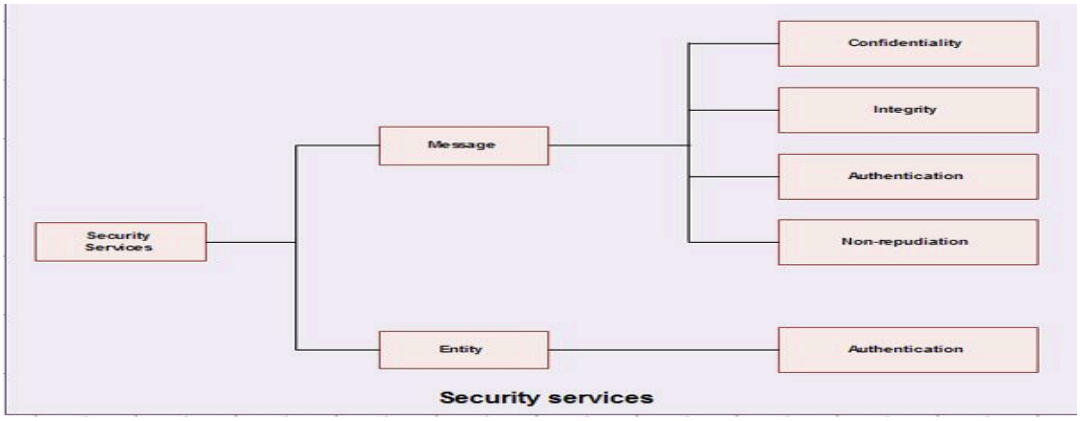
Computer Network Security

1. Explain Security Services and mechanisms to implement it.

Ans. Network security services are an intricate defensive system created to protect any computer devices and systems from potential cyber threats, data leakage, or other malicious activity.



Message Confidentiality: Message confidentiality or privacy means that the sender and the receiver expect confidentiality. The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage. When a customer communicates with her bank, she expects that the communication is totally confidential.

Message Integrity: Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally nor maliciously. As more and more monetary exchanges occur over the Internet, integrity is crucial.

Message Authentication: Message authentication is a service beyond message integrity. In message authentication, the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.

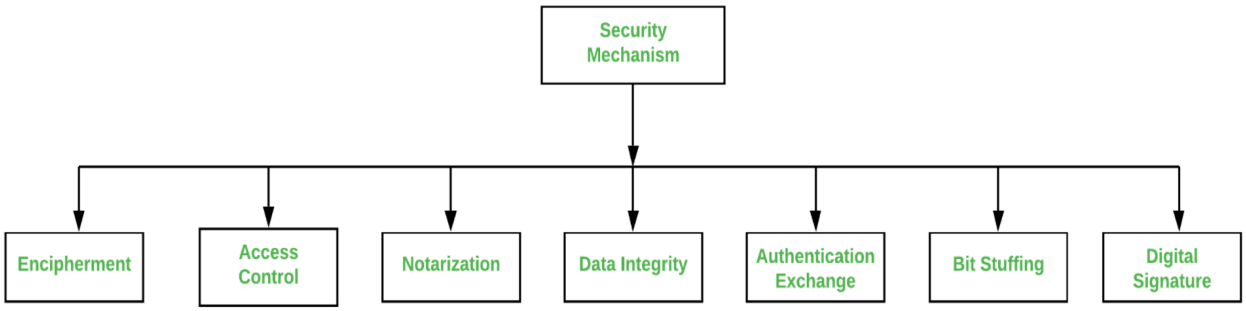
Message Nonrepudiation: Message nonrepudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send. The burden of proof falls on the receiver.

Entity: In entity authentication (or user identification), the entity or user is verified prior to access to the system resources (files, for example).

The above mentioned services can be implemented by the security mechanisms.

Security Mechanism: It can be termed as a set of processes that deal with recovery from security attacks. Various mechanisms are designed to recover from these specific attacks at various protocol layers.

Types of Security Mechanism are :



Encipherment: This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into non-readable form. It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.

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

Notarization : This security mechanism involves use of trusted third parties in communication. It acts as a mediator between sender and receiver so that any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.

Data Integrity : This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending a packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.

Authentication exchange : This security mechanism deals with identity to be known in communication. This is achieved at the TCP/IP layer where a two-way handshaking mechanism is used to ensure data is sent or not.

Bit stuffing : This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.

Digital Signature : This security mechanism is achieved by adding digital data that is not visible to eyes. It is a form of electronic signature which is added by the sender which is checked by the receiver electronically. This mechanism is used to preserve data which is not more confidential but the sender's identity is to be notified.

2. Compare HMAC and CMAC.

Ans. HMAC (Hash-based Message Authentication Code) and CMAC (Cipher-based Message Authentication Code) are both cryptographic constructs used for ensuring the integrity and authenticity of messages. However, they have some key differences in terms of their construction and applications.

Feature	HMAC	CMAC
Construction	Uses a hash function and a secret key.	Uses a block cipher in CBC-MAC mode with a secret key.
Applicability	Commonly used in protocols like TLS, IPsec.	Typically used in contexts with block ciphers, such as disk encryption protocols.
Security	Security is tied to the strength of the hash function.	Security relies on the security of the block cipher and the construction.
Key Length	Key length varies based on the hash function used. Often recommended to match the hash output length.	Key length is typically the same as the block size of the underlying block cipher.
Performance	Generally efficient due to the speed of hash functions.	Slightly higher computational overhead due to block cipher usage.
Example	`HMAC-SHA256(key, message)`	`CMAC-AES(key, message)`

3. Explain the need of Network Access Control in Enterprise Networks.

Ans. Network Access Control is a security solution that uses a set of protocols to keep unauthorized users and devices out of a private network or give restricted access to the devices which are compliant with network security policies. It is also known as Network Admission Control. It handles network management and security that implements security policy, compliance, and management of access control to a network.

NAC works on wired and wireless networks by identifying different devices that are connected to the network. For setting up an NAC network security solution, administrators will determine the protocols that will decide how devices and users are authorized for the right level of authorization. Access rules are generally based on the criterion such as device used, the location accessed from, the access rights of various individuals, as well as the specific data and resources being accessed.

Network Access Control (NAC) plays a crucial role in enhancing the security posture of enterprise networks. Here are some key reasons explaining the need for Network Access Control in enterprise networks:

1. Unauthorized Access Prevention: NAC helps prevent unauthorized devices from gaining access to the enterprise network. It ensures that only devices with proper authentication and authorization are allowed to connect.
2. Endpoint Security: NAC enforces security policies on endpoints (devices) before allowing them to connect to the network. This helps in ensuring that all devices meet a certain level of security compliance, such as having updated antivirus software and operating system patches.
3. BYOD (Bring Your Own Device) Security: With the increasing trend of employees using their own devices for work, NAC provides a mechanism to securely onboard and manage these devices. It helps in segregating personal and corporate data on BYOD devices and ensures that they comply with security policies.
4. Guest Network Security: Many enterprises have guest networks for visitors. NAC allows for secure guest access by providing a controlled and limited network environment. It ensures that guests only have access to the necessary resources without compromising the internal network security.
5. Compliance Requirements: Many industries and organizations have regulatory compliance requirements that mandate the implementation of specific security measures. NAC helps in meeting these compliance requirements by enforcing security policies and providing visibility into the network.
6. Threat Detection and Response: NAC solutions often include features for continuous monitoring of devices on the network. They can detect anomalous behavior or security threats and respond by isolating or quarantining affected devices, preventing the spread of threats within the network.

7. Network Visibility: NAC provides administrators with detailed visibility into the devices connecting to the network. This visibility is crucial for identifying potential security risks, tracking device activity, and responding to security incidents.
8. Dynamic Access Control: NAC allows for dynamic access control based on user roles, device types, and security postures. This ensures that users and devices have access only to the resources they need, reducing the attack surface and minimizing the impact of security incidents.
9. Integration with Security Infrastructure: NAC can be integrated with other security infrastructure components, such as firewalls, intrusion detection systems, and security information and event management (SIEM) systems. This integration enhances overall network security by providing a coordinated and layered defense.

4. **Explain the major NAC enforcement methods**

Ans. First 2 paragraphs as it is.
Network Access Control (NAC) enforcement methods are mechanisms employed to enforce security policies and control access to a network based on the compliance and security posture of connected devices. Here are the major NAC enforcement methods:

IEEE 802.1X:

Description: IEEE 802.1X is a port-based authentication standard that provides a mechanism for devices to authenticate before being allowed access to a network.
How it Works: Devices must authenticate themselves through a challenge-response mechanism before being granted access to the network. This is commonly used for both wired and wireless connections, ensuring that only authorized devices can connect to a network port.

VLANs (Virtual LANs):

Description: VLANs are used to logically segment a network into different broadcast domains.

How it Works: Devices are assigned to specific VLANs based on their roles, departments, or security postures. This segmentation helps in isolating traffic and controlling access between different segments. NAC can enforce VLAN assignments based on the compliance status of devices.

Firewalls:

Description: Firewalls are network security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules.

How it Works: NAC can enforce security policies by communicating with firewalls. For example, based on the compliance status of a device, the NAC system can instruct the firewall to permit or deny certain types of traffic from that device.

DHCP (Dynamic Host Configuration Protocol) Management:

Description: DHCP is used to dynamically assign IP addr esses to devices on a network.

How it Works: NAC can work with DHCP to ensure that only compliant devices receive a valid IP address. Non-compliant devices may be assigned to a restricted network or a quarantine VLAN, limiting their access until they meet security requirements.

RBACs (Role-Based Access Control):

Description: RBAC is a method of restricting network access based on user roles.

How it Works: Users or devices are assigned roles that dictate their level of access. NAC can enforce RBAC by ensuring that only devices with the appropriate role-based permissions are granted access to specific network resources.

5. **Explain playfair cipher with an example.**

Ans. The Playfair Cipher encryption technique can be used to encrypt or encode a message. It operates exactly like typical encryption. The only difference is that it encrypts a digraph, or a pair of two letters, instead of a single letter.

In playfair cipher, unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.

The Playfair Cipher Encryption Algorithm:

The Algorithm consists of 2 steps:

Generate the key Square(5×5):

- The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.
- The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

The Playfair Cipher Decryption Algorithm:

The Algorithm consists of 2 steps:

Generate the key Square(5×5) at the receiver's end:

- The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.

- The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

Algorithm to decrypt the ciphertext: The ciphertext is split into pairs of two letters (digraphs).

Playfair Cipher example

Assume "communication" is the plaintext and "computer" is the encryption key.

The key might be any word or phrase. Let's figure out what was communicated.

1. First, create a digraph from the plaintext by applying rule 2, which is CO MX MU NI CA TE.

2. Make a key matrix that is 5 by 5. (by rule 3). The significant element in our circumstances is the computer

C	O	M	P	U
T	E	R	A	B
D	F	G	H	I
K	L	N	Q	S
V	W	X	Y	Z

3. We will now look through each key-matrix pair individually to find the corresponding encipher.

The first digraph is CO. The two are displayed together in a row. The CO and OM are encrypted using Rule 4(i).

The second digraph is MX. Both of them are visible in the same column. The MX and RM are encrypted using Rule 4(ii).

The third digraph is MU. The two are displayed together in a row. MU is encrypted into the PC using Rule 4(i).

The fourth digraph is NI. The pair is visible in several rows and columns. NI is encrypted into SG using Rule 4(iii).

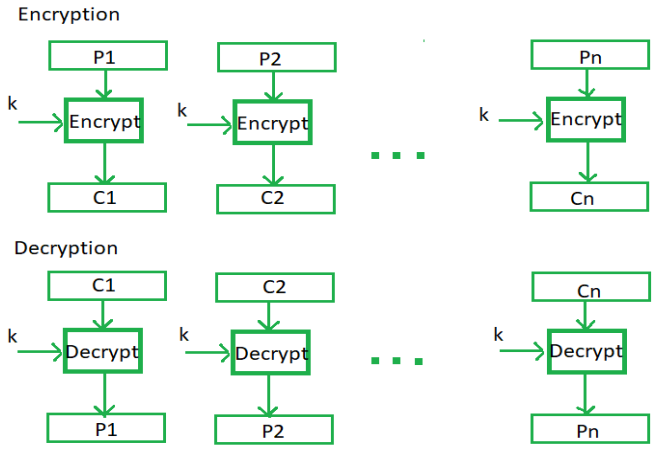
The sixth digraph is CA. The pair is visible in several rows and columns. Rule 4(iii) states are used by CA to encrypt data.

Therefore, the plaintext COMMUNICATE is encrypted using OMRMPCSGPTER.

6. Describe different Block Cipher Modes.

Ans. Block cipher modes of operation are techniques used to encrypt large amounts of data using a block cipher. A block cipher processes fixed-size blocks of data at a time and produces a block of ciphertext of the same size. Here are some common block cipher modes:

1. Electronic Codebook (ECB):

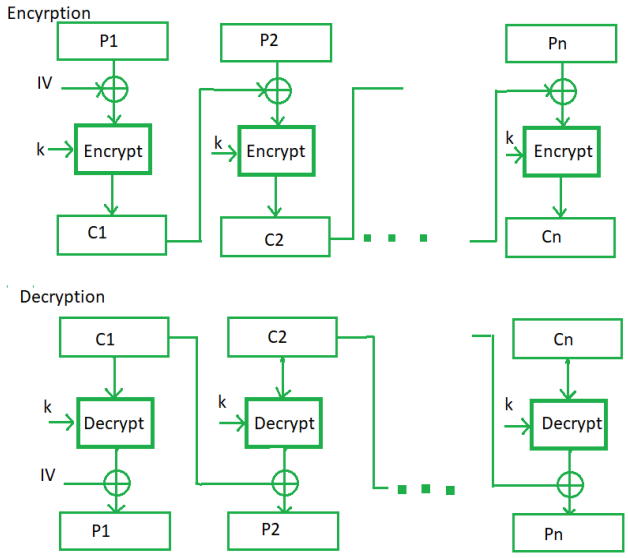


- Description: Electronic code book is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plaintext and output is in the form of blocks of encrypted ciphertext.

- Advantages:

- Simplicity: ECB is straightforward and easy to implement.
- Parallelization: Each block can be encrypted independently, allowing for parallel processing.

- Disadvantages: Lack of Diffusion: Identical blocks of plaintext will produce identical blocks of ciphertext, making it vulnerable to certain attacks. This lack of diffusion can reveal patterns in the data.

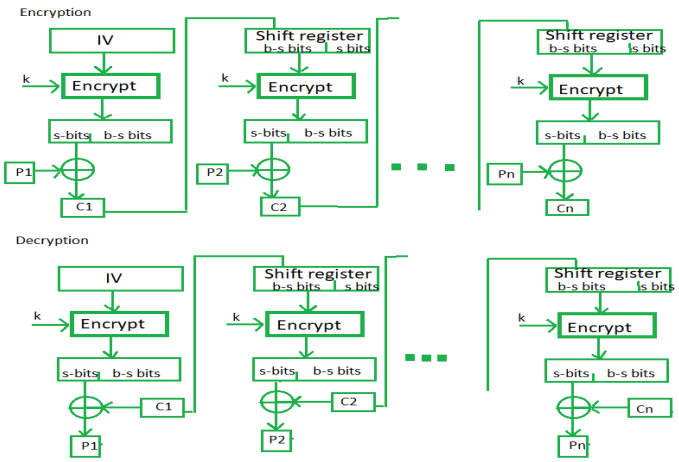


2. Cipher Block Chaining (CBC):

Description: Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. In CBC, the previous cipher block is given as input to the next encryption algorithm after XOR with the original plaintext block.

- Advantages:
  - Diffusion: CBC introduces diffusion, making identical plaintext blocks produce different ciphertext blocks.
  - Security: Generally considered more secure than ECB due to the XOR operation with the previous ciphertext block.
- Disadvantages:
  - Sequential Processing: Blocks must be processed sequentially, which limits parallelization.
  - Initialization Vector: Requires a unique IV for each message, and the IV must be unpredictable.

3. Cipher Feedback (CFB):

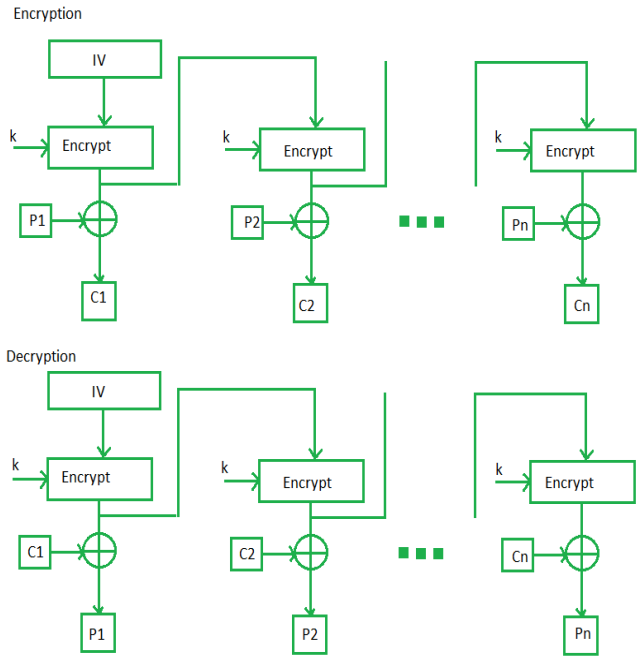


Description: In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first, an initial vector IV is used

for first encryption and output bits are divided as a set of s and b-s bits.The left-hand side s bits are selected along with plaintext bits to which an XOR operation is applied.

- Advantages:
  - Parallelization: CFB can be parallelized, as each block's encryption is independent.
  - Bit Error Propagation: Bit errors only affect the blocks where the error occurs.
- Disadvantages:
  - Bit Errors: Bit errors affect multiple bits in the ciphertext, affecting the corresponding bits in the plaintext.
  - Synchronization: Requires synchronization, as errors can propagate.

4. Output Feedback (OFB):

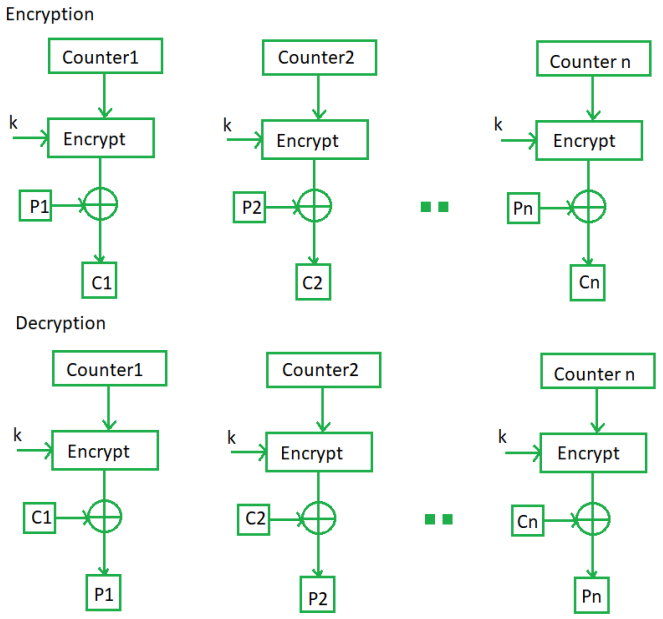


- Description:
  - Similar to CFB, OFB uses the output of the previous encryption as the key stream. The key stream is then XORed with the plaintext to produce the ciphertext.
- Advantages:
  - Parallelization: Like CFB, OFB can be parallelized.
  - Bit Error Isolation: Bit errors only affect one block in the ciphertext.
- Disadvantages:

- Synchronization: Requires synchronization, similar to CFB.

- Error Propagation: Bit errors in the key stream affect multiple bits in the ciphertext.

5. Counter (CTR):



Description: CTR mode turns a block cipher into a stream cipher by encrypting a counter value to produce a key stream, which is then XORed with the plaintext.

- Advantages:

  - Parallelization: Highly parallelizable, as each block's encryption is independent.

  - Random Access: Supports random access to blocks.

- Disadvantages:

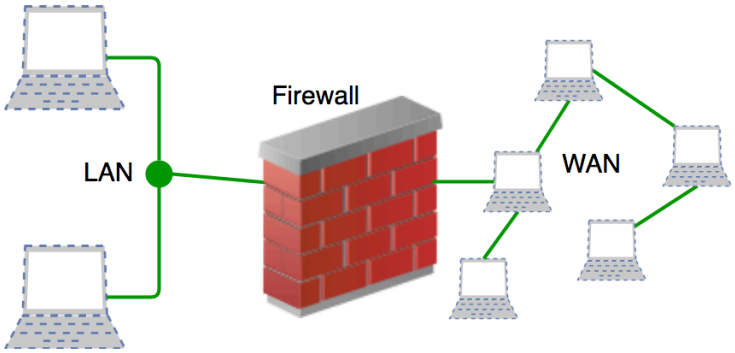
  - Unique Counters: Requires a unique counter value for each block, and the counter should never repeat.

  - Bit Error Impact: Bit errors in the key stream affect only the corresponding bits in the ciphertext.

7. State firewall design principles & its types with advantages & disadvantages.

Ans. A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

There are five key types of firewalls that use different mechanisms to identify and filter out malicious traffic:



1. packet filtering firewall
2. circuit-level gateway
3. application-level gateway (aka proxy firewall)
4. stateful inspection firewall
5. next-generation firewall (NGFW)

1. Packet Filtering: Packet filtering firewalls operate in line at junction points where devices such as routers and switches do their work. However, these firewalls don't route packets; rather they compare each packet received to a set of established criteria. Packets that are flagged as troublesome are, generally speaking, unceremoniously dropped -- that is, they are not forwarded and, thus, cease to exist.

Advantages:

Simple and efficient at filtering traffic based on predefined rules.

Minimal impact on network performance.

Disadvantages:

Limited ability to inspect traffic beyond the packet header, making it vulnerable to certain attacks.

Complex rules can be difficult to manage and maintain.

2. Circuit Level Gateway: Using another relatively quick way to identify malicious content, circuit-level gateways monitor TCP handshakes and other network protocol session initiation messages across the network as they are established

between the local and remote hosts to determine whether the session being initiated is legitimate -- whether the remote system is considered trusted.

Advantages:

Only processes requested transactions; all other traffic is rejected

Easy to set up and manage

3. Application Level Gateway: This kind of device -- technically a proxy and sometimes referred to as a proxy firewall -- functions as the only entry point to and exit point from the network. Application-level gateways filter packets not only according to the service for which they are intended -- as specified by the destination port -- but also by other characteristics, such as the HTTP request string.

Advantages:

Offers deep packet inspection at the application layer, allowing for granular control.

Can identify and block specific applications and services.

Disadvantages:

Can be resource-intensive and may impact network performance.

Complex to configure and maintain.

4. Stateful inspection: State-aware devices not only examine each packet, but also keep track of whether or not that packet is part of an established TCP or other network session. This offers more security than either packet filtering or circuit monitoring alone but exacts a greater toll on network performance.

Advantages:

Examines the state of active connections, providing better security.

Can make decisions based on the state of a connection (e.g., allowing response packets for established connections).

Disadvantages:

More resource-intensive compared to packet filtering firewalls.

Still limited in its ability to inspect application-layer content.

5. Next Generation: A typical NGFW combines packet inspection with stateful inspection and also includes some variety of deep packet inspection (DPI), as well as other network security systems, such as an IDS/IPS, malware filtering and antivirus.

Advantages:

Combines traditional firewall capabilities with advanced features like intrusion prevention, antivirus, and application awareness.

Provides more comprehensive security in a single device.

Disadvantages:

Can be costly, both in terms of hardware and licensing.

May require specialized expertise to configure and manage effectively.

8. Describe different types of protocol offered by SSL.

Ans. Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

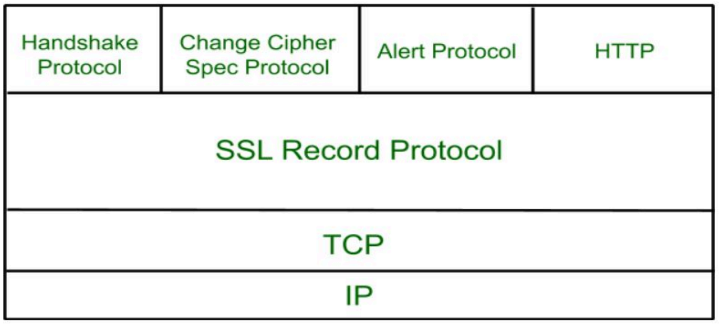
Secure Socket Layer Protocols:

SSL record protocol

Handshake protocol

Change-cipher spec protocol

Alert protocol



SSL Protocol Stack:

SSL Record Protocol:

SSL Record provides two services to SSL connection.

Confidentiality

Message Integrity

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.

Handshake Protocol: Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

Phase-1: In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.

Phase-2: Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.

Phase-3: In this phase, Client replies to the server by sending his certificate and Client-exchange-key.

Phase-4: In Phase-4 Change-cipher suite occurs and after this the Handshake Protocol ends.

Change-cipher Protocol: This protocol uses the SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in a pending state. After the handshake protocol, the Pending state is converted into the current state.

Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value. This protocol's purpose is to cause the pending state to be copied into the current state.

Alert Protocol: This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.

The level is further classified into two parts:

Warning (level = 1): This Alert has no impact on the connection between sender and receiver. Some of them are:

Bad certificate: When the received certificate is corrupt.

No certificate: When an appropriate certificate is not available.

Certificate expired: When a certificate has expired.

Certificate unknown: When some other unspecified issue arose in processing the certificate, rendering it unacceptable.

Close notify: It notifies that the sender will no longer send any messages in the connection.

Unsupported certificate: The type of certificate received is not supported.

Certificate revoked: The certificate received is in the revocation list.

Fatal Error (level = 2): This Alert breaks the connection between sender and receiver. The connection will be stopped, cannot be resumed but can be restarted.

9. What is Network access control? Explain principle elements of NAC

Ans. First two paragraphs from above.

Principle Elements of NAC(Network Access Control):

There are mainly three principle elements of NAC which are:

1.Access Requestor(AR).

2.Policy Servers.

3.Network Access Servers(NAS).

Three Principle Elements of NAC(Network Access Control).

Let's look at them one by one now:

1.Access Requestor(AR): We may determine from the name that it is someone attempting to gain access by requesting it. This access can be granted to any entity, such as a device, person, or process.

This entity attempts to get access to network resources. It might be any device handled by the NAC system, such as servers, cameras, printers, and other IP-enabled devices.

ARs are also known as supplicants or clients at times. ARs ensures that no entity has illegal access to protected resources.

To get access, these ARs must follow to the organization's specific guidelines or policies.

2.Policy Server: The policy server analyzes what access should be provided to AR based on the AR's identity, permission level, attempted request, and an organization's established access policy.

The policy server frequently relies on backend services, such as antivirus, patch management, or a user directory, to function.

The policy server helps to determine the host's state. An organization creates different access policies to clearly authorize or reject such access. If the AR

follows the organization's policy, the policy server gives access based on the requestor's permission; otherwise, the AR will not be permitted access based on its permission.

It should be noted that there are various commercial systems on the market now that provide such policy servers for both on-premises and cloud computing. Some of the most common examples include the Cisco Identity Services Engine(ISE), Forescout Platform, Aruba ClearPass Policy Manager, and FortiNAC.

These tools offer highly detailed ways to set organizational rules and control the organization's full IP infrastructure.

3.Network Access Server(NAS): Users connecting to an organization's internal network from distant locations utilize the NAS as an access control point. These often serve as VPNs and give users access to the company's internal network. These days, NAS functionality is frequently included in policy server systems. Remote employees can connect to the company's internal network via NAS, which serves as an access point for them. This allows the company and its employees to create a secure connection and grant authorized access to the network.

Thus, these were the Three Principle Elements of NAC (Network Access control).

10. Explain Kerberos Protocol in detail, with diagram

Ans. 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.

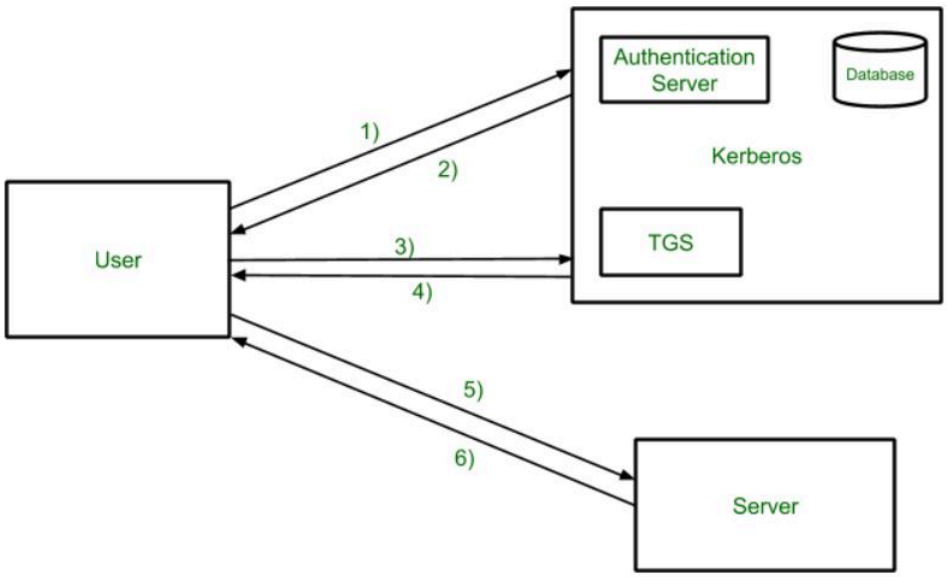
Database:

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

11. Explain the working of IPsec in its different mode.

Ans. IP Sec (Internet Protocol Security) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the

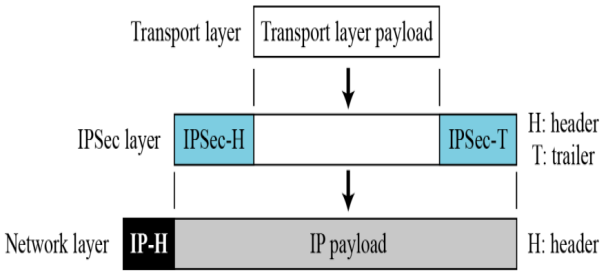
IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted, and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security

- IPsec can be used to do the following things:
- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

IPSec operates in one of two different modes: transport mode or tunnel mode.

Transport Mode

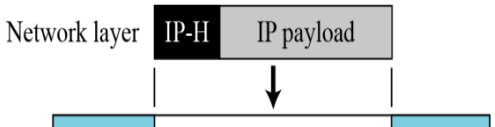


In transport mode, IPSec protects what is delivered from the transport layer to the network layer.

IPSec in transport mode does not protect the IP header; it only protects the information coming from the transport layer.

In this mode only the payload part of the information is protected. The addressing and the routing information is not protected.

Tunnel Mode



In tunnel mode, IPSec protects the entire IP packet. It takes an IP packet, including the header, applies IPSec security methods to the entire packet, and then adds a new IP header.

IPSec in tunnel mode protects the original IP header.

In this mode both the payload and The addressing information is protected.

Tunnel mode provides more security than transport mode.

Modes of operations in Authentication Header:

There are two modes in the authentication header

Authentication Header Transport Mode:

Authentication Header Tunnel Mode:

Authentication Header Transport Mode: In the authentication header transport mode, it is lies between the original IP Header and IP Packets original TCP header.

Authentication Header Tunnel Mode: In this authentication header tunnel mode, the original IP packet is authenticated entire and the authentication header is inserted between the original IP header and new outer IP header. Here, the inner IP header contains the ultimate source IP address and destination IP address. whereas the outer IP header contains different IP address that is IP address of the firewalls or other security gateways.

12. What is Network Management Security? Explain SNMP V3.

Ans. Network Management Security: It refers to the measures and protocols in place to secure the management and monitoring of network devices and infrastructure. The goal is to protect the confidentiality, integrity, and availability of network management data and ensure that only authorized individuals can access and control network devices. This is crucial for preventing unauthorized access,

configuration changes, and potential security breaches in network management systems.

One commonly used protocol for network management is SNMP (Simple Network Management Protocol). SNMP allows for the monitoring and management of network devices such as routers, switches, and servers. To enhance security, SNMP Version 3 (SNMPv3) was developed with improved authentication and encryption features.

SNMP Version 3 (SNMPv3):

SNMPv3 addresses the security shortcomings of earlier versions (SNMPv1 and SNMPv2) by introducing robust security features. Here are key elements of SNMPv3 security:

1. Authentication:
   - SNMPv3 provides strong user authentication using the HMAC (Hashed Message Authentication Code) algorithm. This ensures that the messages exchanged between the SNMP manager and the managed devices are not tampered with during transmission.
2. Authorization:
   - SNMPv3 introduces the concept of user-based security models (USM). Users are authenticated and assigned specific roles or access rights. This allows for fine-grained control over who can access and manage different aspects of the network.
3. Encryption:
   - To address the confidentiality of SNMP messages, SNMPv3 supports encryption. The data payload of SNMP messages can be encrypted using protocols

like DES (Data Encryption Standard) or AES (Advanced Encryption Standard), adding a layer of privacy to the communication.

4. Message Integrity:

- SNMPv3 ensures the integrity of messages through the use of the HMAC algorithm. This prevents unauthorized alterations to SNMP messages, ensuring that the data received by the SNMP manager is the same as what was sent by the managed device.

5. View-Based Access Control:

- SNMPv3 introduces View-Based Access Control Model (VACM), allowing administrators to define what portions of the MIB (Management Information Base) can be accessed or modified by specific users or groups. This adds another layer of control over the SNMP operations.

6. Security Levels:

- SNMPv3 defines three security levels: noAuthNoPriv (no authentication and no privacy), authNoPriv (authentication without privacy), and authPriv (authentication with privacy). Network administrators can choose the appropriate security level based on their specific security requirements.

13. Explain IDS and its types in detail.

Ans. An Intrusion Detection System (IDS) is a security technology that monitors network or system activities for signs of unauthorized access, security breaches, or malicious activities. It serves as an essential component of cybersecurity infrastructure.

Advantages of IDS in general:

Early detection of suspicious or malicious activities, allowing for a rapid response to potential threats.

Helps in identifying patterns and trends in attacks, aiding in the development of more robust security measures.

Provides valuable forensic data for investigating security incidents.

Disadvantages of IDS in general:

False positives can occur, where normal activities are flagged as suspicious, leading to unnecessary alerts.

False negatives are also possible, where actual attacks go undetected.

Maintenance and tuning can be time-consuming, requiring continuous updates to stay effective against evolving threats.

There main types of Intrusion Detection Systems are :

1. Network-based Intrusion Detection System (NIDS):

NIDS monitors network traffic in real-time. It analyzes data packets passing through a network and identifies suspicious or unauthorized activity based on predefined patterns or signatures.

- Advantages:
  - Provides visibility into the entire network, making it suitable for detecting attacks across multiple systems.
  - Can identify abnormal patterns or known attack signatures, offering a high level of accuracy.
- Disadvantages:
  - May not detect attacks on individual hosts or systems that aren't directly monitored by the network.
  - Vulnerable to encrypted traffic, as it can't inspect the contents of encrypted packets.

2. Host-based Intrusion Detection System (HIDS):

- Description: HIDS is installed on individual hosts (computers or servers) and monitors activities specific to that host, including system logs, file integrity, and application behavior.

- Advantages:

  - Provides detailed information about activities on a specific host, making it effective for identifying insider threats or attacks targeting a specific system.

  - Can monitor local activity even if the network is compromised.

- Disadvantages:

  - May have a higher false positive rate due to variations in system behavior and configurations.

  - Requires installation and maintenance on each host, which can be

3. Protocol-based Intrusion Detection System (PIDS) is a type of Intrusion Detection System (IDS) that focuses on monitoring network traffic for deviations from established protocol standards. It looks for anomalies or violations in the way network protocols are used, which can indicate potential security threats.

Advantages of Protocol-based Intrusion Detection System (PIDS):

- Early Detection: It can identify suspicious behavior or deviations from standard protocols, allowing for early detection of potential threats.

- Protocol-specific Analysis: PIDS is specialized in analyzing specific network protocols, providing a focused approach to identifying anomalies.

Disadvantages of Protocol-based Intrusion Detection System (PIDS):

- Limited Scope: PIDS primarily focuses on monitoring protocol compliance, which may not detect more sophisticated or non-standard attacks.

- False Positives: It may generate false alarms if legitimate traffic exhibits unusual behavior due to network changes or configurations.

- Dependent on Protocol Knowledge: PIDS requires a deep understanding of specific protocols, making it less suitable for organizations with diverse or complex network environments.

4. Application Protocol-based Intrusion Detection System (APIDS) monitors network traffic to detect anomalies in application-layer protocols. It focuses on identifying suspicious behavior within specific applications, enhancing security at a more granular level.

Advantages:

- Targets application-layer vulnerabilities
- Offers detailed insights into application-specific threats

Disadvantage:

Limited to application-layer monitoring, potentially missing lower-level or non-application-specific attacks.

14. Define Malware. Explain at least five types with examples.

Ans. Malware, short for malicious software, refers to any software intentionally designed to cause harm, damage, or exploit computer systems, networks, or user devices. Malware encompasses a wide range of malicious programs, including viruses, worms, Trojans, ransomware, and spyware, each with distinct characteristics and purposes.

Types of Malware:

1. Virus:

- Definition: A virus is a self-replicating program that attaches itself to legitimate software or files. When the infected program is executed, the virus spreads to other programs and may damage or corrupt data.

- Example: The "ILOVEYOU" virus in 2000 spread via email and affected millions of Windows computers by overwriting files and stealing sensitive information.

2. Worm:

- Definition: A worm is a standalone, self-replicating program that does not require a host file. It spreads across networks and devices, exploiting vulnerabilities to replicate and carry out malicious activities.

- Example: The "Conficker" worm in 2008 propagated through network shares and USB drives, infecting millions of Windows systems and creating a botnet.

3. Trojan Horse:

- Definition: A Trojan horse disguises itself as legitimate software but contains malicious code. Unlike viruses, Trojans do not replicate on their own but often serve as a means for other malware to enter a system.

- Example: The "Zeus" Trojan is known for stealing banking credentials by injecting malicious code into the web browsers of infected users.

4. Ransomware:

- Definition: Ransomware encrypts a user's files, rendering them inaccessible, and demands a ransom for their release. It often spreads through malicious email attachments, compromised websites, or other deceptive means.

- Example: The "WannaCry" ransomware in 2017 exploited a Windows vulnerability to infect and encrypt files on a global scale, affecting organizations and individuals.

5. Spyware:

- Definition: Spyware is designed to secretly gather and transmit user information, such as keystrokes, browsing habits, and personal data, without the user's knowledge or consent.

- Example: The "FinFisher" spyware is known for its ability to monitor and record user activities, including capturing screenshots and logging keystrokes, for surveillance purposes.

15. A secure e-voting system is to be designed. Discuss the security goals that must be met and enlist mechanisms for the same.

Ans. Designing a secure e-voting system involves addressing various security goals to ensure the integrity, confidentiality, authenticity, and availability of the voting process. Here are key security goals and mechanisms to achieve them:

1. Integrity:
   - Goal: Ensure that votes are accurately cast and counted without any unauthorized tampering.
   - Mechanisms:
     - End-to-End Verifiable (E2E) Encryption: Encrypt votes from the voter's device to the central server, ensuring that only authorized parties can decrypt and verify the contents.
     - Hash Functions: Use cryptographic hash functions to create unique fingerprints (hashes) of votes, making it difficult for attackers to alter the data without detection.
     - Blockchain Technology: Implement a blockchain-based system where votes are recorded in a tamper-evident and transparent manner.
2. Confidentiality:
   - Goal: Protect the secrecy of individual votes to prevent coercion or vote selling.
   - Mechanisms:

- End-to-End Encryption: Encrypt votes in transit and at rest, ensuring that only authorized entities (voters and election officials) can decrypt and access the vote information.

- Anonymous Credentials: Use cryptographic techniques to provide voters with credentials that allow them to cast a vote without revealing their identity.

3. Authenticity:

- Goal: Ensure that each vote is cast by an eligible and authenticated voter.

- Mechanisms:

- Multi-Factor Authentication (MFA): Implement strong authentication methods, such as biometrics or one-time passwords, to verify the identity of voters.

- Voter Registration: Maintain a secure and accurate voter registration database to verify eligibility before allowing voters to cast their ballots.

- Digital Signatures: Require voters to digitally sign their ballots, providing a verifiable proof of the authenticity of their votes.

4. Availability:

- Goal: Ensure that the e-voting system remains operational and accessible throughout the voting period.

- Mechanisms:

- Redundancy and Failover: Implement redundant servers and failover mechanisms to ensure continuous availability, even in the face of hardware failures or network issues.

- Distributed Denial of Service (DDoS) Mitigation: Employ DDoS protection mechanisms to prevent or mitigate attacks that could disrupt the availability of the e-voting system.

5. Non-Coercibility:

- Goal: Protect voters from coercion or intimidation by ensuring that they can cast their votes freely.

- Mechanisms:

  - Receipt-Free Voting: Design the system so that voters cannot prove how they voted, preventing them from providing evidence to coercive entities.

  - Voter Anonymity: Implement mechanisms to dissociate votes from individual voters, making it challenging for external parties to verify individual voting choices.

6. Auditability:

- Goal: Enable independent verification and auditing of the election results.

- Mechanisms:

  - Voter-Verifiable Paper Audit Trail (VVPAT): Provide a paper record for each vote that voters can review, ensuring a physical audit trail for verification.

  - Open Source Software: Use open-source software for the e-voting system to allow scrutiny by the public and security experts, enhancing transparency and trust.

7. Resilience Against Insider Threats:

- Goal: Guard against malicious actions from individuals with insider access.

- Mechanisms:

  - Access Controls: Implement strict access controls to limit the privileges of election officials and system administrators.

  - Regular Security Audits: Conduct regular security audits and penetration testing to identify and address potential vulnerabilities.

16. Enlist properties & applications of Hash function.

Ans. A Hash Function is a function that converts a given numeric or alphanumeric key to a small practical integer value. The mapped integer value is used as an index in the hash table. In simple terms, a hash function maps a significant number or string to a small integer that can be used as the index in the hash table.
There are many hash functions that use numeric or alphanumeric keys. This article focuses on discussing different hash functions:
Division Method.
Mid Square Method.
Folding Method.
Multiplication Method.
Data Integrity:

Properties of Hash Functions:

1. Deterministic: A hash function is deterministic, meaning that for a given input, it will always produce the same hash value.
2. Fixed Output Size: Hash functions produce a fixed-size output, regardless of the size of the input data.
3. Efficient to Compute: Hash functions should be computationally efficient to calculate the hash value for any input.
4. Preimage Resistance: It should be computationally infeasible to determine the original input from its hash value.
5. Second Preimage Resistance: Given an input, it should be computationally infeasible to find another input that produces the same hash value.

Applications of Hash Functions:

1. Data Integrity: Hash functions are widely used to ensure the integrity of data. By comparing hash values before and after data transmission or storage, one can verify whether the data has been altered.

2. Password Storage: Hash functions are employed to securely store passwords. Instead of storing actual passwords, systems store their hash values. During login attempts, the system hashes the entered password and compares it with the stored hash.
3. Digital Signatures: Hash functions play a crucial role in digital signatures. A hash of the message is signed with a private key, and the recipient can verify the signature using the sender's public key.
4. Blockchain Technology: In blockchain, hash functions are used to link blocks together. The hash of a block is included in the next block, creating a chain that ensures the integrity of the entire transaction history.
5. Cryptographic Applications: Hash functions are essential in various cryptographic protocols and algorithms, including HMAC (Hash-based Message Authentication Code) for secure message authentication.

17. Describe different types of Denial of service attacks

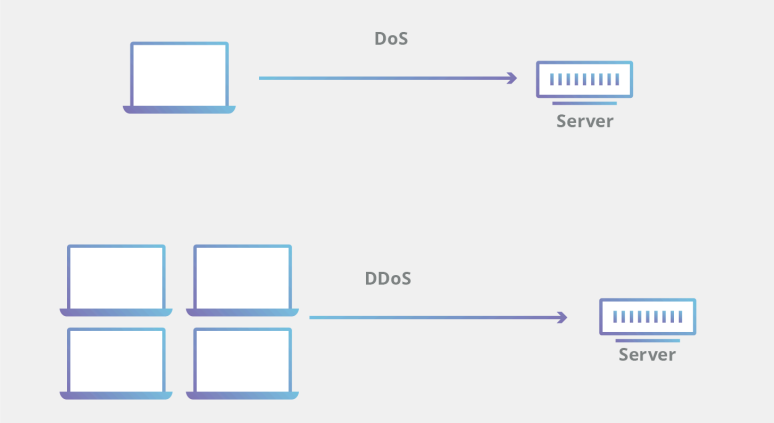
Ans. Denial of Service (DoS) attacks aim to disrupt or deny access to legitimate users by overwhelming a target system with a flood of illegitimate requests or traffic. There are various types of DoS attacks, each with its own method of achieving the goal of rendering a system or network unavailable. Here are some common types:

1. Ping Flood:

- Description: Attackers flood a target system with ICMP echo request (ping) messages.
- Impact: Consumes the target's bandwidth and resources, leading to network unresponsiveness.

2. SYN/ACK Flood:

- Description: Exploits the TCP three-way handshake by sending a large number of SYN requests without completing the handshake.



- Impact: Exhausts server resources, preventing it from establishing legitimate connections.

3. UDP Flood:

- Description: Overwhelms a target system with a flood of UDP packets, often using spoofed source IP addresses.

- Impact: Consumes bandwidth and may overload processing capacity, causing network or service disruptions.

4. HTTP/HTTPS Flood:

- Description: Floods a web server with a large volume of HTTP or HTTPS requests.

- Impact: Overloads the server, leading to slow response times or service unavailability for legitimate users.

5. DNS Amplification:

- Description: Exploits open DNS resolvers to amplify the volume of traffic directed at the target by sending small DNS queries with a spoofed source IP address.

- Impact: Causes a significant increase in traffic to the target, potentially leading to network congestion.

6. Smurf Attack:

- Description: Abuses ICMP to flood a target network with broadcast ping requests, with the source IP address spoofed to that of the victim.

- Impact: Results in a large number of responses being sent to the victim's IP address, overwhelming its resources.

7. Ping of Death:

- Description: Sends oversized or malformed ICMP packets to a target, exploiting vulnerabilities in the target's network stack.

- Impact: Causes the target system to crash or become unresponsive.

18. How is security achieved in the transport & tunnel methods of IPSEC? Describe the role of AH & ESP.

Ans.

19. Explain classical encryption techniques with example

Ans. Classical encryption techniques refer to historical methods of encrypting information that were developed before the advent of modern cryptographic algorithms. These techniques are generally considered to be less secure compared to contemporary cryptographic methods and are primarily of historical interest. Here are two classical encryption techniques:

1. Caesar Cipher:

Description:

The Caesar Cipher, named after Julius Caesar, is a substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet.

Example:

Let's use a shift of 3. The plaintext "HELLO" would be encrypted as follows:

- Plaintext: H E L L O

- Shift by 3: K H O O R

- Ciphertext: K H O O R

In this example, each letter is shifted three positions to the right in the alphabet. To decrypt, the process is reversed by shifting each letter three positions to the left.

2. Playfair Cipher:

Description:

The Playfair Cipher is a digraph substitution cipher that encrypts pairs of letters (digraphs) instead of single letters. It uses a key table to determine the digraph substitutions.

Example:

Consider the key "KEYWORD" and the plaintext "HELLO."

- Key Table:

  K E Y W O

  R D A B C

  F G H I L

  M N P Q S

  T U V X Z

- Plaintext: H E L L O

  HE -> EI

  LL -> LI

  LO -> OL

- Ciphertext: E I L I O

In this example, the letters "H" and "E" are replaced with "E" and "I" respectively, and so on.

20. In an RSA system, given N=91 e=5 Calculate Φ(n),p, q and private key d. What is the cipher text when you encrypt message m=25 using the public key. Also perform decryption.

Ans. In RSA encryption, the public key consists of the modulus N and the public exponent e, while the private key consists of the modulus N and the private exponent d. The totient (Euler's totient function), denoted as $\Phi(n)$, is a crucial value used in the key generation process. The totient is calculated using the prime factorization of N, where $N = p \times q$ for two prime numbers p and q.

Given $N = 91$ and $e = 5$, let's calculate the values:

1. **Calculate $\Phi(n)$:**

   $\Phi(n) = (p-1) \times (q-1)$

   We don't know p and q yet, so let's find them first.

2. **Factorize N:**

   $91 = 7 \times 13$

   Now, we can calculate $\Phi(n)$:

   $\Phi(91) = (7-1) \times (13-1) = 6 \times 12 = 72$

3. **Find p and q:**

   $p = 7$, $q = 13$

4. **Calculate private key d:**
   $d \equiv e^{-1} \pmod{\Phi(n)}$

   Using the extended Euclidean algorithm or a modular inverse calculator, we find $d = 29$ since $5 \times 29 \equiv 1 \pmod{72}$.

Now, we have the public key $(N, e) = (91, 5)$ and the private key $(N, d) = (91, 29)$.

5. **Encrypt the Message:**
   $C \equiv M^e \pmod{N}$ where $M = 25$

   $C \equiv 25^5 \pmod{91}$

   Calculating $25^5 \equiv 15 \pmod{91}$

   So, the ciphertext $C = 15$.

6. **Decrypt the Message:**
   $M \equiv C^d \pmod{N}$

   $M \equiv 15^{29} \pmod{91}$

   Using modular exponentiation, we find $M \equiv 25 \pmod{91}$.

   Therefore, the decrypted message is $M = 25$.

In summary:

- $\Phi(n) = 72$
- $p = 7$, $q = 13$
- Private key $d = 29$
- Ciphertext $C = 15$
- Decrypted message $M = 25$

21. Write Short Notes on:

a. SSL protocol stack

Ans.

b. Compare and contrast AES and DES

Ans.

c. IDS and its types

Ans.

d. Use cases for NAC

Ans.

e. Digital Signature

Ans.

MODULE WISE DISTRIBUTION

Module 1:

1. **explain security services and mechanisms to implement it.**
2. **playfair cipher with eg**
3. **security goals and mechanism**

4. classical encryption technique with eg
5. transposition cipher
6. ARP

Module 2:

1. HMAC vs CMAC
2. Describe different block cipher modes
3. Kerberos protocol in detail
4. Properties and application of hash functions
5. RSA numerical
6. AES vs DES
7. drawbacks of DES
8. Explain digital signature and its significance
9. What is authentication
10. Diffie Hellman key exchange
11. Needham Schroeder protocol
12. PKI
13. KDC

Module 3:

1. Define Malware and explain any 5 types
2. Explain Denial of service attack

Module 4:

1. Explain SSH prottocol stack
2. Explain different types of protocol offered by SSL

3. Explain working of IPsec in its different modes
4. How is security achieved in transport and tunnel modes of ipsec
5. Describe the role of AH and ESP

Module 5:

1. Explain different NAC enforcement methods
2. What is NAC. Discuss different elements present in NAC
3. Principles and need of NAC
4. NAC use cases
5. Explain SNMPv3.
6. Explain network management security

Module 6:

1. State Firewall design principles and its types with advantages
2. Explain firewall and its types along with advantage and disadvantage
3. Explain IDS and its types

Short Note:

1. SSL
2. TSL
3. AES and DES
4. IDS
5. NAC
6. Digital signature
7. HMAC and CMAC
8. ARP spoofing

9. Port scanning
10. Honeypot
11. El Gamal Algo
12. Session Hijack
13. Email Security
14. IPsec
15. PKI
16. KDC
17. ARP