmware, information/ data, and telecommunication.

Integrity

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.
- A loss of integrity is the unauthorized modification or destruction of information.

Availability

- Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system

Confidentiality

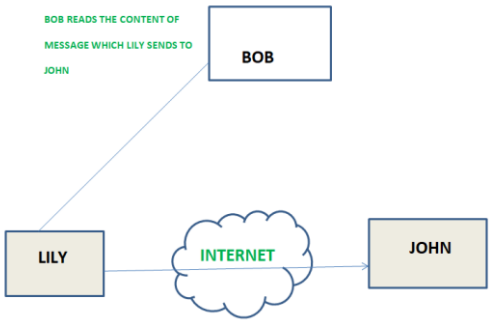
- Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information.
- A loss of confidentiality is the unauthorized disclosure of information.

Security Attacks

- There are two types of Security attacks
  - Passive Attacks
  - Active Attacks

Passive Attacks:

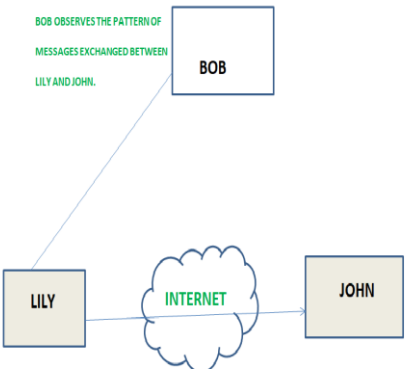
- A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:
- **release of message content**
- **Traffic analysis**



The release of message content –

• Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

Traffic analysis :



• Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.

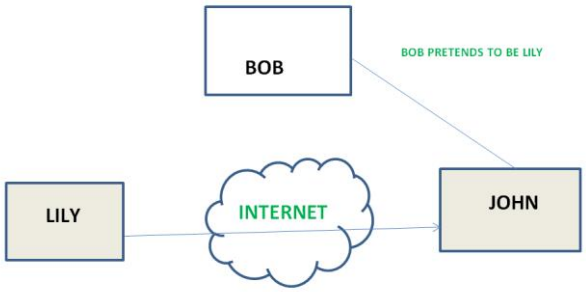
- The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged.
- This information might be useful in guessing the nature of the communication that was taking place.

Active attacks

- **Active attacks:** An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are as following:
  - **Masquerade**
  - **Modification of messages**
  - **Repudiation**
  - **Replay**

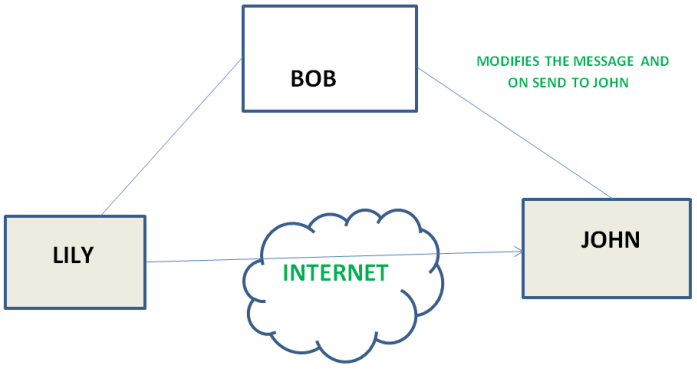
- **Denial of Service**

Masquerade: Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other form of active attacks. E.g. fake ID



Modification of messages

- It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect.
- For example, a message meaning "Allow JOHN to read confidential file X" is modified as "Allow Smith to read confidential file X".

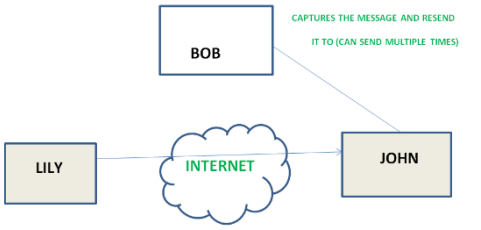


Repudiation

- This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message.
- For example, customer ask his Bank "To transfer an amount to someone" and later on the sender(customer) deny that he had made such a request. This is repudiation.

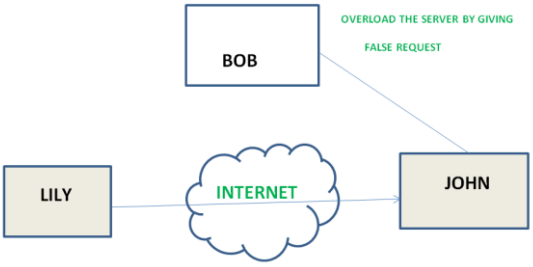
Replay

- It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.
- Storing old message and reutilizing that message



Denial of Service

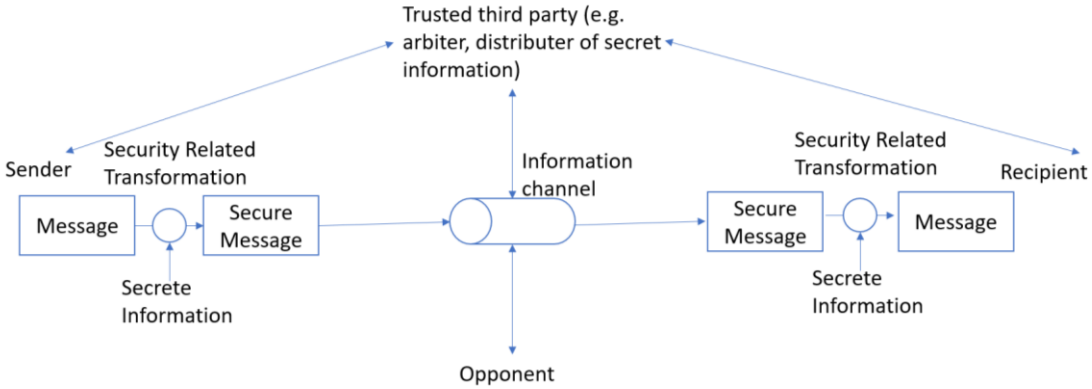
- It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination.
- Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.



Network Security

- A Model for Network Security: A message is to be transferred from one party to another across some sort of Internet Service.
- There are two practices which are the principles in the transactions. A Logical information channel is established by defining a route through the Internet from source to destination.

- 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 & so on..



- 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.
- A trusted third party may be needed to achieve secure transmission. For example it is responsible for distributing the secrete information to the two principles while keeping it from any opponent.
- This general model shows that there are four basic tasks in designing a particular security services:
    - Designing a algorithm such that an opponent cannot defeat its purpose.
    - Generate the secrete information to be used with the algorithm.
    - Develop methods for the distribution and sharing of the secret information.
    - 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.

Information Security

- **Information Security** is not all about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electrical one.
- Information can be anything like Your details or we can say your profile on social media, your data in mobile phone, your biometrics etc. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc.
- Information Security programs are build around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.

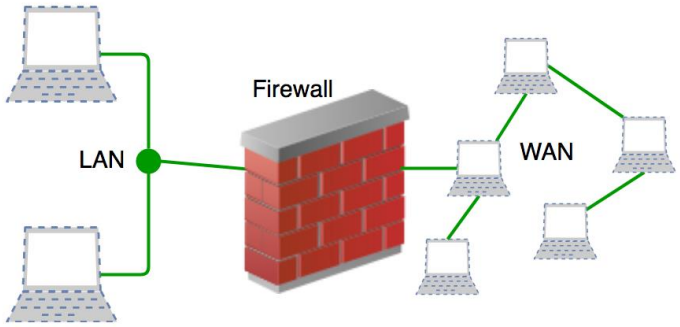
Confidentiality – means information is not disclosed to unauthorized individuals, entities and process.

For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.

Integrity – means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way.

For example if an employee leaves an organisation then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.

must



Availability – means information be available when needed. For example if one needs to access information of a particular employee to check whether employee has outstanded the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management. Denial of service attack is one of the factor that can hamper the availability of information.

Firewall

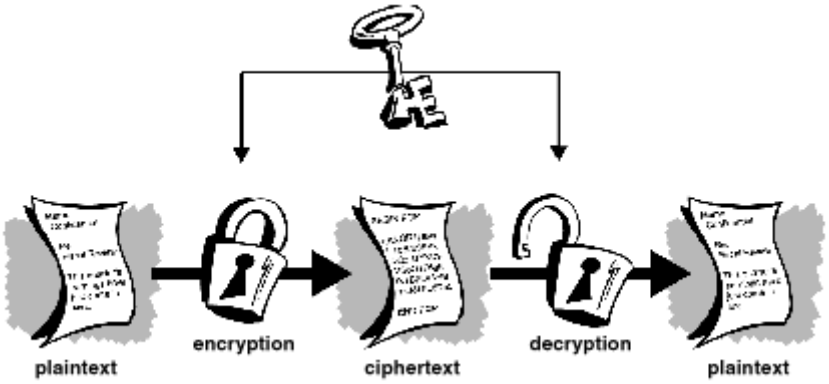
- A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.
- **Accept** : allow the traffic
  Reject : block the traffic but reply with an "unreachable error"
  Drop : block the traffic with no reply
- A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.

Working of Firewalls

- Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.
  From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication. Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.

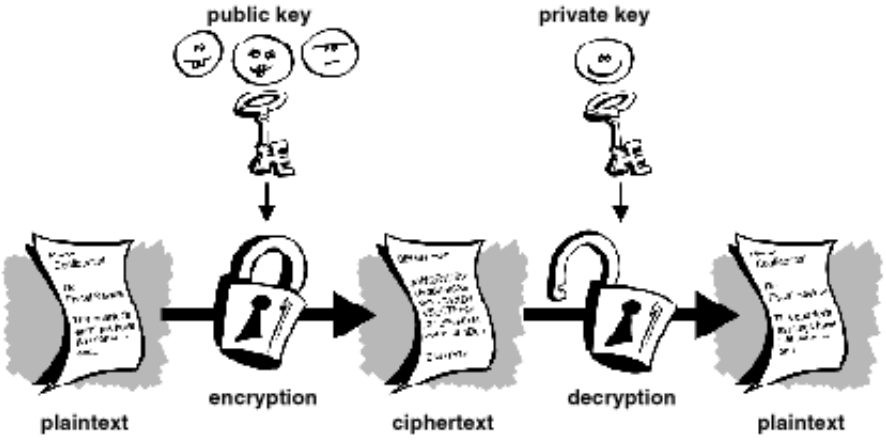
Conventional Cryptography

- In conventional cryptography, also called *secret-key* or *symmetric-key* encryption, one key is used both for encryption and decryption. The Data Encryption Standard (DES) is an example of a conventional cryptosystemthat is widely employed by the Federal Government. *Figure 1-2* is an illustration of the conventional encryption process.



- Caesar's Cipher An extremely simple example of conventional cryptography is a substitution cipher. A substitution cipher substitutes one piece of information for another. This is most frequently done by offsetting letters of the alphabet. Two examples are Captain Midnight's Secret Decoder Ring, which you may have owned when you were a kid, and Julius Caesar's cipher. In both cases, the algorithm is to offset the alphabet and the key is the number of characters to offset it.
- For example, if we encode the word "SECRET" using Caesar's key value of 3, we offset the alphabet so that the 3rd letter down (D) begins the alphabet.
- So starting with
- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- and sliding everything up by 3, you get
- DEFGHIJKLMNOPQRSTUVWXYZABC
- where D=A, E=B, F=C, and so on.
- Using this scheme, the plaintext, "SECRET" encrypts as "VHFUHW." To allow someone else to read the ciphertext, you tell them that the key is 3.
- Obviously, this is exceedingly weak cryptography by today's standards, but hey, it worked for Caesar, and it illustrates how conventional cryptography works.

Public Key Cryptography



- The problems of key distribution are solved by *public key cryptography,* the concept of which was introduced by Whitfield Diffie and Martin Hellman in 1975.
- Public key cryptography is an asymmetric scheme that uses a *pair* of keys for encryption: a *public key,* which encrypts data, and a corresponding *private,* or *secret key* for decryption. You publish your public key to the world while keeping your private key secret.
- Anyone with a copy of your public key can then encrypt information that only you can read. Even people you have never met.
- It is computationally infeasible to deduce the private key from the public key. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information

Example Of Asymmetric Cryptography:

- Let's now take a look at how Users 1 and 2 can use asymmetric encryption to exchange messages securely.
- First of all, they exchange their public keys. User 1 gives his public key to User 2 and User 2 gives his public key to User 1.
- Now User 1 can share his sensitive document again by taking the document and encrypting it with User 2's public key.
- He then sends the document to User 2, who uses his private key to decrypt the document and read it.
- Because they use asymmetric encryption, only User 2 can decrypt the message. Not even User 1, the creator of the message, can decrypt it, since he doesn't have User 2's private key.
- Users 1 and 2 have to keep their private keys well protected in order to maintain a strong and secure asymmetric encryption.
- If User 1's private key is stolen, it can be used to decrypt all messages that are sent to User 1.
- But the attacker cannot decrypt messages that were sent by User 1, because they can only be decrypted using User 2's private key.
- Asymmetric encryption is used in a lot of places where security really matters.
- You might not be aware of it, but every time you visit a website which has been secured via HTTPS, you're actually using asymmetric encryption.
- It is also used to securely send emails with the PGP protocol. As one last example, Bitcoin uses asymmetric encryption to make sure that only the owner of a money wallet can withdraw or transfer money from it.