Computer Network Security Sem-6th CSE (Diploma)

UNIT-1 **By:- Mr. Sonu Kumar**

Definition of network security

Network security is the security designed to protect the integrity of the network from unauthorized access and threats. The network administrators are responsible for adopting various defensive measures to guard their networks from possible security risks.

Computer networks are linked in daily transactions and communication within the government, private, or corporates that needs security. The most common and straightforward strategy of protecting network support is allocating it with a unique name and a corresponding password. The network security consists of:

1. **Protection**: The user should be able to configure their devices and networks accurately.
2. **Detection**: The user must detect whether the configuration has changed or get a notification if there is any problem in the network traffic.
3. **Reaction**: After detecting the problems, the user must respond to them and must return to a protected position as quickly as possible.

How does network security work?

Network security works with multiple layers of protection at the edge and in between the network. All the security layers execute some strategies and follow specified policies.

There are different layers to analyze while addressing any network security for an association. Though the attacks can occur at any layer in the network security model, all the network's constituent devices, unlike hardware, software, and policies, must be composed in sync to approach each division.

The network security model is composed of three different controls: physical, technical, and administrative. Let's cover the brief analysis of network security and will learn how each control works.

Security Features for Networks
Physical Layer
Technical Layer
Administ rative Layer

1. Physical Network Security

Physical security networks are developed to restrict unauthorized users from accessing various physical network devices, unlike routers, cabling cupboards, and so on.

2. Technical Network Security

Technical security controls, safeguard the information, put on the network or transferred over, into, or out of the network. Protection is duplex; it requires protecting information and devices from the unofficial group, and it also needs to guard against unofficial exercises from workers.

3. Administrative Network Security

Administrative network security controls end-user behavior, including their authentication, level of access, and how the IT staff of any organization implements reforms to its infrastructure. Administration security includes various security policies and processes to its functioning.

Types of network security

1. Active Devices

Active security gadgets tackle the surplus traffic. For example, Firewalls, antivirus scanning tools, and content filtering appliances are the most commonly used active devices.

2. Passive Devices

Passive devices are used to recognize and block unwanted traffic, such as invasion detection devices.

3. Preventative Devices

Preventative devices are used to scan the networks and detect possible security threats. Penetration testing appliances and vulnerability assessment devices are the common examples of Preventative devices.

4. Unified Threat Management (UTM)

UTM devices act as all-in-one security tools. Firewalls, content filtering, web caching are the common examples of Unified Threat Management.

5. NAC or Network Access Control

NAC is a technique for applying computer security networks at the most fundamental level. For instance, the user could allow administrators full access to the network but deny access to particular confidential files or restrict their system from connecting any network. It is a method that attempts to unite endpoint security technology that supports network security enforcement.

6. Antivirus and Antimalware Software

Antivirus software's are designed to protect the system from a range of malware and malicious software, including viruses, worms, ransomware, and Trojans. The best software scans the malware, quarantines it and stops it before it causes any damage to the system.

7. Firewall Protection

A firewall acts as a defense barrier between your trusted internal networks and untrusted external networks such as viruses, worms, Trojans, brute force attacks. A firewall could be of any form, i.e., software or hardware, unlike a router. Though both the method performs the same function, scanning incoming network traffic to make sure it doesn't contain blacklisted data.

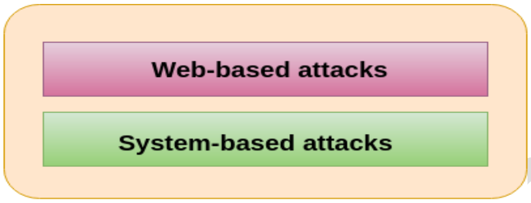
8. Virtual Private Networks

VPN supports the user in creating a secure and reliable private connection between the networks used by his computer or device to another network across the Internet.

Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

Cyber-attacks can be classified into the following categories:



Classification of Cyber attacks

Web-based attacks

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker?s computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

5. Brute force It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

6. Denial of Service It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

7. Dictionary attacks This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks

1. Virus It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

3. Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

Need of Network Security :-

The network needs security against attackers and hackers. Network Security includes two basic securities. The first is the security of data information i.e. to protect the information from unauthorized access and loss. And the second is computer security i.e. to protect data and to thwart hackers. Here network security not only means security in a single network rather in any network or network of networks.

Now our need of network security has broken into two needs. One is the need of information security and other is the need of computer security.

On internet or any network of an organization, thousands of important information is exchanged daily. This information can be misused by attackers. The information security is needed for the following given reasons.

1. To protect the secret information users on the net only. No other person should see or access it.

2. To protect the information from unwanted editing, accidently or intentionally by unauthorized users.
3. To protect the information from loss and make it to be delivered to its destination properly.
4. To manage for acknowledgement of message received by any node in order to protect from denial by sender in specific situations. For example let a customer orders to purchase a few shares XYZ to the broader and denies for the order after two days as the rates go down.
5. To restrict a user to send some message to another user with name of a third one. For example a user X for his own interest makes a message containing some favourable instructions and sends it to user Y in such a manner that Y accepts the message as coming from Z, the manager of the organization.
6. To protect the message from unwanted delay in the transmission lines/route in order to deliver it to required destination in time, in case of urgency.

Computer Network Models

A communication subsystem is a complex piece of Hardware and software. Early attempts for implementing the software for such subsystems were based on a single, complex, unstructured program with many interacting components. The resultant software was very difficult to test and modify. To overcome such problem, the ISO has developed a layered approach. In a layered approach, networking concept is divided into several layers, and each layer is assigned a particular task. Therefore, we can say that networking tasks depend upon the layers.

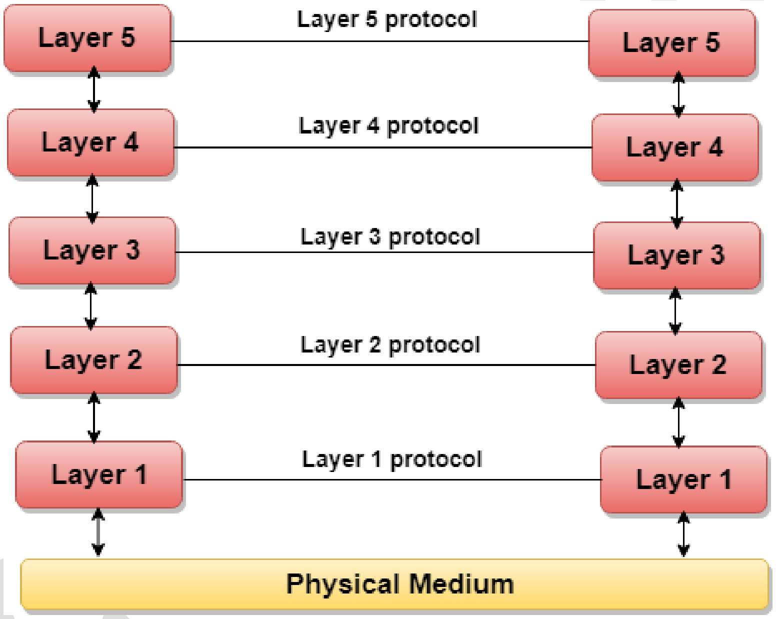
Layered Architecture

- The main aim of the layered architecture is to divide the design into small pieces.
- Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
- It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
- It ensures the independence between layers by providing the services from lower to higher layer without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.
- The number of layers, functions, contents of each layer will vary from network to network. However, the purpose of each layer is to provide the service from lower to a higher layer and hiding the details from the layers of how the services are implemented.
- The basic elements of layered architecture are services, protocols, and interfaces.

- **Service:** It is a set of actions that a layer provides to the higher layer.
- **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
- **Interface:** It is a way through which the message is transferred from one layer to another layer.

- In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.

Let's take an example of the five-layered architecture.



- In case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below it, until the lowest layer is reached.
- Below layer 1 is the physical medium through which the actual communication takes place.
- In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
- The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared

among different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.

- A set of layers and protocols is known as network architecture.

Why do we require Layered architecture?

- **Divide-and-conquer approach:** Divide-and-conquer approach makes a design process in such a way that the unmanageable tasks are divided into small and manageable tasks. In short, we can say that this approach reduces the complexity of the design.
- **Modularity:** Layered architecture is more modular. Modularity provides the independence of layers, which is easier to understand and implement.
- **Easy to modify:** It ensures the independence of layers so that implementation in one layer can be changed without affecting other layers.
- **Easy to test:** Each layer of the layered architecture can be analyzed and tested individually.

Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols that prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security. Secure Communication refers to the scenario where the message or data shared between two parties can't be accessed by an adversary

1. **Confidentiality** refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.

2. **Data integrity** refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.

3. **Authentication** is the process of making sure that the piece of data being claimed by the user belongs to it.

4. **Non-repudiation** refers to the ability to make sure that a person or a party associated with a contract or a communication cannot deny the authenticity of their signature over their document or the sending of a message.

Types of Cryptography:

There are several types of cryptography, each with its own unique features and applications. Some of the most common types of cryptography include:

1.Symmetric-key cryptography: This type of cryptography involves the use of a single key to encrypt and decrypt data. Both the sender and receiver use the same key, which must be kept secret to maintain the security of the communication.

2. Asymmetric-key cryptography: Asymmetric-key cryptography, also known as public-key cryptography, uses a pair of keys – a public key and a private key – to encrypt and decrypt data. The public key is available to anyone, while the private key is kept secret by the owner.

Hash functions: A hash function is a mathematical algorithm that converts data of any size into a fixed-size output. Hash functions are often used to verify the integrity of data and ensure that it has not been tampered with.

Applications of Cryptography:

Cryptography has a wide range of applications in modern-day communication, including:

- **Secure online transactions:** Cryptography is used to secure online transactions, such as online banking and e-commerce, by encrypting sensitive data and protecting it from unauthorized access.
- **Digital signatures:** Digital signatures are used to verify the authenticity and integrity of digital documents and ensure that they have not been tampered with.
- **Password protection:** Passwords are often encrypted using cryptographic algorithms to protect them from being stolen or intercepted.

Military and intelligence applications: Cryptography is widely used in military and intelligence applications to protect classified information and communications.

Challenges of Cryptography:

While cryptography is a powerful tool for securing information, it also presents several challenges, including:

- **Key management**: Cryptography relies on the use of keys, which must be managed carefully to maintain the security of the communication.

- **Quantum computing:** The development of quantum computing poses a potential threat to current cryptographic algorithms, which may become vulnerable to attacks.
- **Human error:** Cryptography is only as strong as its weakest link, and human error can easily compromise the security of a communication.

Advantages of Cryptography

A crucial instrument for information security is cryptography. It offers the four most fundamental information security services:

1. ***Confidentiality*** - An encryption method can protect data and communications against unauthorized access and disclosure.
2. ***Authentication*** - Information can be safeguarded against spoofing and forgeries using cryptographic techniques like MAC and digital signatures, which are used for authentication.
3. ***Data Integrity*** - Cryptographic hash functions are essential in giving users confidence in the accuracy of their data.
4. ***Non-repudiation*** - A digital signature offers the non-repudiation service to protect against disputes that can develop if the sender refuses to acknowledge receipt of the communication.

Disadvantages of Cryptography

- Even an authorized user may find it challenging to access strongly encrypted, authenticated, and password-protected information at a time when access is vital for decision-making. An intrusive party may attempt to assault the network or computer system and disable it.
- Cryptography cannot guarantee high availability, one of the core components of information security. Other defense strategies are required to counter dangers like denial of service (DoS) attacks and total information system failure.
- Selective access control, another essential requirement of information security, also cannot be met by using cryptography. For the same, administrative controls and processes must be used.

- The dangers and weaknesses that result from the shoddy systems, methods, and procedures are not protected by cryptography. These require the correct design and construction of a defensive infrastructure to be installed.
- Cryptography is not free. Costs include both time and money.
    - Information processing is delayed when encryption mechanisms are added.
    - Public key infrastructure must be built up and maintained in order to employ public key cryptography, which needs substantial financial investment.

What is Substitution Technique?

The ***substitution technique*** involves replacing letters with other letters and symbols. In simple terms, the plaintext characters are substituted, and additional substitute letters, numerals, and symbols are implemented in their place. The Caesar cipher employs the substitution technique. In this technique, the alphabet is substituted with the alphabet three positions forward of the line. The substitution cipher technique was invented by Julius Caesar and named after him as the Caesar Cipher.

Features of Substitution Technique

There are various features of the ***substitution technique***. Some features of substitution techniques are as follows:

1. In the substitution cipher technique, the letters in plain text are substituted by other letters, numbers, or symbols.
2. A character's identity is changed, but its place remains constant in the substitution technique.
3. Some algorithms that use the substitution technique are monoalphabetic substitution cipher, Playfair cipher, and polyalphabetic substitution cipher.
4. The substitution cipher approach allows for the detection of plain text by low-frequency letters.
5. Caesar Cipher is an example of the substitution cipher technique.

What is Transposition Technique?

In the ***transposition technique***, the characters' identities are kept the same, but their positions are altered to produce the ciphertext. A transposition cipher in cryptography is a type of encryption that scrambles the locations of characters without altering the characters themselves. Transposition ciphers produce a ciphertext that is a permutation of the plaintext by rearranging the components of the plaintext in accordance with a regular method. It is distinct from substitution ciphers, which don't replace the unit's positions of plaintext but instead substitute the units themselves. A bijective function is utilized to the character locations to encrypt data, and an inverse function is employed to decode data. It is not a very secure technique.

Features of the Transposition Technique

There are various features of the ***transposition technique***. Some main features of the transposition techniques are as follows:

1. The keys that are closer to the proper key in the transposition cipher technique can reveal plain text.
2. The transposition cipher approach does not exchange one sign for another but rather moves the symbol.
3. The two most common types of transposition cipher are keyless and keyed transpositional cipher.
4. The Reil Fence Cipher is an excellent instance of a transposition tehnique.
5. The position of the character is modified in the transposition cipher technique, but the character's identity remains unchanged.

Substitution Technique:-

There are various key differences between ***Substitution Technique and Transposition Technique***. Some main key differences between these techniques are as follows:

1. The substitution approach employs a substitute for the plaintext characters to transform them into ***ciphertext***. In contrast, the transposition technique essentially rearranges the plaintext characters.
2. The substitution technique aims to change the entity's identification. In contrast, the transposition technique affects the entity's position instead of its identity.

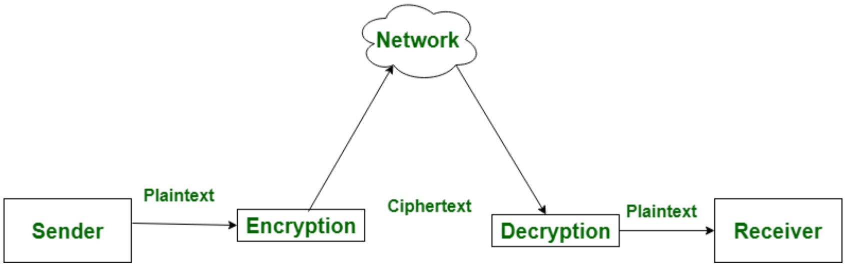
3. The substitution technique replaces every character with an ***integer, character, and symbol***. In contrast, in the transposition technique, every character has been positioned from its actual position.
4. Some algorithms that use the substitution technique are monoalphabetic, polyalphabetic substitution cipher, and Playfair cipher. In contrast, the transposition techniques utilize the keyed and keyless transpositional ciphers.
5. The plaintext in the substitution strategy could be easily determined using the low-frequency letter. In contrast, in the transposition technique, the keys close to the right key lead to the plaintext discovery.

Features	Substitution Technique	Transposition Technique
Definition	It replaces the plaintext characters with other numbers, characters, and symbols.	It scrambles the character's position in the plaintext.
Alterations	The character's identity is changed, while its position does not change.	The character's identity is changed instead of its identity.
Forms	It utilizes the monoalphabetic, polyalphabetic substitution cipher, and Playfair cipher.	It utilizes the keyed and keyless transpositional ciphers.
Detection	The low-frequency letter may easily identify the plaintext.	The keys close to the right key lead to the discovery of the plaintext.
Examples	Caesar Cipher	Reil Fence Cipher

Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext). Whereas.

Decryption is the process of converting meaningless message (Ciphertext) into its original form (Plaintext).

The major distinction between secret writing associated secret writing is that the conversion of a message into an unintelligible kind that's undecipherable unless decrypted.



S.NO	Encryption	Decryption
1.	Encryption is the process of converting normal message into meaningless message.	While decryption is the process of converting meaningless message into its original form.
2.	Encryption is the process which take place at sender's end.	While decryption is the process which take place at receiver's end.
3.	Its major task is to convert the plain text into cipher text.	While its main task is to convert the cipher text into plain text.
4.	Any message can be encrypted with either secret key or public key.	Whereas the encrypted message can be decrypted with either secret key or private key.
5.	In encryption process, sender sends the data to receiver after encrypted it.	Whereas in decryption process, receiver receives the information(Cipher text) and convert into plain text.
6.	The same algorithm with the same key is used for the encryption-decryption process.	The only single algorithm is used for encryption-decryption with a pair of keys where each use for encryption and decryption.

What is encryption?

Encryption means that the sender converts original information into another form and sends the unintelligible message over the network. It helps us to secure data that we send, receives, and store. Data can be text messages saved on our cell phone, logs stored on our fitness watch, and details of banking sent by your online account.

It is the procedure of taking ordinary text, such as a text or email, and transforming it into an unreadable type of format known as "cipher text."

Aymmetric encryption

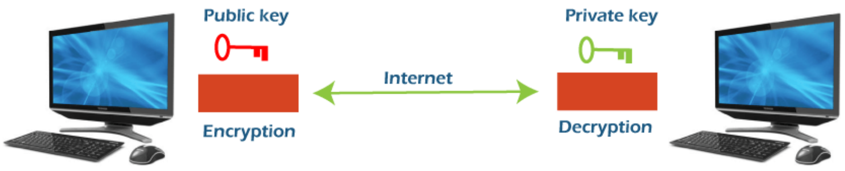
Symmetric encryption encrypts and decrypts the information using a single password. In this encryption technique, the message is encrypted with a key, and the same key is used for decrypting the message. It is the simplest and commonly known encryption technique. It makes it easy to use but less secure.

It is called symmetric encryption because the same key is responsible for encrypting or decrypting the data. The single key used in symmetric encryption is used to encrypt plain text into ciphertext, and that same key is used to decrypt that ciphertext back into plain text.

Symmetric encryption is also called secret key encryption. The algorithm behind the symmetric encryption executes faster and less complex, so it is the preferred technique to transmit the data in bulk.

Asymmetric encryption

Asymmetric encryption uses two keys for encryption and decryption. It is based on the technique of public and private keys. A public key, which is interchanged between more than one user. Data is decrypted by a private key, which is not exchanged. It is slower but more secure.



Asymmetric Encryption

On the basis of	Symmetric Encryption	Asymmetric Encryption
Keys used	It uses a single shared key (secret key) to encrypt and decrypt the message.	It uses two different keys for encryption and decryption.
Size	The size of ciphertext in symmetric encryption could be the same or smaller than the plain text.	The size of ciphertext in asymmetric encryption could be the same or larger than the plain text.
Efficiency	It is efficient as this technique is recommended for large amounts of text.	It is inefficient as this technique is used only for short messages.
Speed	The encryption process of symmetric encryption is faster as it uses a single key for encryption and decryption.	The encryption process in asymmetric encryption is slower as it uses two different keys; both keys are related to each other through the complicated mathematical process.
Purpose	Symmetric encryption is mainly used to transmit bulk data.	It is mainly used in smaller transactions. It is used for establishing a secure connection channel before transferring the actual data.
Security	It is less secured as there is a use of a single key for encryption.	It is safer as there are two keys used for encryption and decryption.
Algorithms	The algorithms used in symmetric encryption are 3DES, AES, DES, and RC4.	RSA, DSA, Diffie-Hellman, ECC, Gamal, and EI.
Existence	It is an old technique.	It is a new technique.

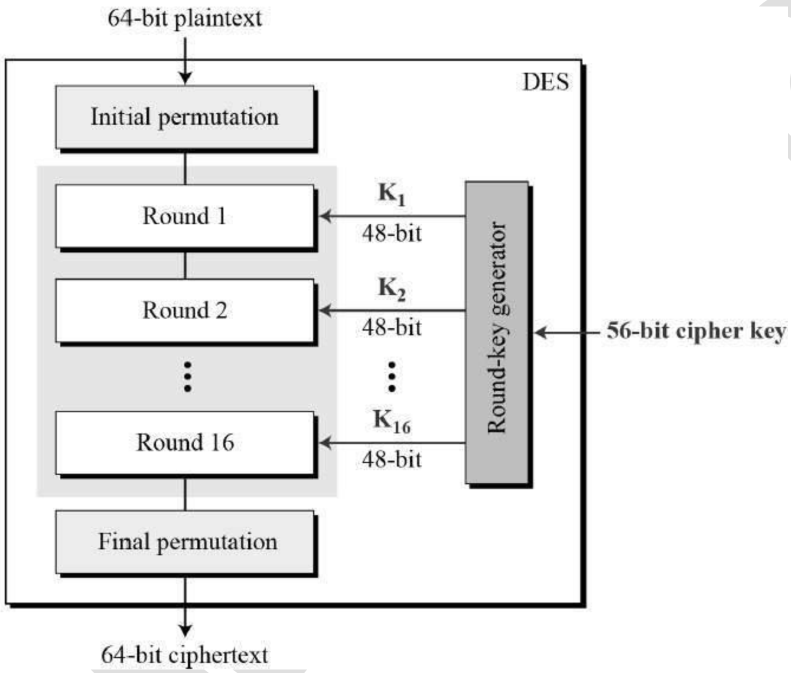
Key Range:-The concept of key range and key-size are related to each other. Key Range is total number of keys from smallest to largest available key.

• If the key is found, the attacker can get original plaintext message. In the brute force attack, every possible key in the key-range is tried, until we get the right key.
• In the best case, the right key is found in the first attempt, in the worst case, the key is found in the last attempt.

UNIT-2

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration –



Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows −

Round Function

The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration −

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

- **Avalanche effect** − A small change in plaintext results in the very great change in the ciphertext.
- **Completeness** − Each bit of ciphertext depends on many bits of plaintext.

During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

Modes of Operation For DES

There are the following five modes of operation that can be chosen:

1. **ECB (Electronic Codebook):** Each 64-bit block is encrypted and decrypted independently.
2. **CBC (Cipher Block Chaining):** In block chaining, each block depends on the previous one and uses an Initialization Vector (IV).
3. **CFB (Cipher Feedback):** The ciphertext that we get from the previous step becomes the input for the algorithm. The operation produces the pseudorandom output. The output that we get is XORed with the plaintext and generates the ciphertext for the next operation.
4. **OFB (Output Feedback):** It is just like CFB. Except that the encryption algorithm input is the output from the preceding DES.
5. **CTR (Counter)**: Each plaintext block is XORed with an encrypted counter. After that, the counter is incremented for each subsequent block.

What is Data Encryption Standard (DES)?

Data Encryption Standard (DES) is an outdated symmetric key method of data encryption. It was adopted in 1977 for government agencies to protect sensitive data and was officially retired in 2005.

IBM researchers originally designed the standard in the early 1970s. It was then adopted by the U.S. National Bureau of Standards -- now the National Institute of Standards and Technology, or NIST -- as an official Federal Information Processing Standard (FIPS) in 1977 for the encryption of commercial and sensitive yet unclassified government computer data.

DES was the first encryption algorithm the U.S. government approved for public disclosure. This move ensured it was quickly adopted by industries, such as financial services, that needed strong encryption. Because of its simplicity, DES was also used in a variety of embedded systems, including the following:

- smart cards
- SIM cards
- modems
- routers
- set-top boxes

How does DES work?

DES uses the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key. DES was once the go-to, symmetric key algorithm for the encryption of electronic data, but it has been superseded by the more secure Advanced Encryption Standard (AES) algorithm.

Some key features affecting how DES works include the following:

- **Block cipher.** The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time. To encrypt a plaintext message, DES groups it into 64-bit blocks. Each block is enciphered using the secret key into a 64-bit ciphertext by means of permutation and substitution.

- **Several rounds of encryption.** The DES process involves encrypting 16 times. It can run in four different modes, encrypting blocks individually or making each cipher block dependent on all the previous blocks. Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied.
- **64-bit key.** DES uses a 64-bit key, but because eight of those bits are used for parity checks, the effective key length is only 56 bits. The encryption algorithm generates 16 different 48-bit subkeys, one for each of the 16 encryption rounds. Subkeys are generated by selecting and permuting parts of the key as defined by the DES algorithm.
- **Replacement and permutation.** The algorithm defines sequences of replacement and permutation that the ciphertext undergoes during the encryption process.
- **Backward compatibility.** DES also provides this capability in some instances.

How is DES used today?

As deprecated standards, both the DES and 3DES algorithms and key lengths could still be used. However, users must accept that there is a security risk in using the deprecated algorithm and key length and that the risk will increase over time.

DES is no longer trusted for encrypting sensitive data. Before it was deprecated and eventually disallowed, the standard was required for U.S. government financial transactions that used electronic funds transfer. It became the default encryption algorithm used in financial services and other industries.

DES and 3DES continue to be used in limited ways.

3DES. NIST guidance for 3DES will change to disallowed in 2023. At that point, the algorithm and key length will not be used for cryptographic protection.

Cryptographic training. DES and its variants continue to be used today for teaching about cryptography. The algorithms are well understood, and there is a significant body of research into both how effective DES can be and how to effectively attack it. The technology is still used in academia to demonstrate the fundamentals of digital cryptography, including the following:

- substitution and permutation of ciphertexts;
- techniques for applying keys and how to find them; and
- exploiting weaknesses in cryptographic algorithms.

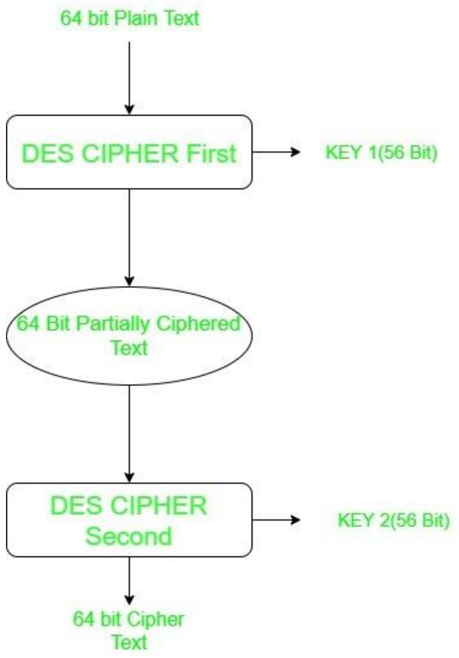
Legacy of DES

Despite having reached the end of its useful life, the arrival of Data Encryption Standard served to promote the study of cryptography and the development of new encryption algorithms. Until DES, cryptography was a dark art confined to military and government intelligence organizations.

Double DES:

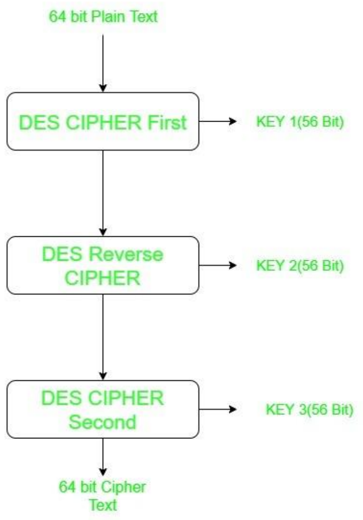
Double DES is a encryption technique which uses two instance of DES on same plain text. In both instances it uses different keys to encrypt the plain text. Both keys are required at the time of decryption.

The 64 bit plain text goes into first DES instance which then converted into a 64 bit middle text using the first key and then it goes to second DES instance which gives 64 bit cipher text by using second key.



However double DES uses 112 bit key but gives security level of 2^56 not 2^112 and this is because of meet-in-the middle attack which can be used to break through double DES.

Triple DES:
Triple DES is a encryption technique which uses three instance of DES on same plain text. It uses there different types of key choosing technique in first all used keys are different and in second two keys are same and one is different and in third all keys are same.



Triple DES is also vulnerable to meet-in-the middle attack because of which it give total security level of 2^112 instead of using 168 bit of key.

The block collision attack can also be done because of short block size and using same key to encrypt large size of text. It is also vulnerable to sweet32 attack.

What is a side-channel attack?

A side-channel attack is a security exploit that aims to gather information from or influence the program execution of a system by measuring or exploiting indirect effects of the system or its hardware -- rather than targeting the program or its code directly. Most commonly, these attacks aim to exfiltrate sensitive information, including cryptographic keys, by measuring coincidental hardware emissions. A side-channel attack may also be referred to as a *sidebar attack* or an *implementation attack*.

Attackers can also go after high-value targets, such as secure processors, Trusted Platform Module (TPM) chips and cryptographic keys. Even having only partial information can assist a traditional attack vector, such as a brute-force attack, to have a greater chance of success.

Side-channel attacks can be tricky to defend against. They are difficult to detect in action, often do not leave any trace and may not alter a system while it's running. Side-channel attacks can even prove effective against air-gapped systems that have been physically segregated from other computers or networks.

Types of side-channel attacks

Bad actors can implement side-channel attacks in several different ways, including the following.

Electromagnetic

An attacker measures the electromagnetic radiation, or radio waves, given off by a target device to reconstruct the internal signals of that device. The earliest side-channel attacks were electromagnetic. van Eck phreaking and the National Security Agency's (NSA) Tempest system could reconstruct the entirety of a computer's screen. Attackers focus modern side-channel attacks on measuring the cryptographic operations of a system to try and derive secret keys. Software-defined radio (SDR) devices have lowered the barrier of entry for electromagnetic attackers, which can be performed through walls and without any contact with the target device.

Acoustic

The attacker measures the sounds produced by a device. Proof-of-concept (POC) attacks have been performed that can reconstruct a user's keystrokes from an audio recording of the user typing. Hackers can obtain some information by listening to the sounds emitted by electronic components as well.

Power

A hacker measures or influences the power consumption of a device or subsystem. By monitoring the amount and timing of power used by a system or one of its subcomponents, an attacker can infer activity of that system. Some attacks may cut or lower power to cause a system to behave in a way beneficial to the attacker, similar to Plundervolt attacks.

Optical

An attacker uses visual cues to gain information about a system. Although rarely used against computers, some POC attacks have been performed where audio can be reconstructed from a video recording of an object vibrating in relation to sounds. Simple shoulder surfing attacks may also fall into this category.

Timing

A bad actor uses the length of time an operation takes to gain information. The total time can provide data about the state of a system or the type of process it is running. Here, the attacker can compare the length of time of a known system to the victim system to make accurate predictions.

Memory cache

An attacker abuses memory caching to gain additional access. Modern systems use data caching and pre-fetching to improve performance. An attacker can abuse these systems to access information that should be blocked. The Spectre and Meltdown vulnerabilities that primarily affected Intel processors exploited this channel.

Hardware weaknesses

Hackers can use physical characteristics of a system to induce a behavior, cause a fault or exploit data remanence, which is data that persists after deletion. Row hammering attacks happen when an attacker causes a change in a restricted area of memory by quickly flipping, or hammering, another area of memory located close by on the physical random access memory (RAM) chip. Error correction code (ECC) memory can help prevent this attack. In a cold boot attack, the attacker quickly lowers the temperature of RAM, causing some of the information to be retained after power is removed so the attacker can read it back.

How to prevent a side-channel attack

Organizations can implement a few best practice mitigations that may help protect against side-channel attacks. These attacks usually require specific detailed knowledge of a system to execute; therefore, a business should keep details related to implementation and vendors as a trade secret.

Address space layout randomization (ASLR) can prevent some memory- or cache-based attacks. Using business-grade equipment can also help to prevent systems from being exploited. Physical access to systems should be restricted as well. Businesses can also keep sensitive systems in shielded Faraday cages, and power conditioning equipment can shield against power attacks.

As extreme mitigations, increasing the amount of noise in a system will make it more difficult for an attacker to gain useful information. Furthermore, while the following ideas are often wasteful and not generally recommended, they may be useful in specific circumstances.

Different Forms of Cryptanalysis:

Cryptanalysis basically has two forms:

1. Linear Cryptanalysis:

Linear cryptanalysis is a general type of cryptanalysis based on discovering affine approximations to a cipher’s action in cryptography. Block and stream ciphers have both been subjected to attacks. Linear cryptanalysis is one of the two most common attacks against block ciphers, with differential cryptanalysis being the other.

2. Differential Cryptanalysis:

Differential cryptanalysis is a sort of cryptanalysis that may be used to decrypt both block and stream ciphers, as well as cryptographic hash functions. In the widest sense, it is the study of how alterations in information intake might impact the following difference at the output. In the context of a block cipher, it refers to a collection of strategies for tracking differences across a network of transformations, finding where the cipher displays non-random behavior, and using such attributes to recover the secret key (cryptography key).

UNIT-3

Symmetric key cryptography:- is a type of encryption scheme in which the similar key is used both to encrypt and decrypt messages. Such an approach of encoding data has been largely used in the previous decades to facilitate secret communication between governments and militaries.

Symmetric-key cryptography is called a shared-key, secret-key, single-key, one-key and eventually private-key cryptography. With this form of cryptography, it is clear that the key should be known to both the sender and the receiver that the shared. The complexity with this approach is the distribution of the key.

Symmetric key cryptography schemes are usually categorized such as stream ciphers or block ciphers. Stream ciphers work on a single bit (byte or computer word) at a time and execute some form of feedback structure so that the key is repeatedly changing.

A block cipher is so-called because the scheme encrypts one block of information at a time utilizing the same key on each block. In general, the same plaintext block will continually encrypt to the same ciphertext when using the similar key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher.

Block ciphers can operate in one of several modes which are as follows −

- Electronic Codebook (ECB) mode is the simplest application and the shared key can be used to encrypt the plaintext block to form a ciphertext block. There are two identical plaintext blocks will always create the same ciphertext block. Although this is the most common mode of block ciphers, it is affected to multiple brute-force attacks.
- Cipher Block Chaining (CBC) mode insert a feedback structure to the encryption scheme. In CBC, the plaintext is exclusively-ORed (XORed) with the prior ciphertext block prior to encryption. In this mode, there are two identical blocks of plaintext not encrypt to the similar ciphertext.
- Cipher Feedback (CFB) mode is a block cipher implementation as a selfsynchronizing stream cipher. CFB mode enable data to be encrypted in units lower than the block size, which can be beneficial in some applications including encrypting interactive terminal input. If it is using 1-byte CFB mode.

  Each incoming character is located into a shift register the similar size as the block, encrypted, and the block transmitted. At the receiving side, the ciphertext is decrypted and the more bits in the block are discarded.
- Output Feedback (OFB) mode is a block cipher implementation conceptually same to a synchronous stream cipher. OFB avoids the similar plaintext block from making the same ciphertext block by using an internal feedback structure that is independent of both the plaintext and ciphertext bitstreams.

What is a Symmetric Key?

a symmetric key is one that is used both to encrypt and decrypt information. This means that to decrypt information, one must have the same key that was used to encrypt it. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption.

What is AES?

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information.

AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection.

The National Institute of Standards and Technology (NIST) started development of AES in 1997 when it announced the need for an alternative to the Data Encryption Standard (DES), which was starting to become vulnerable to brute-force attacks.

How AES encryption works

AES includes three block ciphers:

1. AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages.
2. AES-192 uses a 192-bit key length to encrypt and decrypt a block of messages.
3. AES-256 uses a 256-bit key length to encrypt and decrypt a block of messages.

Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively.

Symmetric, also known as secret key, ciphers use the same key for encrypting and decrypting. The sender and the receiver must both know -- and use -- the same secret key.

The government classifies information in three categories: Confidential, Secret or Top Secret. All key lengths can be used to protect the Confidential and Secret level. Top Secret information requires either 192- or 256-bit key lengths.

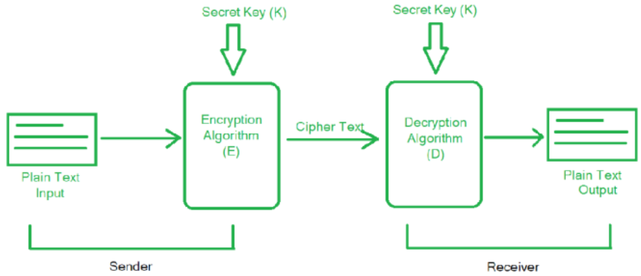
There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. A round consists of several processing steps that include substitution,

What are the features of AES?

NIST specified the new AES algorithm must be a block cipher capable of handling 128-bit blocks, using keys sized at 128, 192 and 256 bits.

Other criteria for being chosen as the next AES algorithm included the following:

- **Security.** Competing algorithms were to be judged on their ability to resist attack as compared to other submitted ciphers. Security strength was to be considered the most important factor in the competition.
- **Cost.** Intended to be released on a global, nonexclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.
- **Implementation.** Factors to be considered included the algorithm's flexibility, suitability for hardware or software implementation, and overall simplicity.
  - **Symmetric Encryption**:- is the most basic and old method of encryption. It uses only one key for the process of both the encryption and decryption of data. Thus, it is also known as Single-Key Encryption.
  - A few basic terms in Cryptography are as follows:
  - ***Plain Text:*** *original message to be communicated between sender and receiver*
  - ***Cipher Text:*** *encoded format of the original message that cannot be understood by humans*
  - ***Encryption (or Enciphering):*** *the conversion of plain text to cipher text*
  - ***Decryption (or Deciphering):*** *the conversion of cipher text to plain text, i.e., reverse of encryption*
  - **The Symmetric Cipher Model:**
  - A symmetric cipher model is composed of five essential parts:



- **1. Plain Text (x):** This is the original data/message that is to be communicated to the receiver by the sender. It is one of the inputs to the encryption algorithm.
- **2. Secret Key (k):** It is a value/string/textfile used by the encryption and decryption algorithm to encode and decode the plain text to cipher text and vice-versa respectively. It is independent of the encryption algorithm. It governs all the conversions in plain text. All the substitutions and transformations done depend on the secret key.
- **3. Encryption Algorithm (E):** It takes the plain text and the secret key as inputs and produces Cipher Text as output. It implies several techniques such as substitutions and transformations on the plain text using the secret key.
- *E(x, k) = y*
- **4. Cipher Text (y):** It is the formatted form of the plain text (x) which is unreadable for humans, hence providing encryption during the transmission. It is completely dependent upon the secret key provided to the encryption algorithm. Each unique secret key produces a unique cipher text.
- **5. Decryption Algorithm (D):** It performs reversal of the encryption algorithm at the recipient's side. It also takes the secret key as input and decodes the cipher text received from the sender based on the secret key. It produces plain text as output.
- *D(y, k) = x*

- **Requirements for Encryption:**

- There are only two requirements that need to be met to perform encryption. They are,

- **1. Encryption Algorithm:** There is a need for a very strong encryption algorithm that produces cipher texts in such a way that the attacker should be unable to crack the secret key even if they have access to one or more cipher texts.
- **2. Secure way to share Secret Key:** There must be a secure and robust way to share the secret key between the sender and the receiver. It should be leakproof so that the attacker cannot access the secret key.

Applications of Blowfish

Blowfish is suitable for a wide range of applications, including the following:

- bulk encryption
- random bit generation
- packet encryption
- password hashing and management
- mobile processors
- email, file or disk encryption
- data backup
- Secure Shell

Blowfish is used by many popular products, such as CryptoDisk, PasswordWallet, Access Manager, Symantec NetBackup and SplashID. Many social media platforms and e-commerce websites also use Blowfish to protect user data.

A series of symmetric encryption algorithms developed by RSA Security.

- **RC4** — a variable key-size stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation.
- **RC5** — a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds. Allowable choices for the block size are 32 bits (for experimentation and evaluation purposes only), 64 bits (for use a drop-in replacement for DES), and 128 bits. The number of rounds can range from 0 to 255, while the key can range from 0 bits to 2040 bits in size. RC5 has three routines: key expansion, encryption, and decryption.
- **RC6** — a block cipher based on RC5. RC6 is a parameterized algorithm where the block size, the key size, and the number of rounds are variable. The upper limit on the key size is 2040 bits. RC6 adds two features to RC5: the inclusion of integer multiplication and the use of four 4-bit working registers instead of RC5 s two 2-bit registers.

Introduction :

The International Data Encryption Algorithm (IDEA) is a symmetric-key block cipher that was first introduced in 1991. It was designed to provide secure encryption for digital data and is used in a variety of applications, such as secure communications, financial transactions, and electronic voting systems.

IDEA uses a block cipher with a block size of 64 bits and a key size of 128 bits. It uses a series of mathematical operations, including modular arithmetic, bit shifting, and exclusive OR (XOR) operations, to transform the plaintext into ciphertext. The cipher is designed to be highly secure and resistant to various types of attacks, including differential and linear cryptanalysis.

One of the strengths of IDEA is its efficient implementation in software and hardware. The algorithm is relatively fast and requires only a small amount of memory and processing power. This makes it a popular choice for use in embedded systems and other applications where resources are limited.

IDEA has been widely used in various encryption applications, although it has been largely replaced by newer encryption algorithms such as AES (Advanced Encryption Standard) in recent years.

The Simplified **International Data Encryption Algorithm (IDEA)** is a **symmetric key block** cipher that:

- uses a fixed-length plaintext of **16 bits** and
- encrypts them in **4 chunks of 4 bits** each
- to produce **16 bits ciphertext**.
- The length of the key used is **32 bits**.
- The key is also divided into 8 blocks of 4 bits each.

Uses of International Data Encryption Algorithm (IDEA) :

Some of the common uses of IDEA include:

1. Secure communication: IDEA can be used to encrypt data transmitted over communication networks such as the internet, providing confidentiality and protecting against unauthorized access.
2. Financial transactions: IDEA can be used to secure financial transactions such as online banking and credit card transactions, helping to prevent identity theft and fraud.
3. Electronic voting systems: IDEA can be used to encrypt votes in electronic voting systems, providing secure and confidential voting.
4. File encryption: IDEA can be used to encrypt files and folders on a computer or other storage device, protecting them from unauthorized access.
5. Password protection: IDEA can be used to encrypt passwords and other sensitive information stored on a computer or network, helping to prevent unauthorized access and data breaches.

Issues in International Data Encryption Algorithm (IDEA) :

1. Key size: While IDEA uses a 128-bit key size, which is generally considered secure, it is still theoretically possible to brute-force the key if an attacker has enough computing power. This is why longer key sizes are often used in modern encryption algorithms.
2. Patents: IDEA was originally patented, which limited its availability and adoption in certain countries. While the patent has since expired, this could still be a consideration for some organizations.

3. Block size: IDEA has a fixed block size of 64 bits, which can limit its effectiveness in certain applications where larger block sizes are required.
4. Implementation issues: Like any encryption algorithm, IDEA can be vulnerable to implementation issues such as side-channel attacks or implementation flaws. This highlights the importance of using best practices and careful implementation when using any encryption algorithm.
5. Availability: While IDEA is still considered to be a strong and effective encryption algorithm, it has been largely replaced by newer algorithms such as AES in modern applications. This means that support and availability of IDEA implementations may become more limited over time.

RSA Encryption Algorithm

RSA encryption algorithm is a type of public-key encryption algorithm. To better understand RSA, lets first understand what is public-key encryption algorithm.

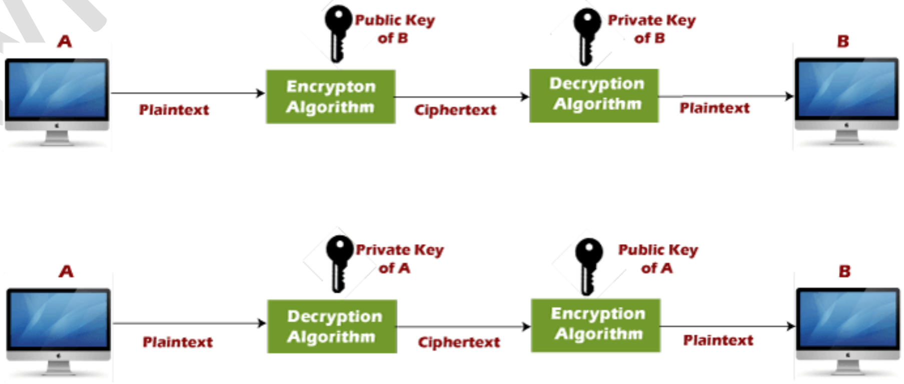
Public key encryption algorithm:

Public Key encryption algorithm is also called the Asymmetric algorithm. Asymmetric algorithms are those algorithms in which sender and receiver use different keys for encryption and decryption. Each sender is assigned a pair of keys:

- **Public key**
- **Private key**

The **Public key** is used for encryption, and the **Private Key** is used for decryption. Decryption cannot be done using a public key. The two keys are linked, but the private key cannot be derived from the public key. The public key is well known, but the private key is secret and it is known only to the user who owns the key. It means that everybody can send a message to the user using user's public key. But only the user can decrypt the message using his private key.

The Public key algorithm operates in the following manner:



Encryption/decryption using public/private keys

  - The data to be sent is encrypted by sender **A** using the public key of the intended receiver
  - B decrypts the received ciphertext using its private key, which is known only to B. B replies to A encrypting its message using A's public key.
  - A decrypts the received ciphertext using its private key, which is known only to him.

Advantages:

- **Security:** RSA algorithm is considered to be very secure and is widely used for secure data transmission.
- **Public-key cryptography:** RSA algorithm is a public-key cryptography algorithm, which means that it uses two different keys for encryption and decryption. The public key is used to encrypt the data, while the private key is used to decrypt the data.
- **Key exchange:** RSA algorithm can be used for secure key exchange, which means that two parties can exchange a secret key without actually sending the key over the network.
- **Digital signatures:** RSA algorithm can be used for digital signatures, which means that a sender can sign a message using their private key, and the receiver can verify the signature using the sender’s public key.
- **Speed:** The RSA technique is suited for usage in real-time applications since it is quite quick and effective.
- **Widely used:** Online banking, e-commerce, and secure communications are just a few fields and applications where the RSA algorithm is extensively developed.

Disadvantages:

- **Slow processing speed:** RSA algorithm is slower than other encryption algorithms, especially when dealing with large amounts of data.
- **Large key size:** RSA algorithm requires large key sizes to be secure, which means that it requires more computational resources and storage space.
- **Vulnerability to side-channel attacks:** RSA algorithm is vulnerable to side-channel attacks, which means an attacker can use information leaked through side channels such as power consumption, electromagnetic radiation, and timing analysis to extract the private key.
- **Limited use in some applications:** RSA algorithm is not suitable for some applications, such as those that require constant encryption and decryption of large amounts of data, due to its slow processing speed.
- **Complexity:** The RSA algorithm is a sophisticated mathematical technique that some individuals may find challenging to comprehend and use.
- **Key Management:** The secure administration of the private key is necessary for the RSA algorithm, although in some cases this can be difficult.
- **Vulnerability to Quantum Computing:** Quantum computers have the ability to attack the RSA algorithm, potentially decrypting the data.

UNIT-4

What is asymmetric cryptography?

Asymmetric cryptography, also known as public-key cryptography, is a process that uses a pair of related keys -- one public key and one private key -- to encrypt and decrypt a message and protect it from unauthorized access or use.

A public key is a cryptographic key that can be used by any person to encrypt a message so that it can only be decrypted by the intended recipient with their private key. A private key -- also known as a secret key -- is shared only with key's initiator.

When someone wants to send an encrypted message, they can pull the intended recipient's public key from a public directory and use it to encrypt the message before sending it. The recipient of the message can then decrypt the message using their related private key.

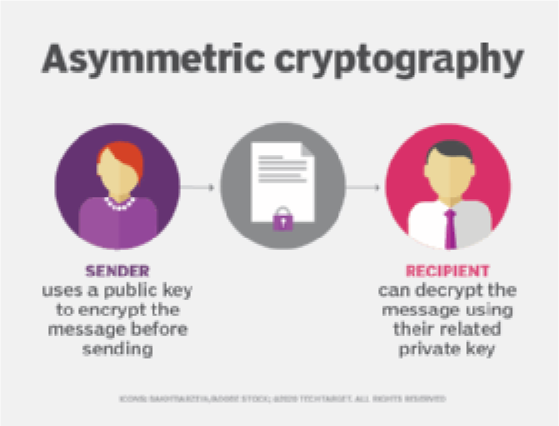
If the sender encrypts the message using their private key, the message can be decrypted only using that sender's public key, thus authenticating the sender. These encryption and decryption processes happen automatically; users do not need to physically lock and unlock the message.

Many protocols rely on asymmetric cryptography, including the transport layer security (TLS) and secure sockets layer (SSL) protocols, which make HTTPS possible.

The encryption process is also used in software programs that need to establish a secure connection over an insecure network, such as browsers over the internet, or that need to validate a digital signature.

How does asymmetric cryptography work?

Asymmetric encryption uses a mathematically related pair of keys for encryption and decryption: a public key and a private key. If the public key is used for encryption, then the related private key is used for decryption. If the private key is used for encryption, then the related public key is used for decryption.


Asymmetric cryptography
SENDER
uses a public key to encrypt the message before sending
RECIPIENT
can decrypt the message using their related private key

Asymmetric cryptography involves a pair of keys to encrypt and decrypt data.

The two participants in the asymmetric encryption workflow are the sender and the receiver. Each has its own pair of public and private keys. First, the sender obtains the receiver's public key. Next, the plaintext message is encrypted by the sender using the receiver's public key. This creates ciphertext. The ciphertext is sent to the receiver, who decrypts it with their private key, returning it to legible plaintext.

Because of the one-way nature of the encryption function, one sender is unable to read the messages of another sender, even though each has the public key of the receiver.

Uses of asymmetric cryptography

Asymmetric cryptography is typically used to authenticate data using digital signatures. A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It is the digital equivalent of a handwritten signature or stamped seal.

Based on asymmetric cryptography, digital signatures can provide assurances of evidence to the origin, identity and status of an electronic document, transaction or message, as well as acknowledge informed consent by the signer.

Asymmetric cryptography can also be applied to systems in which many users may need to encrypt and decrypt messages, including:

- **Encrypted email.** A public key can be used to encrypt a message and a private key can be used to decrypt it.
- **SSL/TLS.** Establishing encrypted links between websites and browsers also makes use of asymmetric encryption.
- **Cryptocurrencies.** Bitcoin and other cryptocurrencies rely on asymmetric cryptography. Users have public keys that everyone can see and private keys that are kept secret. Bitcoin uses a cryptographic algorithm to ensure only legitimate owners can spend the funds.

What are the benefits and disadvantages of asymmetric cryptography?

The benefits of asymmetric cryptography include:

- The key distribution problem is eliminated because there's no need for exchanging keys.
- Security is increased since the private keys don't ever have to be transmitted or revealed to anyone.
- The use of digital signatures is enabled so that a recipient can verify that a message comes from a particular sender.
- It allows for nonrepudiation so the sender can't deny sending a message.

Disadvantages of asymmetric cryptography include:

- It's a slow process compared to symmetric cryptography. Therefore, it's not appropriate for decrypting bulk messages.

- If an individual loses his private key, he can't decrypt the messages he receives.
- Because public keys aren't authenticated, no one can ensure a public key belongs to the person specified. Consequently, users must verify that their public keys belong to them.
- If a malicious actor identifies a person's private key, the attacker can read that individual's messages.

What are examples of asymmetric cryptography?

The RSA algorithm -- the most widely used asymmetric algorithm -- is embedded in the SSL/TLS, which is used to provide secure communications over a computer network. RSA derives its security from the computational difficulty of factoring large integers that are the product of two large prime numbers.

Multiplying two large primes is easy, but the difficulty of determining the original numbers from the product -- *factoring* -- forms the basis of public-key cryptography security. The time it takes to factor the product of two sufficiently large primes is beyond the capabilities of most attackers.

RSA keys are typically 1024 or 2048 bits long, but experts believe 1024-bit keys will be broken soon, which is why government and industry are moving to a minimum key length of 2048-bits.

Elliptic Curve Cryptography (ECC) is gaining favor with many security experts as an alternative to RSA. ECC is a public-key encryption technique based on elliptic curve theory. It can create faster, smaller and more efficient cryptographic keys through the properties of the elliptic curve equation.

To break ECC, an attacker must compute an elliptic curve discrete logarithm, which is significantly more difficult problem than factoring. As a result, ECC key sizes can be significantly smaller than those required by RSA while still delivering equivalent security with lower computing power and battery resource usage.

What's the history of asymmetric cryptography?

Whitfield Diffie and Martin Hellman, researchers at Stanford University, first publicly proposed asymmetric encryption in their 1977 paper, "New Directions in Cryptography."

The concept was independently and covertly proposed by James Ellis several years earlier, while he was working for the Government Communications Headquarters (GCHQ), the British intelligence and security organization.

What is a digital certificate?

A digital certificate, also known as a *public key certificate*, is used to cryptographically link ownership of a public key with the entity that owns it. Digital certificates are for sharing public keys to be used for encryption and authentication.

Digital certificates include the public key being certified, identifying information about the entity that owns the public key, metadata relating to the digital certificate and a digital signature of the public key the certificate issuer created.

The distribution, authentication and revocation of digital certificates are the primary functions of the public key infrastructure (PKI), the system that distributes and authenticates public keys.

How are digital certificates used?

Digital certificates are used in the following ways:

- Credit and debit cards use chip-embedded digital certificates that connect with merchants and banks to ensure that the transactions performed are secure and authentic.
- Digital payment companies use digital certificates to authenticate their automated teller machines, kiosks and point-of-sale equipment in the field with a central server in their data center.

- Websites use digital certificates for domain validation to show they are trusted and authentic.
- Digital certificates are used in secure email to identify one user to another and may also be used for electronic document signing. The sender digitally signs the email, and the recipient verifies the signature.
- Computer hardware manufacturers embed digital certificates into cable modems to help prevent the theft of broadband service through device cloning.

What are the different types of digital certificates?

Web servers and web browsers use three types of digital certificates to authenticate over the internet. These digital certificates are used to link a web server for a domain to the individual or organization that owns the domain. They are usually referred to as *SSL certificates* even though the Transport Layer Security protocol has superseded SSL. The three types are the following:

1. **Domain-validated (DV) SSL** certificates offer the least amount of assurance about the holder of the certificate. Applicants for DV SSL certificates need only demonstrate that they have the right to use the domain name. While these certificates can ensure the certificate holder is sending and receiving data, they provide no guarantees about who that entity is.
2. **Organization-validated (OV) SSL** certificates provide additional assurances about the certificate holder. They confirm that the applicant has the right to use the domain. OV SSL certificate applicants also undergo additional confirmation of their ownership of the domain.
3. **Extended validation (EV) SSL** certificates are issued only after the applicant proves their identity to the CA's satisfaction. The vetting process verifies the existence of the entity applying for the certificate, ensures that identity matches official records and is authorized to use the domain, and confirms that the domain owner has authorized issuance of the certificate.

The exact methods and criteria CAs follow to provide these types of SSL certificates for web domains is evolving as the CA industry adapts to new conditions and applications.

There are also other types of digital certificates used for different purposes:

- **Code signing certificates** may be issued to organizations or individuals who publish software. These certificates are used to share public keys that sign software code, including patches and software updates. Code signing certificates certify the authenticity of the signed code.
- **Client certificates**, also called a *digital ID*, are issued to individuals to bind their identity to the public key in the certificate. Individuals can use these certificates to digitally sign messages or other data. They can also use their private keys to encrypt data that recipients can decrypt using the public key in the client certificate.

Digital certificate benefits

Digital certificates provide the following benefits:

- **Privacy.** When you encrypt communications, digital certificates safeguard sensitive data and prevent the information from being seen by those unauthorized to view it. This technology protects companies and individuals with large troves of sensitive data.
- **Ease of use.** The digital certification process is largely automated.
- **Cost effectiveness.** Compared to other forms of encryption and certification, digital certificates are cheaper. Most digital certificates cost less than $100 annually.
- **Flexibility.** Digital certificates do not have to be purchased from a CA. For organizations that are interested in creating and maintaining their own internal pool of digital certificates, a do-it-yourself approach to digital certificate creation is feasible.

Digital certificate limitations

Some limitations of digital certificates include the following:

- **Security.** Like any other security deterrent, digital certificates can be hacked. The most logical way for a mass hack to occur is if the issuing digital CA is hacked. This gives bad actors an on-ramp into penetrating the repository of digital certificates the authority hosts.
- **Slow performance.** It takes time to authenticate digital certificates and to encrypt and decrypt. The wait time can be frustrating.
- **Integration.** Digital certificates are not standalone technology. To be effective, they must be properly integrated with systems, data, applications, networks and hardware. This is no small task.
- **Management.** The more digital certificates a company uses, the greater the need to manage them and to track which ones are expiring and need to be renewed. Third parties can provide these services, or companies can opt to do the job themselves. But it can be expensive.

Public Key Infrastructure (PKI):- is used to manage pairs of **public and private keys** and bind them to the identities of entities, such as persons and organizations, through the issuance of electronic documents called **digital certificates**.

The mathematics behind PKI ensure that if a certificate is **signed** with a given entity's private key, anyone with the public key from the pair can.

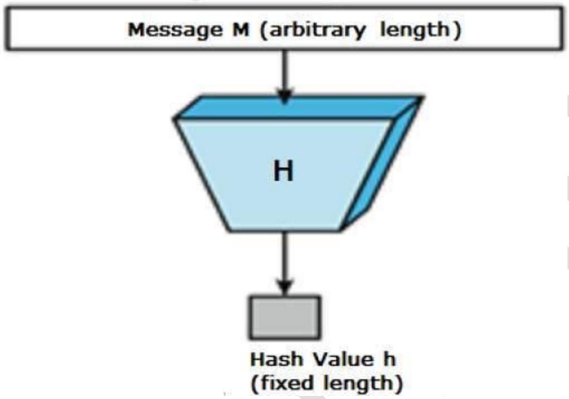
- Verify that the entity presenting the signed certificate is in possession of its corresponding private key **(authenticity)**.
- Trust that the content of the certificate has not been altered since it was initially generated **(integrity)**.
- Use the public key to encrypt a message that can only be decrypted with its associated private key **(encryption)**.

UNIT-5

Cryptography Hash functions:- Hash functions are extremely useful and appear in almost all information security applications.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called **message digest** or simply **hash values**. The following picture illustrated hash function −



Features of Hash Functions

The typical features of hash functions are −

- **Fixed Length Output (Hash Value)**
  - Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as **hashing the data**.
  - In general, the hash is much smaller than the input data, hence hash functions are sometimes called **compression functions**.
  - Since a hash is a smaller representation of a larger data, it is also referred to as a **digest**.
  - Hash function with n bit output is referred to as an **n-bit hash function**. Popular hash functions generate values between 160 and 512 bits.
- **Efficiency of Operation**
  - Generally for any hash function h with input x, computation of h(x) is a fast operation.
  - Computationally hash functions are much faster than a symmetric encryption.

Properties of Hash Functions

In order to be an effective cryptographic tool, the hash function is desired to possess following properties −

- **Pre-Image Resistance**
  - This property means that it should be computationally hard to reverse a hash function.
  - In other words, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z.
  - This property protects against an attacker who only has a hash value and is trying to find the input.
- **Second Pre-Image Resistance**
  - This property means given an input and its hash, it should be hard to find a different input with the same hash.
  - In other words, if a hash function h for an input x produces hash value h(x), then it should be difficult to find any other input value y such that h(y) = h(x).
  - This property of hash function protects against an attacker who has an input value and its hash, and wants to substitute different value as legitimate value in place of original input value.
- **Collision Resistance**
  - This property means it should be hard to find two different inputs of any length that result in the same hash. This property is also referred to as collision free hash function.
  - In other words, for a hash function h, it is hard to find any two different inputs x and y such that h(x) = h(y).
  - Since, hash function is compressing function with fixed hash length, it is impossible for a hash function not to have collisions. This property of collision free only confirms that these collisions should be hard to find.
  - This property makes it very difficult for an attacker to find two input values with the same hash.
  - Also, if a hash function is collision-resistant **then it is second pre-image resistant.**

Popular Hash Functions

Let us briefly see some popular hash functions −

Message Digest (MD)

MD5 was most popular and widely used hash function for quite some years.

- The MD family comprises of hash functions MD2, MD4, MD5 and MD6. It was adopted as Internet Standard RFC 1321. It is a 128-bit hash function.
- MD5 digests have been widely used in the software world to provide assurance about integrity of transferred file. For example, file servers often provide a pre-computed MD5 checksum for the files, so that a user can compare the checksum of the downloaded file to it.
- In 2004, collisions were found in MD5. An analytical attack was reported to be successful only in an hour by using computer cluster. This collision attack resulted in compromised MD5 and hence it is no longer recommended for use.

Secure Hash Function (SHA)

Family of SHA comprise of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3. Though from same family, there are structurally different.

- The original version is SHA-0, a 160-bit hash function, was published by the National Institute of Standards and Technology (NIST) in 1993. It had few weaknesses and did not become very popular. Later in 1995, SHA-1 was designed to correct alleged weaknesses of SHA-0.
- SHA-1 is the most widely used of the existing SHA hash functions. It is employed in several widely used applications and protocols including Secure Socket Layer (SSL) security.
- In 2005, a method was found for uncovering collisions for SHA-1 within practical time frame making long-term employability of SHA-1 doubtful.
- SHA-2 family has four further SHA variants, SHA-224, SHA-256, SHA-384, and SHA-512 depending up on number of bits in their hash value. No successful attacks have yet been reported on SHA-2 hash function.
- Though SHA-2 is a strong hash function. Though significantly different, its basic design is still follows design of SHA-1. Hence, NIST called for new competitive hash function designs.
- In October 2012, the NIST chose the Keccak algorithm as the new SHA-3 standard. Keccak offers many benefits, such as efficient performance and good resistance for attacks.

RIPEMD

The RIPEMD is an acronym for RACE Integrity Primitives Evaluation Message Digest. This set of hash functions was designed by open research community and generally known as a family of European hash functions.

- The set includes RIPEMD, RIPEMD-128, and RIPEMD-160. There also exist 256, and 320-bit versions of this algorithm.
- Original RIPEMD (128 bit) is based upon the design principles used in MD4 and found to provide questionable security. RIPEMD 128-bit version came as a quick fix replacement to overcome vulnerabilities on the original RIPEMD.
- RIPEMD-160 is an improved version and the most widely used version in the family. The 256 and 320-bit versions reduce the chance of accidental collision, but do not have higher levels of security as compared to RIPEMD-128 and RIPEMD-160 respectively.

Whirlpool

This is a 512-bit hash function.

- It is derived from the modified version of Advanced Encryption Standard (AES). One of the designer was Vincent Rijmen, a co-creator of the AES.
- Three versions of Whirlpool have been released; namely WHIRLPOOL-0, WHIRLPOOL-T, and WHIRLPOOL.

Applications of Hash Functions

There are two direct applications of hash function based on its cryptographic properties.

Password Storage

Hash functions provide protection to password storage.

- Instead of storing password in clear, mostly all logon processes store the hash values of passwords in the file.
- The Password file consists of a table of pairs which are in the form (user id, h(P)).

Data Integrity Check

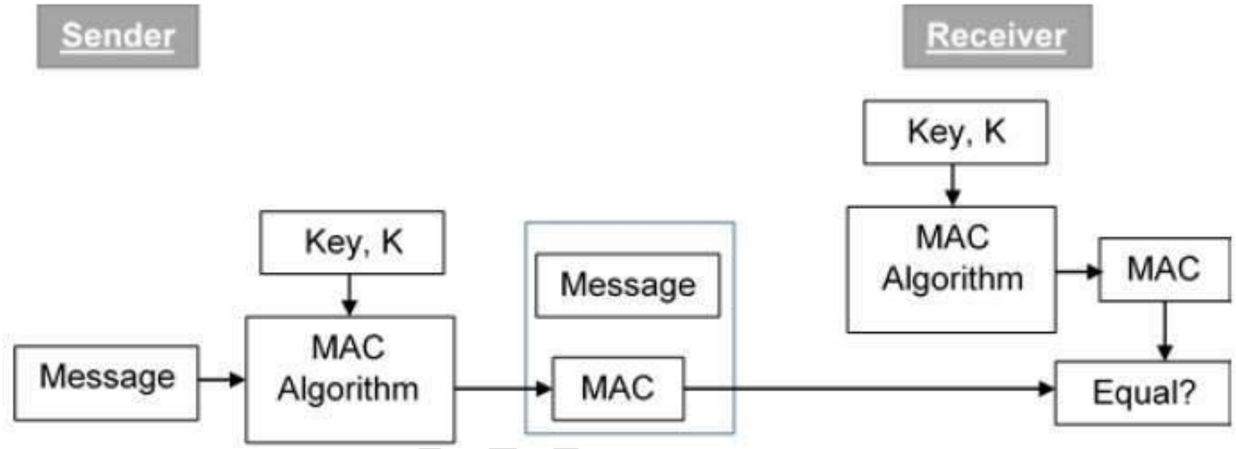
Data integrity check is a most common application of the hash functions. It is used to generate the checksums on data files. This application provides assurance to the user about correctness of the data.

Message Authentication Code (MAC)

MAC algorithm is a symmetric key cryptographic technique to provide message authentication. For establishing MAC process, the sender and receiver share a symmetric key K.

Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.

The process of using MAC for authentication is depicted in the following illustration −



Let us now try to understand the entire process in detail −

- The sender uses some publicly known MAC algorithm, inputs the message and the secret key K and produces a MAC value.
- Similar to hash, MAC function also compresses an arbitrary long input into a fixed length output. The major difference between hash and MAC is that MAC uses secret key during the compression.
- The sender forwards the message along with the MAC. Here, we assume that the message is sent in the clear, as we are concerned of providing message origin authentication, not confidentiality. If confidentiality is required then the message needs encryption.
- On receipt of the message and the MAC, the receiver feeds the received message and the shared secret key K into the MAC algorithm and re-computes the MAC value.
- The receiver now checks equality of freshly computed MAC with the MAC received from the sender. If they match, then the receiver accepts the message and assures himself that the message has been sent by the intended sender.
- If the computed MAC does not match the MAC sent by the sender, the receiver cannot determine whether it is the message that has been altered or it is the origin that has been falsified. As a bottom-line, a receiver safely assumes that the message is not the genuine.

Limitations of MAC

There are two major limitations of MAC, both due to its symmetric nature of operation −

- **Establishment of Shared Secret.**
    - It can provide message authentication among pre-decided legitimate users who have shared key.
    - This requires establishment of shared secret prior to use of MAC.
- **Inability to Provide Non-Repudiation**
    - Non-repudiation is the assurance that a message originator cannot deny any previously sent messages and commitments or actions.
    - MAC technique does not provide a non-repudiation service. If the sender and receiver get involved in a dispute over message origination, MACs cannot provide a proof that a message was indeed sent by the sender.
    - Though no third party can compute the MAC, still sender could deny having sent the message and claim that the receiver forged it, as it is impossible to determine which of the two parties computed the MAC.

ElGamal encryption:- is a public-key cryptosystem. It uses asymmetric key encryption for communicating between two parties and encrypting the message. This cryptosystem is based on the difficulty of finding discrete logarithm **in a cyclic group that is even if we know g^a and g^k, it is extremely difficult to compute g^{ak}.**

Advantages:

- **Security:** ElGamal is based on the discrete logarithm problem, which is considered to be a hard problem to solve. This makes it secure against attacks from hackers.

- **Key distribution:** The encryption and decryption keys are different, making it easier to distribute keys securely. This allows for secure communication between multiple parties.

- **Digital signatures:** ElGamal can also be used for digital signatures, which allows for secure authentication of messages.

Disadvantages:

- **Slow processing:** ElGamal is slower compared to other encryption algorithms, especially when used with long keys. This can make it impractical for certain applications that require fast processing speeds.

- **Key size:** ElGamal requires larger key sizes to achieve the same level of security as other algorithms. This can make it more difficult to use in some applications.

- **Vulnerability to certain attacks:** ElGamal is vulnerable to attacks based on the discrete logarithm problem, such as the index calculus algorithm. This can reduce the security of the algorithm in certain situations.

Digital Signature

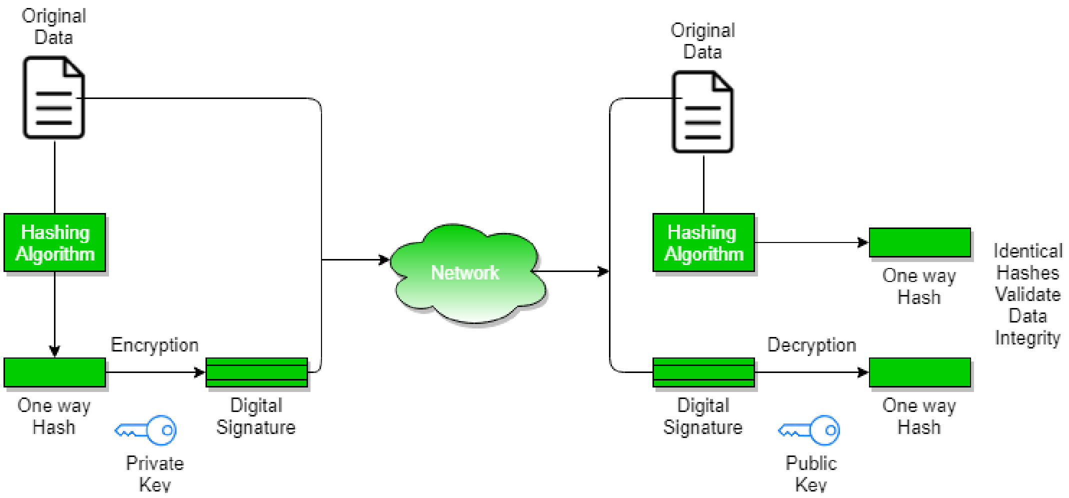
A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document.

1. **Key Generation Algorithms**: Digital signature is electronic signatures, which assure that the message was sent by a particular sender. While performing digital transactions authenticity and integrity should be assured, otherwise, the data can be altered or someone can also act as if he was the sender and expect a reply.
2. **Signing Algorithms**: To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier. The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed-length value. This saves time as now instead of signing a long message a shorter hash value has to be signed and moreover hashing is much faster than signing.
3. **Signature Verification Algorithms** : Verifier receives Digital Signature along with the data. It then uses Verification algorithm to process on the digital signature and the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. Then the hash value and the output of the verification algorithm are compared. If they both are equal, then the digital signature is valid else it is invalid.

The steps followed in creating digital signature are :

1. Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).
2. Digital signature is then transmitted with the message.(message + digital signature is transmitted)
3. Receiver decrypts the digital signature using the public key of sender.(This assures authenticity, as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender’s public key).
4. The receiver now has the message digest.
5. The receiver can compute the message digest from the message (actual message is sent with the digital signature).
6. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.

Message digest is computed using one-way hash function, i.e. a hash function in which computation of hash value of a message is easy but computation of the message from hash value of the message is very difficult.



Benefits of Digital Signatures

- **Legal documents and contracts:** Digital signatures are legally binding. This makes them ideal for any legal document that requires a signature authenticated by one or more parties and guarantees that the record has not been altered.
- **Sales contracts:** Digital signing of contracts and sales contracts authenticates the identity of the seller and the buyer, and both parties can be sure that the signatures are legally binding and that the terms of the agreement have not been changed.
- **Financial Documents:** Finance departments digitally sign invoices so customers can trust that the payment request is from the right seller, not from a bad actor trying to trick the buyer into sending payments to a fraudulent account.
- **Health Data:** In the healthcare industry, privacy is paramount for both patient records and research data. Digital signatures ensure that this confidential information was not modified when it was transmitted between the consenting parties.
- Federal, state, and local government agencies have stricter policies and regulations than many private sector companies. From approving permits to stamping them on a timesheet, digital signatures can optimize productivity by ensuring the right person is involved with the proper approvals.
- **Shipping Documents:** Helps manufacturers avoid costly shipping errors by ensuring cargo manifests or bills of lading are always correct. However, physical papers are cumbersome, not always easily accessible during transport, and can be lost. By digitally signing shipping documents, the sender and recipient can quickly access a file, check that the signature is up to date, and ensure that no tampering has occurred.

Digital Certificate

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.

A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or an entity.

Digital certificate contains:- The authenticity

1. Name of certificate holder.
2. Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate
3. Expiration dates.
4. Copy of certificate holder's public key.(used for decrypting messages and digital signatures)
5. Digital Signature of the certificate issuing authority.

What is the Digital Signature Standard (DSS)?

The Digital Signature Standard (DSS) is a digital signature algorithm developed by the U.S. National Security Agency as a means of authentication for electronic documents.

A digital signature is equivalent to a written signature used to sign documents and provide physical authentication.

After its creation, DSS was published by the National Institute of Standards and Technology in 1994. It has since become the United States government standard for authentication of electronic documents.

DSS is also specified as a verified means for authentication in Federal Information Processing Standards (FIPS) 186.

There have been four revisions to the FIPS 186 DSS specification since 1994:

1. FIPS 186-1 in 1996
2. FIPS 186-2 in 2000
3. FIPS 186-3 in 2009
4. FIPS 186-4 in 2013

Digital Signature Algorithms (DSA):- **The need for privacy and secrecy applies to every organization and individual in personal and official matters. Plans and programs will only succeed if confidentiality is maintained. In the digital world, with millions of messages exchanged daily, it is also necessary to observe privacy. Sensitive websites that deal with Banking and E-commerce, for instance, require greater secrecy.**

Recounting the DSA Steps

- Using the key generation algorithm, the keys are used to sign the message.
- The digital signature algorithm provides the signature.
- The hash is used for making the message digest.
- Combining DSA and the message digest results in the digital signature.
- The digital signature accompanies the transmitted message.
- Verification algorithms help to confirm the validity, and the same hash function is used.

DSA Disadvantages

US National Standard follows the DSA that applies in private and non-private messages, but some weaknesses exist along with major advantages.

Types of Authentication Protocols

When we develop software, our first and most important priority is user authentication. To authenticate the user there are several mechanisms by which we can authenticate the data that are given by the user. In this article, we are going to learn the most common types of the authentication protocol and their advantages and disadvantages.

Why is user authentication important?

Requiring users to provide and prove their identity adds a layer of security between adversaries and sensitive data. With authentication, IT teams can employ the least privileged access to limit what employees can see. The average employee, for example, doesn't need access to company financials, and accounts payable doesn't need to touch developer projects. When selecting an authentication type, companies must consider UX along with security. Some user authentication types are less secure than others, but too much friction during authentication can lead to poor employee practices.

1. Kerberos

Kerberos is a type of protocol that is used to authenticate users. It validates the client and server during networking with the help of a cryptographic key. It is designed to strongly authenticate the users during the reporting of the application. All the proposals of Kerberos are available at MIT. The main use of the Kerberos is in the product-based companies.

Advantages

1. The various operating systems are supported by the Kerberos.
2. In Kerberos, the authentication key is shared very efficiently in comparison to public sharing.

Disadvantages

1. The client and service can only authenticate themselves with the help of Kerberos.
2. When we use a soft or weak password, it always shows vulnerability.

2. Lightweight Directory Access Protocol(LDAP)

LDAP stands for Lightweight Directory Access Protocol. With the help of this protocol, we can determine the organization, individual, or any other devices during the networking over the internet. It is also called a Directory as a service. Lightweight Directory Access Protocol (LDAP) is the ground for Microsoft Building Activity Directory.

Advantages for Lightweight Directory Access Protocol (LDAP)

1. It is a type of automated protocol that is why it is very easier for the organization.
2. All the existing software is supported by Lightweight Directory Access Protocol (LDAP).
3. Multiple directories can be allowed in Lightweight Directory Access Protocol(LDAP)

Some disadvantages of LDAP

1. It requires the experience of deployment.
2. The directory servers are required to be LDAP-obedient for deployment.

3. OAuth2

OAuth2 is a type of authentication protocol for the framework. It provides permission to the users which are coming through the HTTP servers. When the user makes a request to access the resources, suddenly, an API call is created, and after that, the authentication token is generated.

Advantages of OAuth2

1. It is a very simple type of authentication protocol, and it is very easy to use.

2. It provides the code for server-side authentication.

Disadvantages for OAuth2

1. It is a little bit difficult to manage the different sets of codes.
2. When we connect it to an affected system, it also shows some serious effects.

4. SAML

SAML stands for **Security Assertion Markup Language**. It is based on an XML-based authentication protocol. It provides authorization between the service provider and the identity provider. It is also a product of the OASIS Security Service Technical Committee.

Advantages of SAML

1. The administrative cost is reduced for the end user with the help of SAML (Security Assertion Markup Language).
2. It provides a single window for authentication for all the services.

Disadvantages of SAML

1. It is fully dependent on the identity provider.
2. A single XML format manages all the data.

5. RADIUS

RADIUS stands for **Remote Authentication Dial-In User Service**. It is a type of network protocol that provides accounting, centralized authentication, and authorization. When the user makes a request to access all the resources, the RADIUS server creates a temporary credential to access all the resources. After this, the temporary credential is saved on the local database and provides access to the user.

Advantages of RADIUS

1. It has a feature to provide multiple accesses to the admin.
2. It also provides a unique id for every session of the user.

The disadvantage of RADIUS

1. The mechanism for initial implementation is very hard on hardware.
2. It has a variety of models that may require a special team which is cost-consuming.

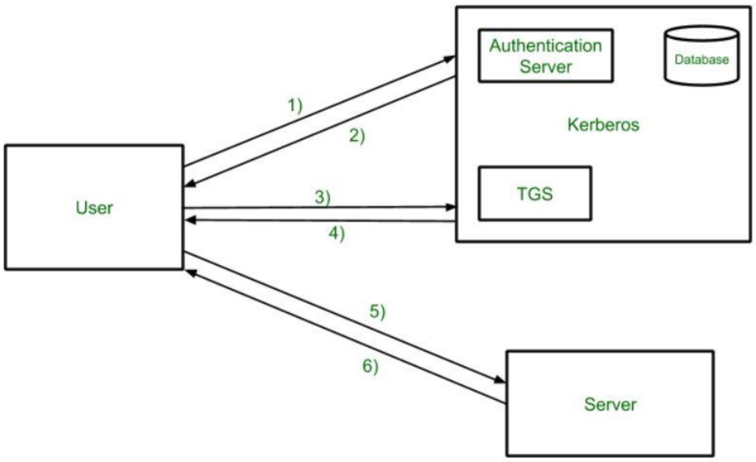
Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. In Kerberos Authentication server and database is used for client authentication. Kerberos runs as a third-party trusted server known as the Key Distribution Center (KDC). Each user and service on the network is a principal.
The main components of Kerberos are:

- **Authentication Server (AS):**
  The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.

- **Database:**
  The Authentication Server verifies the access rights of users in the database.

- **Ticket Granting Server (TGS):**
  The Ticket Granting Server issues the ticket for the Server

Kerberos Overview:



- **Step-1:**
  User login and request services on the host. Thus user requests for ticket-granting service.

- **Step-2:**
  Authentication Server verifies user’s access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using the Password of the user.

- **Step-3:**
  The decryption of the message is done using the password then send the ticket to Ticket Granting Server. The Ticket contains authenticators like user names and network

addresses.

- **Step-4:**
  Ticket Granting Server decrypts the ticket sent by User and authenticator verifies the request then creates the ticket for requesting services from the Server.

- **Step-5:**
  The user sends the Ticket and Authenticator to the Server.

- **Step-6:**
  The server verifies the Ticket and authenticators then generate access to the service. After this User can access the services.

Kerberos Limitations

- Each network service must be modified individually for use with Kerberos
- It doesn't work well in a timeshare environment
- Secured Kerberos Server
- Requires an always-on Kerberos server
- Stores all passwords are encrypted with a single key
- Assumes workstations are secure
- May result in cascading loss of trust.
- Scalability

Applications

- **User Authentication**: User Authentication is one of the main applications of Kerberos. Users only have to input their username and password once with Kerberos to gain access to the network. The Kerberos server subsequently receives the encrypted authentication data and issues a ticket granting ticket (TGT).
- **Single Sign-On (SSO)**: Kerberos offers a Single Sign-On (SSO) solution that enables users to log in once to access a variety of network resources. A user can access any network resource they have been authorized to use after being authenticated by the Kerberos server without having to provide their credentials again.
- **Mutual Authentication**: Before any data is transferred, Kerberos uses a mutual authentication technique to make sure that both the client and server are authenticated. Using a shared secret key that is securely kept on both the client and server, this is accomplished. A client asks the Kerberos server for a service ticket whenever it tries to access a network resource. The client must use its shared secret key to decrypt the challenge that the Kerberos server sends via encryption. If the decryption is successful, the client responds to the server with evidence of its identity.
- **Authorization**: Kerberos also offers a system for authorization in addition to authentication. After being authenticated, a user can submit service tickets for certain network resources. Users can access just the resources they have been given permission to use thanks to information about their privileges and permissions contained in the service tickets.

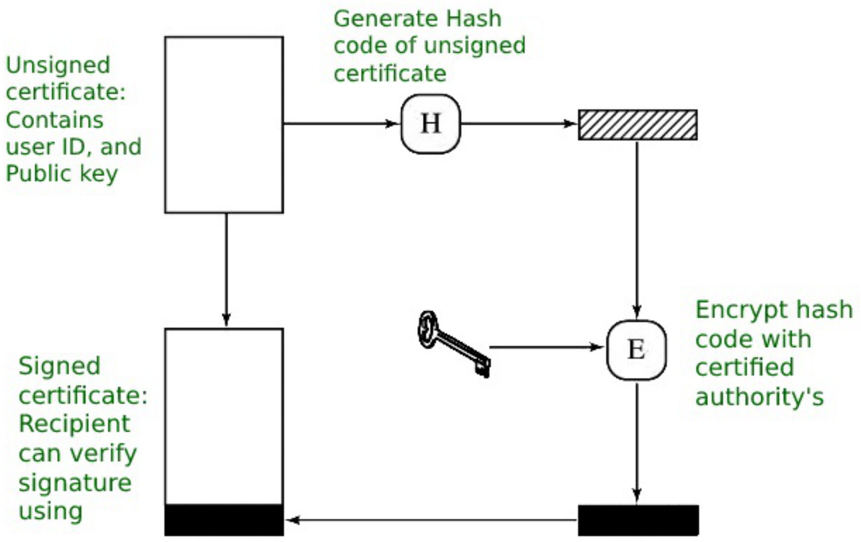
- **Network Security**: Kerberos offers a central authentication server that can regulate user credentials and access restrictions, which helps to ensure network security. In order to prevent unwanted access to sensitive data and resources, this server may authenticate users before granting them access to network resources.

X.509 Authentication Service:- X.509 is a digital certificate that is built on top of a widely trusted standard known as ITU or International Telecommunication Union X.509 standard, in which the format of PKI certificates is defined. X.509 digital certificate is a certificate-based authentication security framework that can be used for providing secure transaction processing and private information. These are primarily used for handling the security and identity in computer networking and internet-based communications.

Working of X.509 Authentication Service Certificate:

The core of the X.509 authentication service is the public key certificate connected to each user. These user certificates are assumed to be produced by some trusted certification authority and positioned in the directory by the user or the certified authority. These directory servers are only used for providing an effortless reachable location for all users so that they can acquire certificates. X.509 standard is built on an IDL known as ASN.1. With the help of Abstract Syntax Notation, the X.509 certificate format uses an associated public and private key pair for encrypting and decrypting a message.

Once an X.509 certificate is provided to a user by the certified authority, that certificate is attached to it like an identity card. The chances of someone stealing it or losing it are less, unlike other unsecured passwords. With the help of this analogy, it is easier to imagine how this authentication works: the certificate is basically presented like an identity at the resource that requires authentication.


Generate Hash code of unsigned certificate
Unsigned certificate: Contains user ID, and Public key
H
Encrypt hash code with certified authority's
E
Signed certificate: Recipient can verify signature using

, the certificate includes the elements given below:

- **Version number:** It defines the X.509 version that concerns the certificate.
- **Serial number:** It is the unique number that the certified authority issues.
- **Signature Algorithm Identifier:** This is the algorithm that is used for signing the certificate.
- **Issuer name:** Tells about the X.500 name of the certified authority which signed and created the certificate.
- **Period of Validity:** It defines the period for which the certificate is valid.
- **Subject Name:** Tells about the name of the user to whom this certificate has been issued.
- **Subject's public key information:** It defines the subject's public key along with an identifier of the algorithm for which this key is supposed to be used.
- **Extension block:** This field contains additional standard information.
- **Signature:** This field contains the hash code of all other fields which is encrypted by the certified authority private key.

Applications of X.509 Authentication Service Certificate:

Many protocols depend on X.509 and it has many applications, some of them are given below:

- Document signing and Digital signature
- Web server security with the help of Transport Layer Security (TLS)/Secure Sockets Layer (SSL) certificates
- Email certificates
- Code signing
- Secure Shell Protocol (SSH) keys
- Digital Identities

UNIT-6

Introduction to Internet Security Protocols

In today's computer network world, internet security has achieved great importance. Since internet technology is vast and encompasses many years, there are various aspects associated with internet security. Various security mechanisms exist for specialized internet services like email, electronic commerce, and payment, wireless internet, etc. To provide the security to this internet various protocols have been used like SSL (Secure Socket Layer), TLS (Transport Layer Security), etc.

Various Internet Security Protocols

Given below are the various protocols:

1. SSL Protocol

SSL Protocol stands for Secure Socket Layer protocol, which is an internet security protocol used for exchanging the information between a web browser and a web server in a secure manner. It provides two basic security services like authentication and confidentiality. SSL protocol has become the world's most popular web security mechanism, all major web browsers support SSL. Secure socket layer protocol is considered as an additional layer in TCP/IP protocol suite. It is located between the application layer and the transport layer. SSL has three sub protocols namely Handshake Protocol, Record Protocol, and Alert Protocol.

OpenSSL is an open source implementation of the Secure Socket Layer protocol. OpenSSL is subject to four remotely exploitable buffer overflow. Buffer overflow vulnerabilities allow attackers to execute arbitrary code on the target computer with a privilege level of OpenSSL process as well as providing opportunities for launching a denial of service attack.

2. TLS Protocol

TLS stands for Transport Layer Security, which is an internet security protocol. TLS is an IETF standardization initiative whose goal is to come out with an internet standard version of SSL. To standardized SSL, Netscape handed the protocol to IETF. The idea and implementation are quite similar. Transport layer security protocol uses a pseudo random function to create a master secret. TLS also has three sub protocols same as SSL protocol – Handshake Protocol, Record Protocol, and Alert Protocol. In Handshake Protocol some details are changed, Record Protocol uses HMAC, Alert protocol newly added features like record overflow, Unknown CA, Decryption failed, Decode error, Access denied, Export restrictions, Protocol version, insufficient security, internal error. Transport layer security is defined in RFC 2246.

3. SHTTP

SHTTP stands for Secure HyperText Transfer Protocol, is a set of security mechanism defined for protecting internet traffic. It also includes data entry forms and internet based transaction. Services provided by SHTTP are quite similar to SSL protocol. Secure HyperText Transfer Protocol works at the application layer, and therefore tightly coupled with HTTP. SHTTP supports both authentication and encryption of HTTP traffic between the client and the server. Encryption and digital signature format used in SHTTP have the origins in the PEM (Privacy Enhanced Mail) protocol. SHTTP works at the level of an individual message. It can encrypt and sign an individual message.

4. SET Protocol

SET Protocol stands for Secure Electronic Transaction protocol is an open encryption and security mechanism designed for protecting the eCommerce transaction over the internet. SET is not a payment system, it is a security protocol used over the internet for secure transaction.

The SET protocol provides the following services:

- SET provides authentication by using digital certificates.
- It provides a secure communication channel among all parties involved in an eCommerce transaction.
- It ensures confidentiality because the information is only available for parties involved in a transaction and that too only when and where required.

The SET protocol includes the following participants:

- **Cardholder:** It is an authorized holder of payment card such as visa card, Master card.
- **Merchant:** It is a specific person or organization who wants to sell goods and services to the cardholder.
- **Issuer:** It is a financial institution which provides payment card to the cardholder.
- **Acquirer:** It is a financial institution which has a relationship with merchants for processing payment card Authorization and payments.
- **Payment Gateway:** It acts as an interface between SET and existing card payment networks for payment Authorization.
- **Certification Authority:** It is an authority that is trusted to provide a public key certificate to cardholder, merchant, and payment gateways.

5. PEM Protocol

PEM Protocol stands for privacy enhanced mail, used for email security over the internet. If we adopted by IAB (Internet Architecture Board) to provide secure electronic mail communication over the internet. It was initially developed by the IRTF (Internet Research Task Force) PSRG (Privacy Security Research Group). Then they handed over the PEM to the IETF (Internet Engineering Task Force) PEM working group Privacy Enhanced Mail protocol is described in four specific documents RFC 1421, RFC 1422, RFC 1423, and RFC 1424. It supports cryptographic functions namely encryption, nonrepudiation, and message integrity.

6. PGP Protocol

PGP Protocol stands for Pretty Good Privacy, which we developed by Phil Zimmerman. PGP protocol is easy to use and free including its source code documentation. It also supports the basic requirements of cryptography. However, for those organizations that require support, a low-cost commercial version Of PGP protocol is available from an organization called viacrypt. PGP protocol becomes extremely popular and more widely used as compared to PEM protocol. PGP protocol support cryptography like encryption, Non-repudiation, and message integrity.

What is Email Security:

Email (short for electronic mail) is a digital method by using it we exchange messages between people over the internet or other computer networks. With the help of this, we can send and receive text-based messages, often an attachment such as documents, images, or videos, from one person or organization to another.

It was one of the first applications developed for the internet and has since become one of the most widely used forms of digital communication. It has an essential part of personal and professional communication, as well as in marketing, advertising, and customer support.
In this article, we will understand the concept of **email security**, how we can protect our email, email security policies, and email security best practices, and one of the features of email is an email that we can use to protect the email from unauthorized access.

Email Security:

Basically**, Email security** refers to the steps where we protect the email messages and the information that they contain from unauthorized access, and damage. It involves ensuring the confidentiality, integrity, and availability of email messages, as well as safeguarding against phishing attacks, spam, viruses, and another form of malware. It can be achieved through a combination of technical and non-technical measures.

Some standard technical measures include the encryption of email messages to protect their contents, the use of digital signatures to verify the authenticity of the sender, and email filtering systems to block unwanted emails and malware, and the non-technical measures may include training employees on how to recognize and respond to phishing attacks and other email security threats, establishing policies and procedures for email use and management, and conducting regular security audits to identify and address vulnerabilities.

We can say that email security is important to protect sensitive information from unauthorized access and ensure the reliability and confidentiality of electronic communication.

Steps to Secure Email:

We can take the following actions to protect our email.

- Choose a secure password that is at least 12 characters long, and contains uppercase and lowercase letters, digits, and special characters.
- Activate the two-factor authentication, which adds an additional layer of security to your email account by requiring a code in addition to your password.
- Use encryption, it encrypts your email messages so that only the intended receiver can decipher them. Email encryption can be done by using the programs like PGP or S/MIME.
- Keep your software up to date. Ensure that the most recent security updates are installed on your operating system and email client.
- **Beware of phishing scams:** Hackers try to steal your personal information by pretending as someone else in phishing scams. Be careful of emails that request private information or have suspicious links because these are the resources of the phishing attack.
- **Choose a trustworthy email service provider:** Search for a service provider that protects your data using encryption and other security measures.
- **Use a VPN:** Using a VPN can help protect our email by encrypting our internet connection and disguising our IP address, making it more difficult for hackers to intercept our emails.
- **Upgrade Your Application Regularly:** People now frequently access their email accounts through apps, although these tools are not perfect and can be taken advantage of by hackers. A cybercriminal might use a vulnerability, for example, to hack accounts and steal data or send spam mail. Because of this, it’s important to update your programs frequently.

Email Security Policies

The email policies are a set of regulations and standards for protecting the privacy, accuracy, and accessibility of email communication within the organization. An email security policy should include the following essential components:

- **Appropriate Use:** The policy should outline what comprises acceptable email usage inside the organization, including who is permitted to use email, how to use it, and for what purpose email we have to use.
- **Password and Authentication:** The policy should require strong passwords and two-factor authentication to ensure that only authorized users can access email accounts.
- **Encryption**: To avoid unwanted access, the policy should mandate that sensitive material be encrypted before being sent through email.

- **Virus Protection: T**he policy shall outline the period and timing of email messages and attachment collection.
- **Retention and Detection**: The policy should outline how long email messages and their attachments ought to be kept available, as well as when they should continue to be removed.
- **Training**: The policy should demand that all staff members take a course on email best practices, which includes how to identify phishing scams and other email-based threats.
- **Incident Reporting**: The policy should outline the reporting and investigation procedures for occurrences involving email security breaches or other problems.
- **Monitoring**: The policy should outline the procedures for monitoring email communications to ensure that it is being followed, including any logging or auditing that will be carried out.
- **Compliance**: The policy should ensure compliance with all essential laws and regulations, including the health
- Insurance rules, including the health portability and accountability act and the General Data Protection Regulation (GDPR)(HIPPA).
- **Enforcement:** The policy should specify the consequences for violating the email security policy, including disciplinary action and legal consequences if necessary.

Hence, organizations may help safeguard sensitive information and lower the risk of data breaches and other security incidents by creating an email security strategy.

Now, Let's look at how to enable the confidential mode in our Gmail account. With Gmail.com, there is a feature called confidential mode that we may use to safeguard our email.These are the steps to use this feature:

Step 1: On your computer, go to Gmail and click compose as shown in the below screenshot.

Step 2: If you have already enabled confidential mode for an email, click Edit in the bottom right corner of the window to add an expiration date and a passcode. These setting impact both the message text and any attachments.

If you select "No SMS passcode," recipients using the Gmail app will be able to open it directly and those who don't use Gmail will receive an email with a passcode.

On the other hand, if you select the "SMS passcode" recipients will get a passcode by a text message for that you have to provide the recipient's phone number.

Step 3: After providing the phone number click the save button.
Step 4: In the next step write the email and sent it to the recipient.

Advantages of email:

1. Convenient and fast communication with individuals or groups globally.
2. Easy to store and search for past messages.
3. Ability to send and receive attachments such as documents, images, and videos.
4. Cost-effective compared to traditional mail and fax.
5. Available 24/7.

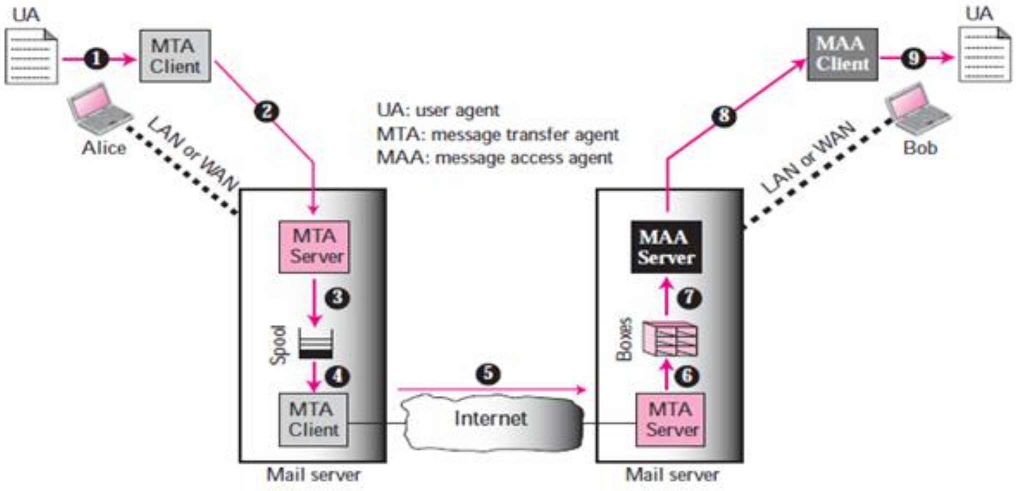
Disadvantages of email:

1. Risk of spam and phishing attacks.
2. Overwhelming amount of emails can lead to information overload.
3. Can lead to decreased face-to-face communication and loss of personal touch.
4. Potential for miscommunication due to lack of tone and body language in written messages.
5. Technical issues, such as server outages, can disrupt email service.
6. It is important to use email responsibly and effectively, for example, by keeping the subject line clear and concise, using proper etiquette, and protecting against security threats.

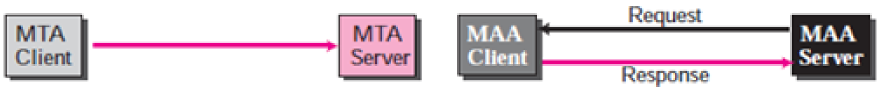
Email Architecture:

Email architecture consists of three components:

- **User Agent (UA)**
- **Message Transfer Agent (MTA)**
- **Message Access Agent (MAA)**



Push vs. pull



User Agent:

A user agent is a Package “or in simple words a program” of a software that composes, Reads, Responds to, and forward messages. It also handles user computers with local mailboxes.

Sending Mail:

In order to send a mail, the user creates mail through the UA which looks very similar to Postal Mail.

Receiving Mail:

The User agent, or a timer, is triggered by the User. Where a user has mail, the UA will notify the user with a notice if the user is ready to read the mail, a list will be shown in which each line includes a description of a particular message's mailbox information.

Addresses:

A mail handling system must use a system address with unique addresses to deliver mails. Each user has a unique email address which is selected the time a person sign up for an email ID.

Mailing List or Group List:

Electronic mail allows for the one name, an alias, to represent several different email addresses; this is called a mailing list. The system checks the name of the recipient against the alias database whenever a message is to be sent; if there is a mailing list for the defined alias, separate messages, one for each entry in the list, must be prepared and given to the MTA.

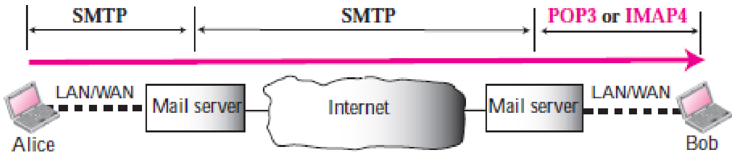
Mail Transfer Agent "MTA":

The actual mail transmission is done through MTAs. A system must have the client MTA for sending mail, and a system must have a server MTA for receiving mail. Simple Mail Transfer Protocol "SMTP" is the formal protocol that defines the MTA client and server within the internet.

Message Access Agent "MAA":

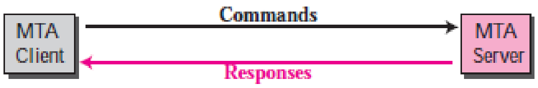
SMTP is used in the first and second phases of mail deliver. SMTP is not involved in the third stage, however, as SMTP is a push protocol; it transmits the client's message to the server. The path of the bulk data "messages" is from client to server, in other words. On the other hand, a pull protocol is required to the third stage. The client must use the server to pull messages. The direction from the server to the client for the bulk data is the third stage that uses an agent for accessing messages. There are currently two protocols for accessing messages.

Post Office Protocol version 3 “POP3” and Internet Mail Access Protocol “IMAP”.



Simple Mail Transfer Protocol (SMTP):

SMTP is used two times, between the sender and the sender’s mail server and between the two mail servers. SMTP simply defines how commands and responses must be sent back and forth between an MTA client and an MTA server.



MIME Protocol

MIME stands for Multipurpose Internet Mail Extensions. It is used to extend the capabilities of Internet e-mail protocols such as SMTP. The MIME protocol allows the users to exchange various types of digital content such as pictures, audio, video, and various types of documents and files in the e-mail. MIME was created in 1991 by a computer scientist named Nathan Borenstein at a company called Bell Communications.

MIME is an e-mail extension protocol, i.e., it does not operate independently, but it helps to extend the capabilities of e-mail in collaboration with other protocols such as SMTP. Since MIME was able to transfer only text written file in a limited size English language with the help of the internet. At present, it is used by almost all e-mail related service companies such as Gmail, Yahoo-mail, Hotmail.

Need of MIME Protocol

MIME protocol is used to transfer e-mail in the computer network for the following reasons:

1. The MIME protocol supports multiple languages in e-mail, such as Hindi, French, Japanese, Chinese, etc.
2. Simple protocols can reject mail that exceeds a certain size, but there is no word limit in MIME.

3. Images, audio, and video cannot be sent using simple e-mail protocols such as SMTP. These require MIME protocol.
4. Many times, emails are designed using code such as HTML and CSS, they are mainly used by companies for marketing their product. This type of code uses MIME to send email created from HTML and CSS.

MIME Header

MIME adds five additional fields to the header portion of the actual e-mail to extend the properties of the simple email protocol. These fields are as follows:

1. MIME Version
2. Content Type
3. Content Type Encoding
4. Content Id
5. Content description

1. MIME Version

It defines the version of the MIME protocol. This header usually has a parameter value 1.0, indicating that the message is formatted using MIME.

2. Content Type

It describes the type and subtype of information to be sent in the message. These messages can be of many types such as Text, Image, Audio, Video, and they also have many subtypes such that the subtype of the image can be png or jpeg. Similarly, the subtype of Video can be WEBM, MP4 etc.

3. Content Type Encoding

In this field, it is told which method has been used to convert mail information into ASCII or Binary number, such as 7-bit encoding, 8-bit encoding, etc.

4. Content Id

In this field, a unique "Content Id" number is appended to all email messages so that they can be uniquely identified.

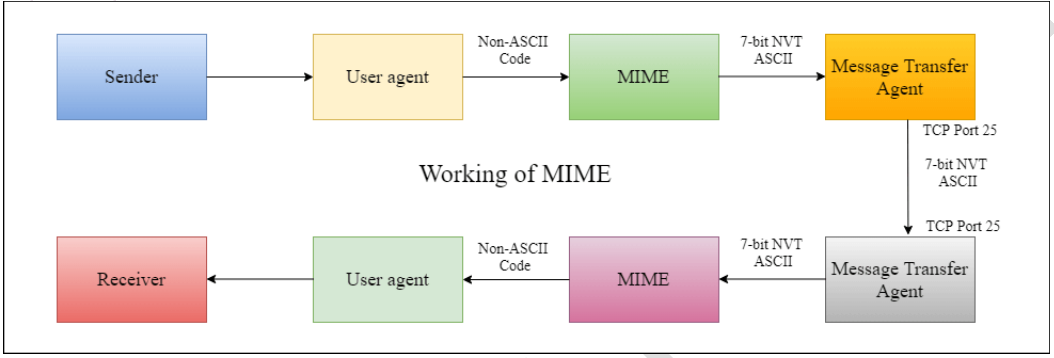
5. Content description

This field contains a brief description of the content within the email. This means that information about whatever is being sent in the mail is clearly in the "Content Description". This field also provides the information of name, creation date, and modification date of the file.

Example of Content description

```
Content-Description: attachment; filename = javatpoint.jpeg;
modification-date = "Wed, 12 Feb 1997 16:29:51 -0500";
```

Working diagram of MIME Protocol



Features of MIME Protocol

1. It supports multiple attachments in a single e-mail.
2. It supports the non-ASCII characters.
3. It supports unlimited e-mail length.
4. It supports multiple languages.

Advantage of the MIME

The MIME protocol has the following advantages:

1. It is capable of sending various types of files in a message, such as text, audio, video files.
2. It also provides the facility to send and receive emails in different languages like Hindi, French, Japanese, Chinese etc.
3. It also provides the facility of connecting HTML and CSS to email, due to which people can design email as per their requirement and make it attractive and beautiful.
4. It is capable of sending the information contained in an email regardless of its length.
5. It assigns a unique id to all e-mails.

IP address:- **A series of integers with periods in between make up an IP address. An example IP address would be** 192.158.1.38**. IP addresses are represented as a series of four integers. Each integer in the set has a 0 to 255 possible range. 0.0.0.0 to** 255.255.255.255 **is the whole IP addressing range.**

An IP address is the identifier that enables your device to send or receive data packets across the internet. It holds information related to your location and therefore making devices available for two-way communication. The internet requires a process to distinguish between different networks, routers, and websites. Therefore, IP addresses provide the mechanism of doing so, and it forms an indispensable part in the working of the internet. You will notice that most of the IP addresses are essentially numerical. Still, as the world is witnessing a colossal growth of network users, the network developers had to add letters and some addresses as internet usage grows.

An IP address is represented by a series of numbers segregated by periods(.). They are expressed in the form of four pairs - an example address might be 255.255.255.255 wherein each set can range from 0 to 255.

IP addresses are not produced randomly. They are generated mathematically and are further assigned by the IANA (Internet Assigned Numbers Authority), a department of the ICANN.

ICANN stands for Internet Corporation for Assigned Names and Numbers. It is a non-profit corporation founded in the US back in 1998 with an aim to manage Internet security and enable it to be available by all.

How do IP addresses work?

Sometimes your device doesn't connect to your network the way you expect it to be, or you wish to troubleshoot why your network is not operating correctly. To answer the above questions, it is vital to learn the process with which IP addresses work.

Internet Protocol or IP runs the same manner as other languages, i.e., applying the set guidelines to communicate the information. All devices obtain, send, and pass information with other associated devices with the help of this protocol only. By using the same language, the computers placed anywhere can communicate with one another.

The process of IP address works in the following way:

1. Your computer, smartphone, or any other Wi-Fi-enabled device firstly connects to a network that is further connected to the internet. The network is responsible for giving your device access to the internet.

2. While working from home, your device would be probably using that network provided by your Internet Service Provider (ISP). In a professional environment, your device uses your company network.
3. Your ISP is responsible to generate the IP address for your device.
4. Your internet request penetrates through the ISP, and they place the requested data back to your device using your IP address. Since they provide you access to the internet, ISP's are responsible for allocating an IP address to your computer or respective device.
5. Your IP address is never consistent and can change if there occurs any changes in its internal environment. For instance, if you turn your modem or router on or off, it will change your IP address. Or the user can also connect the ISP to change their IP address.
6. When you are out of your home or office, mainly if you travel and carry your device with you, your computer won't be accessing your home IP address anymore. This is because you will be accessing the different networks (your phone hotspot, Wi-Fi at a cafe, resort, or airport, etc.) to connect the device with the internet. Therefore, your device will be allocated a different (temporary) IP address by the ISP of the hotel or cafe.

Types of IP addresses

There are various classifications of IP addresses, and each category further contains some types.

Consumer IP addresses

Every individual or firm with an active internet service system pursues two types of IP addresses, i.e., Private IP (Internet Protocol) addresses and public IP (Internet Protocol) addresses. The public and private correlate to the network area. Therefore, a private IP address is practiced inside a network, whereas the other (public IP address) is practiced outside a network.

1. Private IP addresses

All the devices that are linked with your internet network are allocated a private IP address. It holds computers, desktops, laptops, smartphones, tablets, or even Wi-Fi-enabled gadgets such as speakers, printers, or smart Televisions. With the expansion of IoT (internet of things), the demand for private IP addresses at individual homes is also seemingly growing. However, the router requires a method to identify these things distinctly. Therefore, your router produces unique private IP addresses that act as an identifier for every device using your internet network. Thus, differentiating them from one another on the network.

2. Public IP addresses

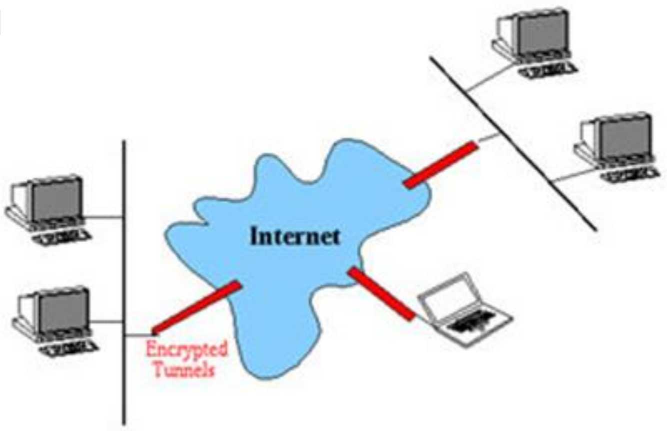
A public IP address or primary address represents the whole network of devices associated with it. Every device included within with your primary address contains their own private IP address. ISP is responsible to provide your public IP address to your router. Typically, ISPs contains the bulk stock of IP addresses that they dispense to their clients. Your public IP address is practiced by every device to identify your network that is residing outside your internet network.

Public IP addresses are further classified into two categories- dynamic and static.

- **Dynamic IP addresses**
  As the name suggests, Dynamic IP addresses change automatically and frequently. With this types of IP address, ISPs already purchase a bulk stock of IP addresses and allocate them in some order to their customers. Periodically, they re-allocate the IP addresses and place the used ones back into the IP addresses pool so they can be used later for another client. The foundation for this method is to make cost savings profits for the ISP.
- **Static IP addresses**
  In comparison to dynamic IP addresses, static addresses are constant in nature. The network assigns the IP address to the device only once and, it remains consistent. Though most firms or individuals do not prefer to have a static IP address, it is essential to have a static IP address for an organization that wants to host its network server. It protects websites and email addresses linked with it with a constant IP address.

VPN: Virtual Private Network

VPN stands for Virtual Private Network. It refers to a safe and encrypted network that allows you to use network resources in a remote manner. Using VPN, you can create a safe connection over a less secure network, e.g. internet. It is a secure network as it is completely isolated from rest of the internet. The government, businesses, military can use this network to use network resources securely.



VPN is free to use and it uses site-to-site and remote access methods to work. It uses an arrangement of encryption services to establish a secure connection. It is an ideal tool for encryption; it provides you strong AES256 encryption with an 8192bit key.

How VPN Works?

VPN works by creating a secure tunnel using powerful VPN protocols. It hides your IP address behind its own IP address that encrypts all your communication. Thus, your communication passes through a secure tunnel that allows you use network resources freely and secretly.

VPN protocols

There are several different VPN protocols that are used to create secure networks. Some of such protocols are given below.

- IP security (IPsec)
- Point to Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

What is TLS?

TLS is a cryptographic protocol that provides end-to-end security of data sent between applications over the Internet. It is mostly familiar to users through its use in secure web browsing, and in particular the padlock icon that appears in web browsers when a secure session is established. However, it can and indeed should also be used for other applications such as e-mail, file transfers, video/audioconferencing, instant messaging and voice-over-IP, as well as Internet services such as DNS and NTP.

TLS evolved from Secure Socket Layers (SSL) which was originally developed by Netscape Communications Corporation in 1994 to secure web sessions. SSL 1.0 was never publicly released, whilst SSL 2.0 was quickly replaced by SSL 3.0 on which TLS is based.

UNIT-7

System Security

Every computer system and software design must handle all security risks and implement the necessary measures to enforce security policies. At the same time, it's critical to strike a balance because strong security measures might increase costs while also limiting the system's usability, utility, and smooth operation. As a result, system designers must assure efficient performance without compromising security.

In this article, you will learn about operating system security with its issues and other features.

What is Operating System Security?

The process of ensuring OS availability, confidentiality, integrity is known as operating system security. OS security refers to the processes or measures taken to protect the operating system from dangers, including viruses, worms, malware, and remote hacker intrusions. Operating system security comprises all preventive-control procedures that protect any system assets that could be stolen, modified, or deleted if OS security is breached.

Security refers to providing safety for computer system resources like software, CPU, memory, disks, etc. It can protect against all threats, including viruses and unauthorized access. It can be enforced by assuring the operating system's **integrity, confidentiality**, and **availability**. If an illegal user runs a computer application, the computer or data stored may be seriously damaged.

System security may be threatened through two violations, and these are as follows:

1. Threat

A program that has the potential to harm the system seriously.

2. Attack

A breach of security that allows unauthorized access to a resource.

There are two types of security breaches that can harm the system: malicious and accidental. Malicious threats are a type of destructive computer code or web script that is designed to cause system vulnerabilities that lead to back doors and security breaches. On the other hand, Accidental Threats are comparatively easier to protect against.

Security may be compromised through the breaches. Some of the breaches are as follows:

1. Breach of integrity

This violation has unauthorized data modification.

2. Theft of service

It involves the unauthorized use of resources.

3. Breach of confidentiality

It involves the unauthorized reading of data.

4. Breach of availability

It involves the unauthorized destruction of data.

5. Denial of service

It includes preventing legitimate use of the system. Some attacks may be accidental.

The goal of Security System

There are several goals of system security. Some of them are as follows:

1. Integrity

Unauthorized users must not be allowed to access the system's objects, and users with insufficient rights should not modify the system's critical files and resources.

2. Secrecy

The system's objects must only be available to a small number of authorized users. The system files should not be accessible to everyone.

3. Availability

All system resources must be accessible to all authorized users, i.e., no single user/process should be able to consume all system resources. If such a situation arises, service denial may occur. In this case, malware may restrict system resources and preventing legitimate processes from accessing them.

Types of Threats

There are mainly two types of threats that occur. These are as follows:

Program threats

The operating system's processes and kernel carry out the specified task as directed. Program Threats occur when a user program causes these processes to do malicious operations. The common example of a program threat is that when a program is installed on a computer, it could store and transfer user credentials to a hacker. There are various program threats. Some of them are as follows:

1.Virus

A virus may replicate itself on the system. Viruses are extremely dangerous and can modify/delete user files as well as crash computers. A virus is a little piece of code that is implemented on the system program. As the user interacts with the program, the virus becomes embedded in other files and programs, potentially rendering the system inoperable.

2. Trojan Horse

This type of application captures user login credentials. It stores them to transfer them to a malicious user who can then log in to the computer and access system resources.

3. Logic Bomb

A logic bomb is a situation in which software only misbehaves when particular criteria are met; otherwise, it functions normally.

4. Trap Door

A trap door is when a program that is supposed to work as expected has a security weakness in its code that allows it to do illegal actions without the user's knowledge.

System Threats

System threats are described as the misuse of system services and network connections to cause user problems. These threats may be used to trigger the program threats over an entire network, known as program attacks. System threats make an environment in which OS resources and user files may be misused. There are various system threats. Some of them are as follows:

1. Port Scanning

It is a method by which the cracker determines the system's vulnerabilities for an attack. It is a fully automated process that includes connecting to a specific port via TCP/IP. To protect the attacker's identity, port scanning attacks are launched through Zombie Systems, which previously independent systems now serve their owners while being utilized for such terrible purposes.

2. Worm

The worm is a process that can choke a system's performance by exhausting all system resources. A Worm process makes several clones, each consuming system resources and preventing all other processes from getting essential resources. Worm processes can even bring a network to a halt.

3. Denial of Service

Denial of service attacks usually prevents users from legitimately using the system. For example, if a denial-of-service attack is executed against the browser's content settings, a user may be unable to access the internet.

Threats to Operating System

There are various threats to the operating system. Some of them are as follows:

Malware

It contains viruses, worms, trojan horses, and other dangerous software. These are generally short code snippets that may corrupt files, delete the data, replicate to propagate further, and even crash a system. The malware frequently goes unnoticed by the victim user while criminals silently extract important data.

Network Intrusion

Network intruders are classified as masqueraders, misfeasors, and unauthorized users. A masquerader is an unauthorized person who gains access to a system and uses an authorized person's account. A misfeasor is a legitimate user who gains unauthorized access to and misuses programs, data, or resources. A rogue user takes supervisory authority and tries to evade access constraints and audit collection.

Buffer Overflow

It is also known as buffer overrun. It is the most common and dangerous security issue of the operating system. It is defined as a condition at an interface under which more input may be placed into a buffer and a data holding area than the allotted capacity, and it may overwrite other information. Attackers use such a situation to crash a system or insert specially created malware that allows them to take control of the system.

How to ensure Operating System Security?

There are various ways to ensure operating system security. These are as follows:

Authentication

The process of identifying every system user and associating the programs executing with those users is known as authentication. The operating system is responsible for implementing a security system that ensures the authenticity of a user who is executing a specific program. In general, operating systems identify and authenticate users in three ways.

1. Username/Password

Every user contains a unique username and password that should be input correctly before accessing a system.

2. User Attribution

These techniques usually include biometric verification, such as fingerprints, retina scans, etc. This authentication is based on user uniqueness and is compared to database samples already in the system. Users can only allow access if there is a match.

3. User card and Key

To login into the system, the user must punch a card into a card slot or enter a key produced by a key generator into an option provided by the operating system.

One Time passwords

Along with standard authentication, one-time passwords give an extra layer of security. Every time a user attempts to log into the One-Time Password system, a unique password is needed. Once a one-time password has been used, it cannot be reused. One-time passwords may be implemented in several ways.

1. Secret Key

The user is given a hardware device that can generate a secret id that is linked to the user's id. The system prompts for such a secret id, which must be generated each time you log in.

2. Random numbers

Users are given cards that have alphabets and numbers printed on them. The system requests numbers that correspond to a few alphabets chosen at random.

3. Network password

Some commercial applications issue one-time passwords to registered mobile/email addresses, which must be input before logging in.

Firewalls

Firewalls are essential for monitoring all incoming and outgoing traffic. It imposes local security, defining the traffic that may travel through it. Firewalls are an efficient way of protecting network systems or local systems from any network-based security threat.

Physical Security

The most important method of maintaining operating system security is physical security. An attacker with physical access to a system may edit, remove, or steal important files since operating system code and configuration files are stored on the hard drive.

Operating System Security Policies and Procedures

Various operating system security policies may be implemented based on the organization that you are working in. In general, an OS security policy is a document that specifies the procedures for ensuring that the operating system maintains a specific level of integrity, confidentiality, and availability.

OS Security protects systems and data from worms, malware, threats, ransomware, backdoor intrusions, viruses, etc. Security policies handle all preventative activities and procedures to ensure an operating system's protection, including steal, edited, and deleted data.

As OS security policies and procedures cover a large area, there are various techniques to addressing them. Some of them are as follows:

1. Installing and updating anti-virus software
2. Ensure the systems are patched or updated regularly
3. Implementing user management policies to protect user accounts and privileges.
4. Installing a firewall and ensuring that it is properly set to monitor all incoming and outgoing traffic.

Difference Between Virus and Worm

While discussing the differences between virus and worm, it is important to first understand the larger category of malicious programs, called "**Malware**". Malware can be defined as a special kind of code or application specifically developed to harm electronic devices or the people using those devices. Viruses and worms are both types of malware; however, there are significant differences between them.

In this article, we are discussing the significant differences between viruses and worms. Let's first understand both with the definitions:

What is a Virus?

According to the definition, a Virus is a program developed using malicious codes with a nature that links itself to the executable files and propagate device to device. Viruses are often transferred through the downloaded files and the shared files. They can also be attached with a scripting program and non-executable files like images, documents, etc. However, the virus remains dormant even after arriving on the device with the infected files. After the user executes the infected program, the virus gets activated and starts replicating further on its own.

Viruses can harm the system by the following means:

- Filling up the disk space unnecessarily
- Formatting the hard disk drive automatically
- Making the system slow
- Modify, or delete personal data or system files
- Stealing sensitive data

How does a virus spread?

The virus does not have the capability of spreading itself. It requires the host and human support to spread. The virus is developed in such a way that it attaches itself to the executable files. It further spreads when the infected executable file or software is transferred from one device to another. As soon as human launches the infected file or a program, the virus starts replicating itself.

Typically, the infected program continues to work normally even after the viral infection. However, some viruses can overwrite all the infected program files, destroying the particular program altogether. Besides, the virus attaches itself to new executable files and repeats the entire vicious cycle all over again. This is the reason why the viruses spread at a slower speed. Usually, the viruses are transferred using collaboration apps, email attachments, network share, hard drive, and USB flash drive.

What is a Worm?

Worms are the type of virus that can self-replicate and travel from device to device using a computer network. That means worms don't need any host to spread. They are standalone computer malware that doesn't even require human support to execute. Usually, worms use computer networks by exploiting vulnerabilities, and that makes them spread more quickly.

Besides, worms stay within the memory of an infected computer, making a computer think they are part of the system files. This helps worms to avoid any suspicious detection. Unlike a typical virus, worms don't harm the system data. Instead, they tend to consume system resources like CPU, memory, or network bandwidth and make the entire system or network crash. Because of self-replicating nature, worms can even disrupt systems in a series worldwide using a network.

How does a worm spread?

Unlike viruses, worms don't require host files to spread. This means that worms do not attach themselves with executable files or programs. Instead, worms find a weak spot in the system and enter through a vulnerability in the network. Before we detect and remove worms from our system, they replicate and spread automatically and consume all the network bandwidth. This can result in the failure of the entire network and web servers. Because worms can spread automatically, their spreading speed is comparatively faster than other malware.

Apart from this, worms can also reach other networks that are attached to the infected system. The most dangerous thing is that the worms can send themselves into other systems using email services.

Key Differences between Virus and Worm

Few key differences between Virus and Worm are listed below:

- Worms usually spread using a computer network, whereas viruses use executable files to spread from one system to others.
- Worms can automatically replicate to different systems, while viruses require human action to replicate.
- The spreading speed of viruses is comparatively slower than worms. Because worms can replicate automatically, they spread at a much faster speed.
- The viruses are designed to corrupt, delete, or modify the target devices' data or software, whereas worms don't harm the stored data but aim to harm the resources.
- Viruses are found in executable files or can attach themselves to executable files to operate on target devices, whereas worms remain independent in an infected device's memory.
- The viruses require hosts to spread from one device to another. Worms, on the other side, don't need any host.
- Viruses usually destroy and damage the stored data, whereas worms can harm the entire network by using maximum resources. For example- by consuming bandwidth, sending mass emails, or deleting or copying files in bulk.

Major Differences between Virus and Worm

The other major differences between a virus and a worm can be explained in a tabulated form, as below:

Attributes	Virus	Worm
Nature	The virus is a malicious program attached to the executable files so that it can spread from one system to another.	A worm is a program made up of malicious code that replicates itself and propagates itself from device to device using a network.
Human Action	Human action is required for viruses. Without human help, they cannot execute and spread.	Human action is not required for the worms. They are designed and developed in such a way that they can automatically execute and spread.
Speed of Spread	The virus spreads at a relatively slower speed than a Worm.	Worms spreading speed is fast, and they can infect multiple devices or networks quickly.
Host Requirement	The host is required to spread viruses. Viruses connect themselves to the host and travel with the host. They spread into devices where the host reaches.	The host is not necessary for the worms to replicate from one device to another. Worms exploit the vulnerability of a network to spread.
Protection Method	To protect the devices from viruses, the user must have installed trusted antivirus software.	To protect the devices from worms, the user is required to use antivirus software and a firewall. Many modern antivirus software come with an in-built firewall system.
Malware Removal	To clean the virus's infection or stop spreading it further, the user must scan the device using antivirus software and remove the infected files. Sometimes, formatting an entire system is the only option to remove the infection	To remove the worm's infection, the user needs a virus removal tool. Also, users must allow only trusted software through a firewall to eliminate the chances of spreading worms. In a complex situation,

	completely.	formatting the system is the best option.
Consequences	Viruses can corrupt, alter, or delete the stored files or programs in the infected device.	Worms do not harm stored files or software; instead, they consume system resources and increase the system's load. This eventually leads to slow processing and system crashes. Also, it can result in network failures.

Which is more dangerous?

The impact of viruses and worms can be mild to severe. Both are developed to harm the computer and other devices. They can steal and damage the data of individuals, organizations, and government institutions. However, worms seem to look more dangerous because of their self-replicating nature. Also, they can spread faster than viruses. Worms can silently spread into multiple devices by detecting the vulnerability and then inset themselves by exploiting that vulnerability.

For instance, let's assume that a worm has attacked us. A worm will infect our emails and transfer itself to all our contacts. It can further replicate itself and spread to all of our contacts' contacts. By doing this, a worm can create an infinite cycle with huge potential damage and harm the resources of all the connected devices or systems.

Viruses, on the other side, cannot replicate themselves. They need human-support to start operating, and they are relatively slower at spreading. This makes them less dangerous than worms.

How to be safe from viruses and worms?

Viruses and worms can cause severe damage to the computer and other devices. It is not enough to only use antivirus software and a firewall system. We are required to follow proper safety guidelines to protect our devices against viruses and worms. Some of the best practices that can be followed to be safe from viruses and worms are given below:

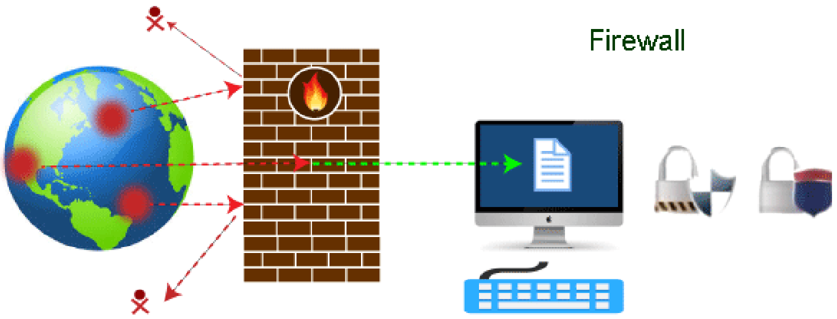
- **Proactive**: Be cautious while opening an email from unknown people or sources. We should avoid clicking on links or attachments, which are part of the email unless we are sure that they are genuine. Several offers and banners look too good to be true (however, they are not in most cases).

- **Updates**: We should keep our software and operating system updated. Outdated software may have vulnerabilities, and attackers may benefit from sending viruses, worms, or other malware into our devices.
- **Ad-blocker**: Malware can cause many advertisements to appear on our computer screens, and those ads can be harmful if we accidentally click on them. Thus, it is best to install good ad-blocking software or browser extension to block all malicious ads.
- **Authorized Store**: We should be careful while downloading software on our devices. It is a best practice to download software from official websites or authorized application store. Many third-party stores are available on the internet, and most of them do not verify software safety.
- **Monitoring**: Analyzing and monitoring the system files and system activities' behavior can help us spot suspicious actions, if any. In case the system suddenly becomes slow, or there are several advertisements on the screen, such activities can be a sign of an anomaly. Scanning a full system using an antivirus can be beneficial in this situation.

What is a Firewall?

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.



Firewall: Hardware or Software

This is one of the most problematic questions whether a firewall is a hardware or software. As stated above, a firewall can be a network security device or a software program on a computer. This means that the firewall comes at both levels, i.e., hardware and software, though it's best to have both.

Each format (a firewall implemented as hardware or software) has different functionality but the same purpose. A hardware firewall is a physical device that attaches between a computer network and a gateway. For example, a broadband router. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software.

Apart from that, there are cloud-based firewalls. They are commonly referred to as FaaS (firewall as a service). A primary advantage of using cloud-based firewalls is that they can be managed centrally. Like hardware firewalls, cloud-based firewalls are best known for providing perimeter security.

Why Firewall

Firewalls are primarily used to prevent malware and network-based attacks. Additionally, they can help in blocking application-layer attacks. These firewalls act as a gatekeeper or a barrier. They monitor every attempt between our computer and another network. They do not allow data packets to be transferred through them unless the data is coming or going from a user-specified trusted source.

Firewalls are designed in such a way that they can react quickly to detect and counter-attacks throughout the network. They can work with rules configured to protect the network and perform quick assessments to find any suspicious activity. In short, we can point to the firewall as a traffic controller.

Some of the important risks of not having a firewall are:

Open Access

If a computer is running without a firewall, it is giving open access to other networks. This means that it is accepting every kind of connection that comes through someone. In this case, it is not possible to detect threats or attacks coming through our network. Without a firewall, we make our devices vulnerable to malicious users and other unwanted sources.

Lost or Comprised Data

Without a firewall, we are leaving our devices accessible to everyone. This means that anyone can access our device and have complete control over it, including the network. In this case, cybercriminals can easily delete our data or use our personal information for their benefit.

Network Crashes

In the absence of a firewall, anyone could access our network and shut it down. It may lead us to invest our valuable time and money to get our network working again.

Therefore, it is essential to use firewalls and keep our network, computer, and data safe and secure from unwanted sources.

Brief History of Firewall

Firewalls have been the first and most reliable component of defense in network security for over 30 years. Firewalls first came into existence in the late 1980s. They were initially designed as packet filters. These packet filters were nothing but a setup of networks between computers. The primary function of these packet filtering firewalls was to check for packets or bytes transferred between different computers.

Firewalls have become more advanced due to continuous development, although such packet filtering firewalls are still in use in legacy systems.

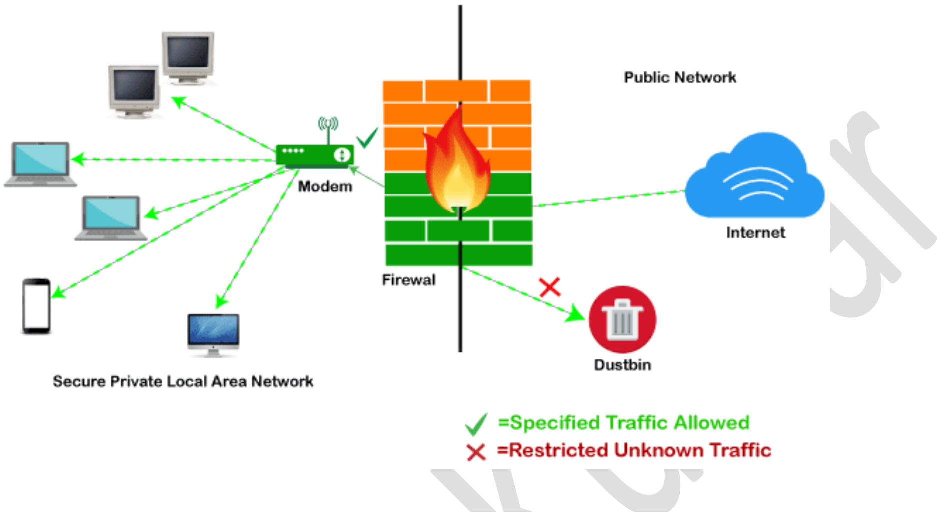
As the technology emerged, **Gil Shwed** from **Check Point Technologies** introduced the first stateful inspection firewall in 1993. It was named as FireWall-1. Back in 2000, **Netscreen** came up with its purpose-built firewall **'Appliance'**. It gained popularity and fast adoption within enterprises because of increased internet speed, less latency, and high throughput at a lower cost.

The turn of the century saw a new approach to firewall implementation during the mid-2010. The **'Next-Generation Firewalls'** were introduced by the **Palo Alto Networks**. These firewalls came up with a variety of built-in functions and capabilities, such as Hybrid Cloud Support, Network Threat Prevention, Application and Identity-Based Control, and Scalable Performance, etc. Firewalls are still getting new features as part of continuous development. They are considered the first line of defense when it comes to network security.

How does a firewall work?

A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IP addresses, or sources.


Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ =Specified Traffic Allowed
✗ =Restricted Unknown Traffic

Functions of Firewall

As stated above, the firewall works as a gatekeeper. It analyzes every attempt coming to gain access to our operating system and prevents traffic from unwanted or non-recognized sources.

Since the firewall acts as a barrier or filter between the computer system and other networks (i.e., the public Internet), we can consider it as a traffic controller. Therefore, a firewall's primary function is to secure our network and information by controlling network traffic, preventing unwanted incoming network traffic, and validating access by assessing network traffic for malicious things such as hackers and malware.

Generally, most operating systems (for example - Windows OS) and security software come with built-in firewall support. Therefore, it is a good idea to ensure that those options are turned on. Additionally, we can configure the security settings of the system to be automatically updated whenever available.

Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features:

- Network Threat Prevention
- Application and Identity-Based Control
- Hybrid Cloud Support
- Scalable Performance
- Network Traffic Management and Control

- Access Validation
- Record and Report on Events

Limitations of Firewall

When it comes to network security, firewalls are considered the first line of defense. But the question is whether these firewalls are strong enough to make our devices safe from cyber-attacks. The answer may be "no". The best practice is to use a firewall system when using the Internet. However, it is important to use other defense systems to help protect the network and data stored on the computer. Because cyber threats are continually evolving, a firewall should not be the only consideration for protecting the home network.

The importance of using firewalls as a security system is obvious; however, firewalls have some limitations:

- Firewalls cannot stop users from accessing malicious websites, making it vulnerable to internal threats or attacks.
- Firewalls cannot protect against the transfer of virus-infected files or software.
- Firewalls cannot prevent misuse of passwords.
- Firewalls cannot protect if security rules are misconfigured.
- Firewalls cannot protect against non-technical security risks, such as social engineering.
- Firewalls cannot stop or prevent attackers with modems from dialing in to or out of the internal network.
- Firewalls cannot secure the system which is already infected.

Therefore, it is recommended to keep all Internet-enabled devices updated. This includes the latest operating systems, web browsers, applications, and other security software (such as anti-virus). Besides, the security of wireless routers should be another practice. The process of protecting a router may include options such as repeatedly changing the router's name and password, reviewing security settings, and creating a guest network for visitors.

Types of Firewall

Depending on their structure and functionality, there are different types of firewalls. The following is a list of some common types of firewalls:

- Proxy Firewall
- Packet-filtering firewalls
- Stateful Multi-layer Inspection (SMLI) Firewall

- Unified threat management (UTM) firewall
- Next-generation firewall (NGFW)
- Network address translation (NAT) firewalls

Difference between a Firewall and Anti-virus

Firewalls and anti-viruses are systems to protect devices from viruses and other types of Trojans, but there are significant differences between them. Based on the vulnerabilities, the main differences between firewalls and anti-viruses are tabulated below:

Attributes	**Firewall**	**Anti-virus**
Definition	A firewall is defined as the system which analyzes and filters incoming or outgoing data packets based on pre-defined rules.	Anti-virus is defined as the special type of software that acts as a cyber-security mechanism. The primary function of Anti-virus is to monitor, detect, and remove any apprehensive or distrustful file or software from the device.
Structure	Firewalls can be hardware and software both. The router is an example of a physical firewall, and a simple firewall program on the system is an example of a software firewall.	Anti-virus can only be used as software. Anti-virus is a program that is installed on the device, just like the other programs.
Implementation	Because firewalls come in the form of hardware and software, a firewall can be implemented either way.	Because Anti-virus comes in the form of software, therefore, Anti-virus can be implemented only at the software level. There is no possibility of implementing Anti-virus at the hardware level.
Responsibility	A firewall is usually defined as a network controlling system. It means that firewalls are primarily responsible for monitoring and filtering network traffic.	Anti-viruses are primarily responsible for detecting and removing viruses from computer systems or other devices. These viruses can be in the form of infected files or software.

Scalability	Because the firewall supports both types of implementations, hardware, and software, therefore, it is more scalable than anti-virus.	Anti-viruses are generally considered less-scalable than firewalls. This is because anti-virus can only be implemented at the software level. They don't support hardware-level implementation.
Threats	A firewall is mainly used to prevent network related attacks. It mainly includes external network threats?for example- Routing attacks and IP Spoofing.	Anti-virus is mainly used to scan, find, and remove viruses, malware, and Trojans, which can harm system files and software and share personal information (such as login credentials, credit card details, etc.) with hackers.

What is Wireless Security?

Wireless security revolves around the concept of securing the wireless network from malicious attempts and unauthorized access.

The wireless security can be delivered through different ways such as:

1. Hardware-based: where routers and switches are fabricated with encryption measures protects all wireless communication. So, in this case, even if the data gets compromised by the cybercriminal, they will not be able to decrypt the data or view the traffic's content.
2. Wireless setup of IDS and IPS: helps in detecting, alerting, and preventing wireless networks and sends an alarm to the network administrator in case of any security breach.
3. Wireless security algorithms: such as WEP, WPA, WPA2, and WPA3. These are discussed in the subsequent paragraphs.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the oldest security algorithm of 1999. It uses the initialization vector (IV) method. The first versions of the WEP algorithm were not predominantly strong enough, even when it got released. But the reason for this weak release was because of U.S. limits on exporting different cryptographic technologies, which led the manufacturing companies to restrict their devices to 64-bit encryption only. As the limitation was withdrawn, the 128 bit and 256 bit WEP encryption were developed and came into the wireless security market, though 128 became standard.

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) was the next Wi-Fi Alliance's project that replaced the WEP standard's increasingly noticeable vulnerabilities. WPA was officially adopted in the year 2003, one year before the retirement of WEP. WPA's most common configuration is with WPA-PSK, which is abbreviated as Pre-Shared Key. WPA uses 256-bit, which was a considerable enhancement above the 64-bit as well as 128-bit keys.

Wi-Fi Protected Access II (WPA2)

Wi-Fi Protected Access II (WPA2) became official in the year 2006 after WPA got outdated. It uses the AES algorithms as a necessary encryption component as well as uses CCMP (Counter Cipher Mode - Block Chaining Message Authentication Protocol) by replacing TKIP.

Wi-Fi Protected Access 3 (WPA3)

Wi-Fi Protected Access 3 (WPA3) is the latest and the third iteration of this family developed under Wi-Fi Alliance. It has personal and enterprise security-support features and uses 384-bit Hashed Message Authentication Mode, 256-bit Galois / Counter Mode Protocol (GCMP-256) well as Broadcast/Multicast Integrity Protocol of 256-bit. WPA3 also provides perfect forward secrecy mechanism support.

What is ad-hoc network?

An ad hoc network is one that is spontaneously formed when devices connect and communicate with each other. The term ad hoc is a Latin word that literally means "for this," implying improvised or impromptu.

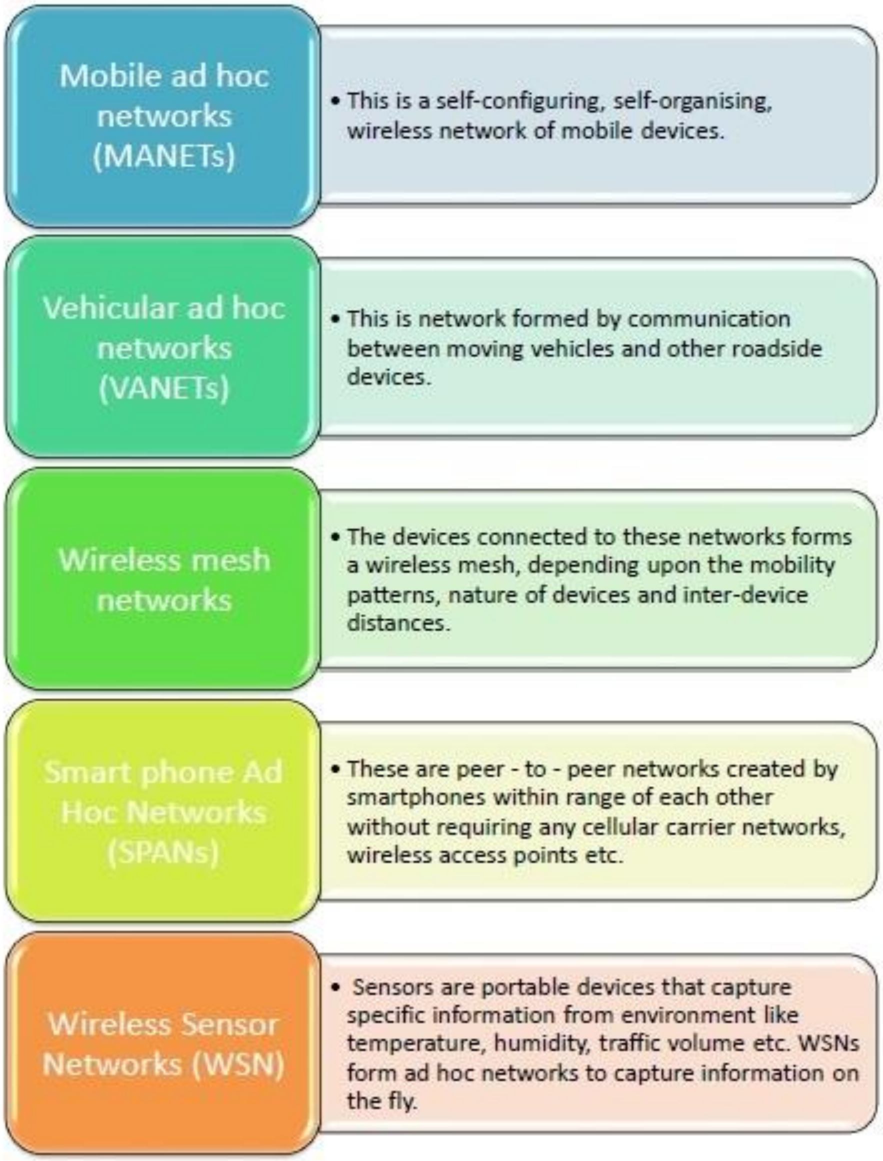
Ad hoc networks are mostly wireless local area networks (LANs). The devices communicate with each other directly instead of relying on a base station or access points as in wireless LANs for data transfer co-ordination. Each device participates in routing activity, by determining the route using the routing algorithm and forwarding data to other devices via this route.

Classifications of Ad Hoc Networks

Ad hoc networks can be classified into several types depending upon the nature of their applications. The most prominent ad hoc networks that are commonly incorporated are illustrated in the diagram below −

What is a wireless ad hoc network (WANET)?

A wireless ad hoc network (WANET) is a type of local area network (LAN) that is built spontaneously to enable two or more wireless devices to be connected to each other without requiring typical network infrastructure equipment, such as a wireless router or access point.



Mobile ad hoc networks (MANETs)

- This is a self-configuring, self-organising, wireless network of mobile devices.

Vehicular ad hoc networks (VANETs)

- This is network formed by communication between moving vehicles and other roadside devices.

Wireless mesh networks

- The devices connected to these networks forms a wireless mesh, depending upon the mobility patterns, nature of devices and inter-device distances.

Smart phone Ad Hoc Networks (SPANs)

- These are peer - to - peer networks created by smartphones within range of each other without requiring any cellular carrier networks, wireless access points etc.

Wireless Sensor Networks (WSN)

- Sensors are portable devices that capture specific information from environment like temperature, humidity, traffic volume etc. WSNs form ad hoc networks to capture information on the fly.