NETWORK SECURITY & CRYPTOLOGY

UNIT-1

Security:

Security for information technology (IT) refers to the methods, tools and personnel used to defend an organization's digital assets. The goal of IT security is to protect these assets, devices and services from being disrupted, stolen or exploited by unauthorized users, otherwise known as threat actors.

Network Security:

Network Security refers to the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data, has a degree of solutions against many cyber threats.

Security Threats:

1. Social Engineering

Social engineering attacks rely on manipulating human emotion to gain unauthorized network access. Attackers send messages that arouse curiosity, fear, or other emotions, and trick the user into deploying malware or divulging their network credentials. Common types of social engineering attacks include phishing, baiting, tailgating, and pretexting.

2. DDoS Attacks

A distributed denial of service (DDoS) attack leverages a botnet controlled by the attacker, which may consist of thousands or millions of machines, to flood networks with fake traffic. Sometimes, the goal of a DDoS attack is to distract IT and security teams, while attackers are conducting a primary attack.

3. Insider Threats

Insider threats might be malicious insiders motivated by vengeance or financial gain, compromised accounts, or negligent insiders who violate security policies. Insider threats are difficult to detect with traditional security tools, and because insiders have privileged access to sensitive systems, can be very dangerous.

4. Malware

Malware is malicious software that can spread across computer systems, and can be used to compromise a device or cause damage to data and systems. An especially damaging form of malware is ransomware, which encrypts data, making it unusable to its owners.

5. Third-Party Vendors

Most organizations make use of third-party vendors, and commonly give these vendors access to critical systems. Several global security incidents were due to compromise of high-profile suppliers, which were used by some of the world's leading organizations.

6. Advanced Persistent Threats (APT)

APTs are organized attackers, sometimes operated by groups of hackers, who launch sophisticated, highly evasive attacks against an organization.

APTs typically use multi-stage attacks with several attack vectors (such as social engineering, malware, and vulnerability exploitation) to penetrate a network, get around security defenses, and avoid detection.

Security Services/Principles of Network Security:

1. **Confidentiality:** Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. E.g. Printing, displaying and other forms of disclosure.
2. **Authentication:** Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.
3. **Integrity:** Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.
4. **Non repudiation:** Requires that neither the sender nor the receiver of a message be able to deny the transmission.
5. **Access control:** Requires that access to information resources may be controlled by or the target system.
6. **Availability:** Requires that computer system assets be available to authorized parties when needed.

Security Mechanisms:

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.

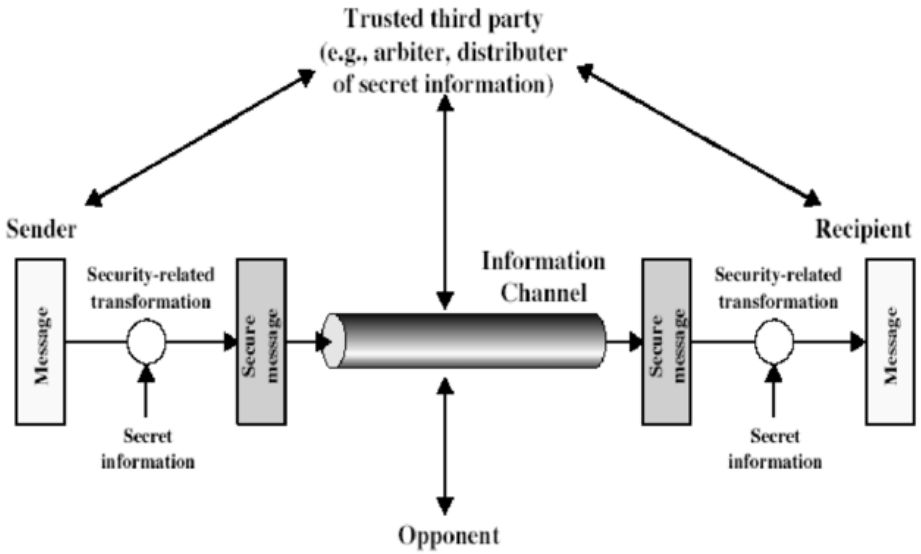
The various security mechanisms to provide security are as follows:

1. **Encipherment:** This is hiding or covering of data which provides confidentiality. It is also used to complement other mechanisms to provide other services. Cryptography and Steganography are used for enciphering
2. **Digital Integrity:** The data integrity mechanism appends to the data a short check value that has been created by a specific process from the data itself. Data integrity is preserved by comparing check value received to the check value generated.
3. **Digital Signature:** A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature. Public and private keys can be used.
4. **Authentication Exchange:** In these two entities exchange some messages to prove their identity to each other.
5. **Traffic Padding:** Traffic padding means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.
6. **Routing Control:** Routing control means selecting and continuously changing different available routes between sender and receiver to prevent the opponent from eavesdropping on a particular route.
7. **Notarization:** Notarization means selecting a third trusted party to control the communication between two entities. The receiver can involve a trusted third party to store the sender request in order to prevent the sender from later denying that she has made a request.
8. **Access Control:** Access control used methods to prove that a user has access right to the data or resources owned by a system. Examples of proofs are passwords and PINs.

Network Security Model:

A Network Security Model exhibits how the security service has been designed over the network to prevent the opponent from causing a threat to the confidentiality or authenticity of the information that is being transmitted through the network.

When we send our data from source side to destination side we have to use some transfer method like the internet or any other communication channel by which we are able to send our message. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. When the transfer of data happened from one source to another source some logical information channel is established between them 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.



Well, we are concerned about the security of the message over the network when the message has some confidential or authentic information which has a threat from an opponent present at the information channel. Any security service would have the **three components** discussed below:

1. A security-related transformation on the information to be sent.
2. Some secret information shared by the two principals and, it is hoped, unknown to the opponent.
3. 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.

Model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of secret information.
4. Specify a protocol to be used by the two principals that make use of the security algorithm and the secret information to achieve a particular security service.

Cryptology:

Cryptology is the mathematics, such as number theory and the application of formulas and algorithms, that underpin cryptography and cryptanalysis. Cryptanalysis concepts are highly specialized and complex, so this discussion will concentrate on some of the key mathematical concepts behind cryptography, as well as modern examples of its use.

In order for data to be secured for storage or transmission, it must be transformed in such a manner that it would be difficult for an unauthorized individual to be able to discover its true meaning. To do this, security systems and software use certain mathematical equations that are very difficult to solve unless strict criteria are met. The level of difficulty of solving a given equation is known as its intractability. These equations form the basis of cryptography.

Cryptography:

Cryptography is technique of securing information and communications through use of codes so that only those persons for whom the information is intended can understand it and process it. Thus, preventing unauthorized access to information.

In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy.

Features Of Cryptography:

1. **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:** The creator/sender of information cannot deny his intention to send information at later stage.
4. **Authentication:** The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Difference between Cryptography and Cryptology:

S no.	Cryptography	Cryptology
1.	Cryptography is the process of conversion of plain text to cipher text.	Cryptology Is the process of conversion of plain text to cipher text and vice versa.
2.	It is also called the study of encryption	It is also called the study of encryption and decryption.
3.	It takes place on the sender side	It takes place on the sender and receiver side
4.	In Cryptography, sender sends the message to receiver.	In Cryptology, both sender and receiver send messages to each other.
5.	Cryptography can be seen as the child of Cryptology	Cryptology can be seen as the parent of Cryptography

Cryptanalysis:

The process of attempting to discover X or K or both is known as cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst.

There are various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

Cipher text only – A copy of cipher text alone is known to the cryptanalyst.

Known plaintext – The cryptanalyst has a copy of the cipher text and the corresponding plaintext.

Chosen plaintext – The cryptanalysts gain temporary access to the encryption machine. They cannot open it to find the key, however; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key.

Chosen cipher text – The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several strings of symbols, and tries to use the results to deduce the key.

Types of Cryptosystems:

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system –

1. Symmetric Key Encryption
2. Asymmetric Key Encryption

1. Symmetric Key Encryption

Symmetric Encryption is an Encryption algorithm where the same key is used for both Encryption and Decryption. The key must be kept secret, and is shared by the message sender and recipient.

Symmetric encryption, also known as single-key and/or private-key encryption, uses a secret key (could be a number, a word, a random string of characters) as a means to modify or mask the content of a given message.

There are two types of symmetric encryption algorithms:

Block algorithms: Set lengths of bits are encrypted in blocks of electronic data with the use of a specific secret key. As the data is being encrypted, the system holds the data in its memory as it waits for complete blocks.

Stream algorithms: Data is encrypted as it streams instead of being retained in the system's memory.

2. Asymmetric Key Encryption:

Asymmetric Encryption is a form of Encryption where keys come in pairs. What one key encrypts, only the other can decrypt.

Asymmetric Encryption is also known as Public Key Cryptography, since users typically create a matching key pair, and make one public while keeping the other secret.

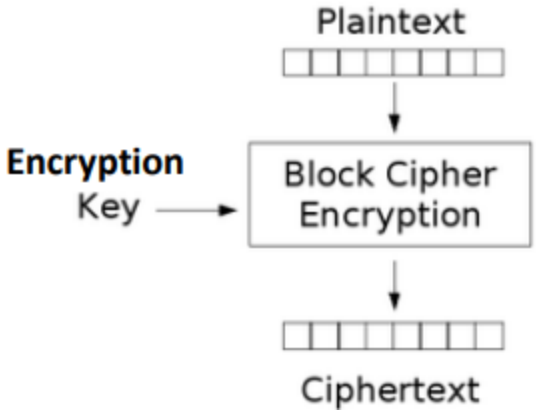
Symmetric v/s Asymmetric

Characteristic	Symmetric Key Cryptography	Asymmetric Key Cryptography
Key used for encryption / decryption	Same key is used for encryption and decryption	One key used for encryption and another, different key is used for decryption
Speed of encryption / decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original clear text size	More than the original clear text size
Key agreement / exchange	A big problem	No problem at all
Number of keys required as compared to the number of participants in the message exchange	Equals about the square of the number of participants, so scalability is an issue	Same as the number of participants, so scales up quite well
Usage	Mainly for encryption and decryption (confidentiality), cannot be used for digital signatures (integrity and non-repudiation checks)	Can be used for encryption and decryption (confidentiality) as well as for digital signatures (integrity and non-repudiation checks)

Block Cipher:

In cryptography, a block cipher is a symmetric key cipher which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation. When encrypting, a block cipher might take (for example) a 128-bit block of plaintext as input, and output a corresponding 128-bit block of cipher text.

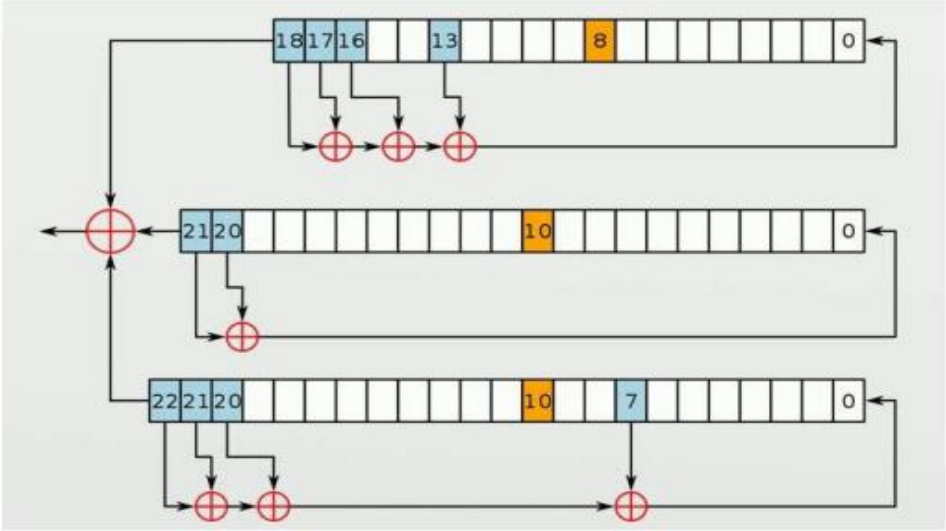
The exact transformation is controlled using a second input — the secret key. Decryption is similar: the decryption algorithm takes, in this example, a 128- bit block of cipher text together with the secret key, and yields the original 128-bit block of plaintext. To encrypt messages longer than the block size (128 bits in the above example), a mode of operation is used.



Stream Cipher:

A stream cipher encrypts plaintext messages by applying an encryption algorithm with a pseudorandom cipher digit stream (key stream). Each bit of the message is encrypted one by one with the corresponding key stream digit. Stream ciphers are typically used in cases where speed and simplicity are both requirements.

It uses an infinite stream of pseudorandom bits as the key. For a stream cipher implementation to remain secure, its pseudorandom generator should be unpredictable and the key should never be reused. Stream ciphers are designed to approximate an idealized cipher, known as the One-Time Pad.



Steganography:

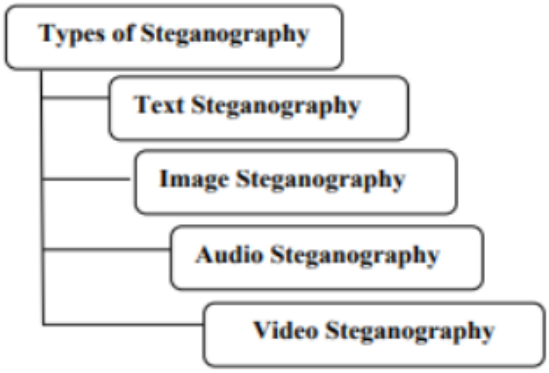
Steganography is the technique of embedding hidden messages /data in such a way that no one can detect the existence of the messages, except the sender and intended receiver(s). The main aim of steganography is to hide the secret message or information in such a way that no one is able to detect it. If they found any suspicion data, then goal is defeated.

The various types of data in steganography can be audio, video, text and images etc.

The basic model of Steganography consists of three components:

- **The Carrier image:** The carrier image is also called the cover object that will carry the message/data which is used to be hidden.
- **The Message:** A message can be anything like data, file or image etc.
- **The Key:** A key is used to decode/decipher the hidden message.

Basic Model of Steganography



Techniques of Steganography