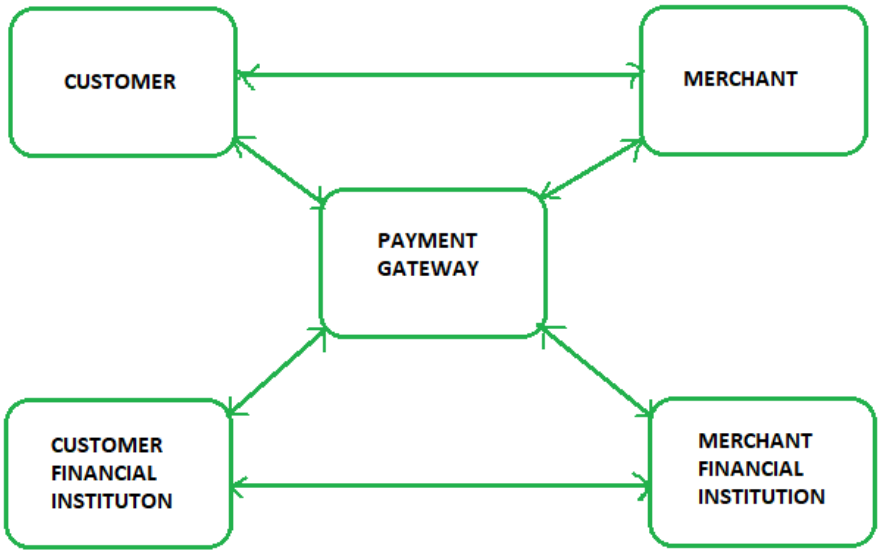
Practice sheet 4

Answers

1. How Secure Electronic Transaction (SET) Protocol enhance the online payment security.
   Ans :- Secure Electronic Transaction or SET is a system that ensures the security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied to those payments. It uses different encryption and hashing techniques to secure payments over the internet done through credit cards.
   SET protocol restricts the revealing of credit card details to merchants thus keeping hackers and thieves at bay. The SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.



Requirements in SET:

1. Mutual Authentication:
   - Customer authentication to confirm if they are the intended user.
   - Merchant authentication to verify their identity.
2. Confidentiality:
   - Protection of Payment Information (PI) and Order Information (OI) through encryption.
3. Integrity:

- Resistance against message modifications to ensure that transmitted content remains unchanged.

4. Interoperability:
    - Compatibility with various systems and adherence to established standards to facilitate seamless transactions.
5. Utilization of Best Security Mechanisms:
    - Implementation of robust security measures to ensure the highest level of protection for online transactions.

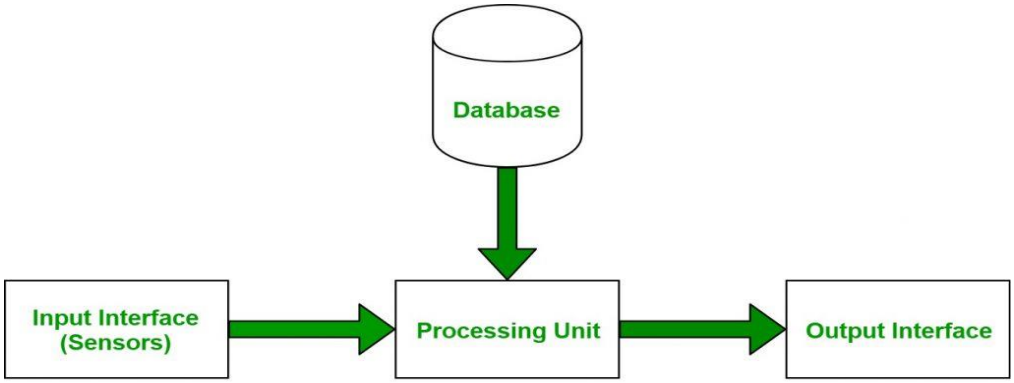
Participants in SET:

1. Cardholder: The customer making the purchase.
2. Issuer: The financial institution that issued the card to the customer.
3. Merchant: The entity selling goods or services online.
4. Acquirer: The financial institution that processes the payment on behalf of the merchant.
5. Certificate Authority: An authority that follows specific standards and issues certificates (such as X.509V3) to all participants involved in the SET protocol.

Working of SET:

- SET protocols use digital certificates to securely access funds for online purchases.
- Each transaction generates encrypted certificates for the merchant, financial institution, and customer.
- Digital keys verify the transaction, ensuring only authorized participants confirm it.
- SET algorithms protect customers' card details from online threats.
- Overall, SET ensures secure electronic transactions, safeguarding sensitive payment information.

2. Elaborate the working and types of Biometric authentication.
   Ans:- Biometrics is measure of biological or behavioral features which are used for identification of individuals. Most of these features are inherit and cannot be guessed or stolen.



Biometric System

It is a system that takes an individual's physiological, behavioral or both traits as input, analyzes it and identifies the individual as legitimate or malicious user.

Working of Biometric Authentication:

1. **Enrollment**: Capture biometric data and create a digital template.
2. **Storage**: Securely store the template for future comparison.
3. **Authentication**: Present biometric trait for comparison.
4. **Verification**: Compare presented data with stored template.
5. **Decision**: Grant or deny access based on the comparison result.

Types of Biometric Authentication:

1. **Fingerprint Recognition**: Unique patterns on fingertips.
2. **Iris Recognition**: Patterns in the iris of the eye.
3. **Facial Recognition**: Facial features and structures.
4. **Voice Recognition**: Unique characteristics of the voice.
5. **Palmprint Recognition**: Patterns on the palm of the hand.
6. **Behavioral Biometrics**: Patterns in behavior, like typing rhythm or gait.

3. Outline the need of Transport layer security and explain the Secure Socket Layer (SSL) protocol.

Ans :- **Need for Transport Layer Security (TLS):**

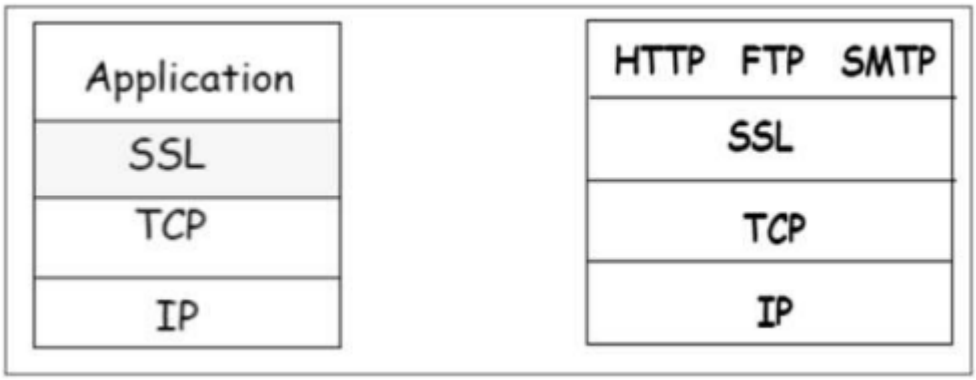
- **Confidentiality**: TLS encrypts data transmitted between clients and servers, preventing unauthorized parties from eavesdropping on sensitive information.
- **Data Integrity**: TLS ensures that data remains unchanged during transmission, preventing tampering or modification by malicious entities.
- **Authentication**: TLS verifies the identities of communicating parties, ensuring that clients are connecting to legitimate servers and vice versa.

- **Trust**: TLS relies on digital certificates issued by trusted Certificate Authorities (CAs) to establish trust between communicating parties, enhancing the security of the communication channel.

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 itself is not a single layer protocol as depicted in the image; in fact it is composed of two sub-layers.

 Lower sub-layer comprises of the one component of SSL protocol called as SSL Record Protocol. This component provides integrity and confidentiality services.

 Upper sub-layer comprises of three SSL-related protocol components and an application protocol. Application component provides the information transfer service between client/server interactions. Technically, it can operate on top of SSL layer as well. Three SSL related protocol components are –

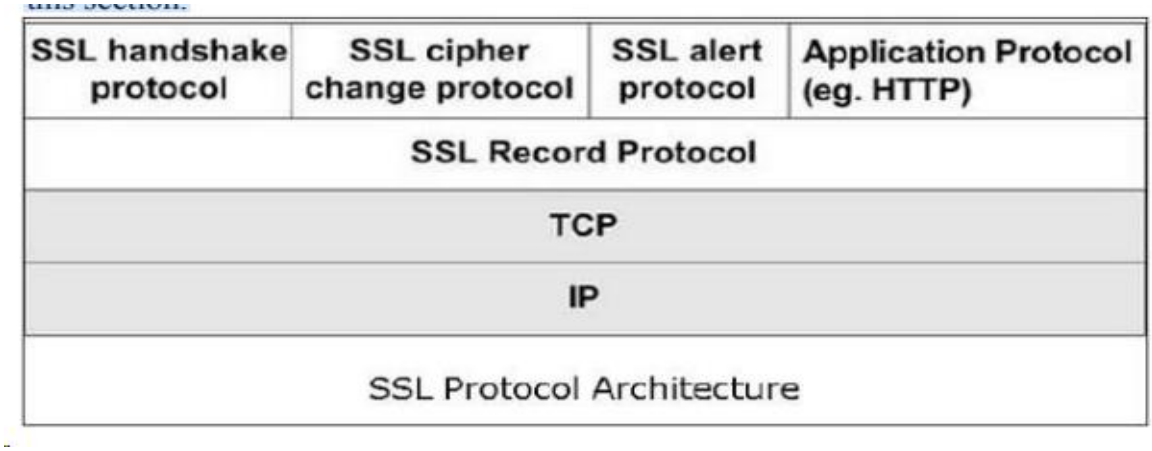
o SSL Handshake Protocol

o Change Cipher Spec Protocol

o Alert Protocol.

 These three protocols manage all of SSL message exchanges and are discussed later in

this section.



- SSL was the predecessor to TLS and served a similar purpose in securing communication over the internet.
- It employed encryption algorithms and digital certificates to establish secure connections between clients and servers.
- SSL operated at the application layer of the OSI model, providing a secure channel for protocols such as HTTP, SMTP, and FTP.
- However, due to vulnerabilities and security flaws identified in SSL, it has largely been deprecated in favor of newer TLS versions.

4. Discover the role of intrusion detection system (IDS) to analyses the network traffic and how it help to strengthen the security on network.

Ans :-

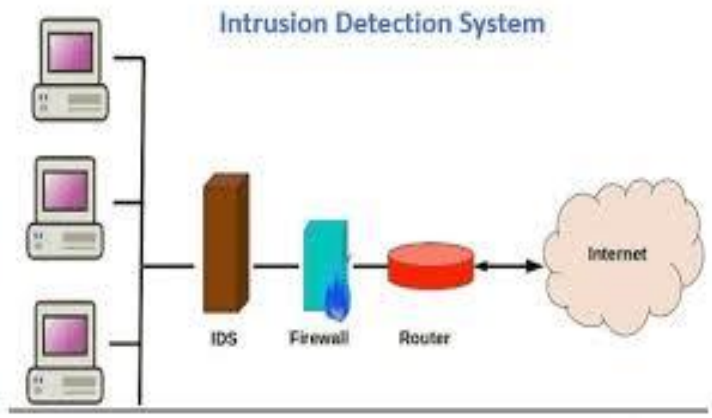
An Intrusion Detection System (IDS) maintains network traffic looks for unusual activity and sends alerts when it occurs. The main duties of an Intrusion Detection System (IDS) are anomaly detection and reporting, however, certain Intrusion Detection Systems can take action when malicious activity or unusual traffic is discovered. In this article, we will discuss every point about the Intrusion Detection System.

Classification of Intrusion Detection System(IDS)

Intrusion Detection System are classified into 5 types:

1. **Network Intrusion Detection System (NIDS)**:
   - Monitors traffic at planned points within the network.
   - Observes passing traffic on the entire subnet.
   - Matches traffic against known attacks and alerts administrators of anomalies.

2. **Host Intrusion Detection System (HIDS)**:
    - Runs on independent hosts or devices on the network.
    - Monitors incoming and outgoing packets from the device.
    - Alerts administrators if suspicious activity is detected, such as changes to system files.
3. **Protocol-based Intrusion Detection System (PIDS)**:
    - Resides at the front end of a server, controlling and interpreting the protocol between users/devices and the server.
    - Monitors specific protocols, such as HTTPS, to secure web servers.
4. **Application Protocol-based Intrusion Detection System (APIDS)**:
    - Resides within a group of servers.
    - Monitors and interprets communication on application-specific protocols, such as SQL, to detect intrusions.
5. **Hybrid Intrusion Detection System**:
    - Combines two or more approaches to IDS, such as host-based and network-based.
    - Integrates host agent or system data with network information to provide a comprehensive view of the network.
    - Example: Prelude is a Hybrid IDS.



Role of Intrusion Detection System (IDS) in Analyzing Network Traffic:

1. **Continuous Monitoring**: IDS continuously monitor network traffic, examining packets and data flows in real-time.
2. **Anomaly Detection**: IDS analyze network traffic patterns and behavior to identify deviations from normal or expected behavior. Any unusual activity is flagged as a potential security threat.
3. **Signature Detection**: IDS compare network traffic against a database of known attack signatures or patterns. If a match is found, it indicates the presence of a known threat or attack.
4. **Alert Generation**: When suspicious or malicious activity is detected, IDS generate alerts or notifications to alert administrators or security personnel. These alerts

include information about the nature of the threat, affected systems, and recommended response actions.

5. **Log Generation**: IDS create detailed logs of detected events, including information about the source and destination of network traffic, the type of attack or anomaly detected, and the timestamp of the event. These logs are valuable for forensic analysis and incident response.

How IDS Helps Strengthen Network Security:

1. **Early Threat Detection**: IDS provide early detection of security threats, allowing administrators to respond promptly before they escalate into full-blown attacks. This helps prevent or minimize potential damage to network resources and sensitive data.
2. **Reduced Dwell Time**: By quickly identifying and alerting on security incidents, IDS help reduce dwell time—the time between a security breach and its detection. This minimizes the window of opportunity for attackers to exploit vulnerabilities and carry out further attacks.
3. **Improved Incident Response**: IDS provide valuable information and context about security incidents, enabling administrators to take appropriate response actions. This may include isolating affected systems, blocking malicious traffic, or applying security patches and updates to mitigate vulnerabilities.
4. **Enhanced Situational Awareness**: IDS contribute to a better understanding of the network environment and potential security risks. By monitoring network traffic and analyzing patterns, IDS help administrators identify trends, emerging threats, and areas of vulnerability, allowing them to proactively strengthen security measures.
5. **Compliance and Regulatory Requirements**: Many regulatory standards and industry guidelines require organizations to implement intrusion detection systems as part of their security infrastructure. By deploying IDS, organizations can demonstrate compliance with these requirements and maintain a robust security posture.

5.Discussed the different Threats to Information Security.

Ans :- Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

1. **Malware**: Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. This includes viruses, worms, trojans, ransomware, and spyware.

2. **Phishing**: Cybercriminals use deceptive emails, messages, or websites to trick individuals into revealing sensitive information, such as passwords, credit card numbers, or personal details.
3. **Social Engineering**: Manipulating individuals or employees into divulging confidential information or performing actions that compromise security, often through impersonation or psychological manipulation.
4. **Denial-of-Service (DoS) Attacks**: Overwhelming a system, network, or website with a flood of traffic or requests, causing it to become inaccessible to legitimate users.
5. **Insider Threats**: Employees, contractors, or partners who misuse their access privileges to steal data, sabotage systems, or compromise security from within the organization.
6. **Data Breaches**: Unauthorized access to sensitive or confidential data, resulting in its disclosure, theft, or exposure to unauthorized parties.
7. **Advanced Persistent Threats (APTs)**: Sophisticated and targeted attacks by skilled adversaries with specific objectives, such as espionage, sabotage, or data theft, often involving multiple stages and prolonged periods of stealthy infiltration.
8. **Man-in-the-Middle (MitM) Attacks**: Intercepting and manipulating communication between two parties by an unauthorized third party, allowing them to eavesdrop on sensitive information or alter communication for malicious purposes.
9. **Zero-Day Exploits**: Security vulnerabilities in software or systems that are unknown to the vendor and have not been patched, allowing attackers to launch targeted attacks before a fix is available.
10. **Data Loss**: Accidental or intentional loss of sensitive or confidential data, often due to human error, hardware failures, or inadequate security measures.
11. **Unauthorized Access**: Gaining unauthorized access to systems, networks, or data, either through exploiting vulnerabilities, weak passwords, or bypassing security controls.
12. **Physical Threats**: Theft, vandalism, or damage to physical assets such as servers, computers, or storage devices, leading to loss of data or disruption of services.
13. **Supply Chain Attacks**: Targeting vulnerabilities in the supply chain, such as compromised hardware, software, or third-party services, to gain unauthorized access or compromise security.
14. **IoT Vulnerabilities**: Exploiting vulnerabilities in Internet of Things (IoT) devices, such as smart home appliances, medical devices, or industrial sensors, to gain unauthorized access to networks or data.

6. How Smart Cards are use in security along with its uses and types.

Ans :- Smart cards provide ways to securely identify and authenticate the holder and third parties who want access to the card. For example, a cardholder can use a PIN code or biometric data for authentication. They also provide a way to securely store data on the card and protect communications with encryption.

Smart cards are highly secure portable devices that store and process data for various security applications. Here's how they are used in security:

1. **Authentication**: Smart cards are widely used for user authentication in both physical and logical access control systems. Users authenticate themselves by presenting the smart card and, in some cases, entering a Personal Identification Number (PIN). This ensures that only authorized individuals can access secured resources or facilities.
2. **Digital Signatures**: Smart cards can generate and store cryptographic keys used for digital signatures. This enables users to sign electronic documents or transactions securely, ensuring their integrity and authenticity.
3. **Data Storage**: Smart cards have onboard memory that can securely store sensitive information such as personal identification details, medical records, or financial data. This data is protected by encryption and can only be accessed with the appropriate authentication credentials.
4. **Payment Transactions**: Smart cards, particularly contactless ones like EMV (Europay, Mastercard, and Visa) cards, are widely used for secure payment transactions. They store payment credentials and use encryption to securely communicate with payment terminals, reducing the risk of fraud and unauthorized access to payment information.

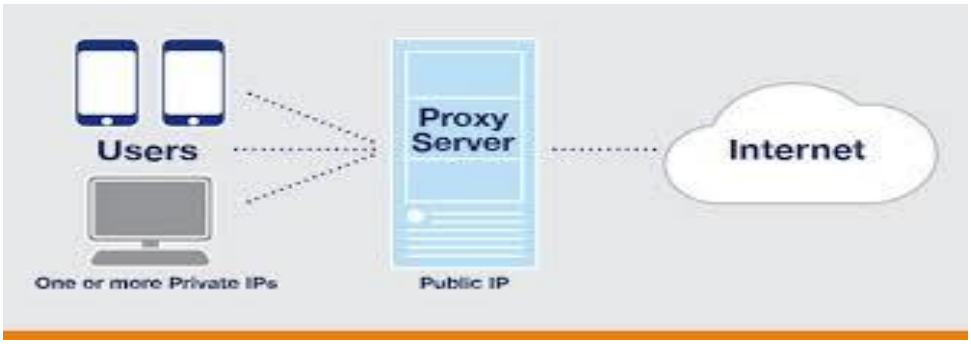
Types of Smart Cards:

1. **Contact Smart Cards**: Require physical contact with a card reader to transmit data. They contain a microprocessor and memory chip, enabling secure storage and processing of information.
2. **Contactless Smart Cards**: Utilize radio frequency identification (RFID) or near-field communication (NFC) technology to communicate wirelessly with card readers. They are convenient for quick transactions and are commonly used in payment cards and access control systems.
3. **Dual-Interface Smart Cards**: Combine both contact and contactless capabilities, allowing them to be used in a wide range of applications. They offer the flexibility of contactless communication while retaining compatibility with traditional contact-based systems.

Smart cards enhance security by providing strong authentication, secure storage of sensitive data, and cryptographic capabilities, making them indispensable in various security applications. Whether it's accessing secure facilities, signing digital documents, or making secure payments, smart cards play a crucial role in ensuring the integrity, confidentiality, and authenticity of transactions.

7. Explain the role of proxy servers in network security. How do they enhance privacy and

security?

Ans :- 

Proxy servers play a crucial role in enhancing network security and privacy by acting as intermediaries between clients and servers. Here's how they enhance privacy and security:

1. **Anonymity and Privacy**: Proxy servers hide the IP addresses of clients, making it difficult for websites and servers to track users' online activities. By masking users' IP addresses, proxy servers enhance anonymity and privacy, protecting users' identities and sensitive information from being exposed.

2. **Content Filtering and Access Control**: Proxy servers can filter and block access to websites or content based on predefined rules or policies. This allows organizations to enforce acceptable use policies, restrict access to inappropriate or malicious websites, and prevent users from accessing potentially harmful content. By filtering web traffic, proxy servers help prevent users from inadvertently accessing malicious websites or content.

3. **Caching and Performance Optimization**: Proxy servers can cache frequently accessed web content, such as web pages, images, and videos. By storing cached content locally, proxy servers reduce bandwidth usage, speed up access to web resources, and improve overall network performance for users. Additionally, caching helps mitigate the impact of distributed denial-of-service (DDoS) attacks by serving cached content during periods of high traffic or network congestion.

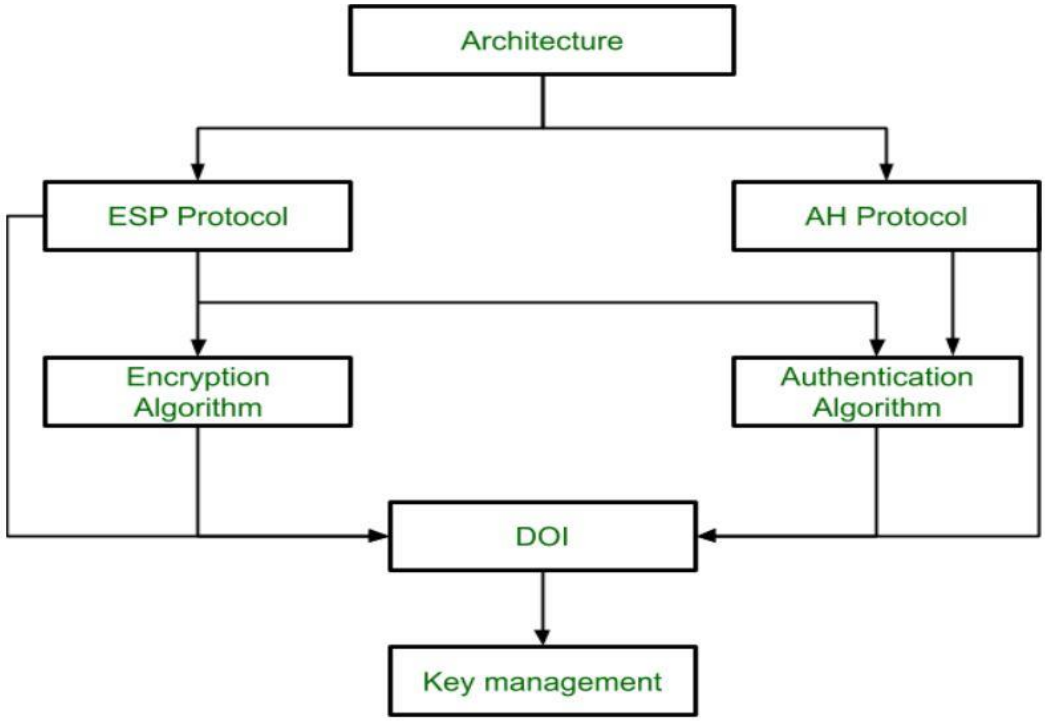
4. **Security and Intrusion Prevention**: Proxy servers can inspect incoming and outgoing traffic for malicious content, such as malware, viruses, or phishing attempts. They can block or quarantine suspicious traffic, preventing it from reaching users' devices and reducing the risk of security breaches or data loss. By acting as a gateway between clients and external servers, proxy servers provide an additional layer of defense against cyber threats and unauthorized access to sensitive information.

5. **Network Segmentation and Load Balancing**: Proxy servers can segregate network traffic into separate segments or routes, directing traffic to different destinations based on predefined criteria. This helps optimize network resources, balance traffic loads, and improve network efficiency and reliability. Additionally, proxy servers can distribute incoming traffic across multiple servers or network paths, reducing the risk of server overload or network congestion.

8. Explain the components of the IPsec protocol suite and its role in providing security at the network layer.

Ans :-

The IPsec (Internet Protocol Security) protocol suite consists of several components designed to provide security at the network layer (Layer 3) of the OSI model. Here are the main components of the IPsec protocol suite and their roles in enhancing network security:



1. **Authentication Header (AH)**:
    - Role: Provides data integrity, authentication, and anti-replay protection for IP packets.
    - Functionality: AH adds a header to the IP packet, including a cryptographic hash (authentication code) of the packet contents. This hash ensures that the packet has not been tampered with during transit and verifies the sender's identity. AH also includes a sequence number to prevent replay attacks.
2. **Encapsulating Security Payload (ESP)**:
    - Role: Provides confidentiality, data integrity, authentication, and anti-replay protection for IP packets.

- Functionality: ESP encrypts the payload of the IP packet to ensure confidentiality, protecting the data from eavesdropping by unauthorized parties. It also adds a header with authentication and integrity checks similar to AH, ensuring the integrity of the encrypted payload and verifying the sender's identity. ESP also includes a sequence number to prevent replay attacks.

3. **Security Associations (SA)**:
    - Role: Defines the security parameters and keys used for securing communication between two IPsec-enabled devices.
    - Functionality: A Security Association is established between two communicating devices to negotiate security parameters such as encryption algorithms, authentication methods, and key management protocols. Each SA is uniquely identified by a Security Parameter Index (SPI) and is associated with a specific security protocol (AH or ESP), encryption algorithm, authentication method, and key.
4. **Key Management Protocol**:
    - Role: Facilitates the secure exchange and management of cryptographic keys required for encryption, authentication, and integrity protection.
    - Functionality: Key management protocols such as Internet Key Exchange (IKE) or IKEv2 automate the negotiation, establishment, and refreshment of security associations between IPsec-enabled devices. These protocols use cryptographic techniques to securely exchange keys, authenticate communicating parties, and protect against key compromise or theft.

    The role of the IPsec protocol suite in providing security at the network layer is to ensure the confidentiality, integrity, authenticity, and anti-replay protection of IP packets transmitted over the network. By encrypting packet payloads, authenticating packet contents, and preventing replay attacks, IPsec helps mitigate various network security threats, such as eavesdropping, tampering, and impersonation. Additionally, IPsec enables secure communication between network devices, ensuring that sensitive information remains protected from unauthorized access or interception. Overall, IPsec plays a crucial role in enhancing network security by providing a comprehensive framework for securing IP-based communication in both private and public networks.

9. Explain the use of smart cards in enhancing security in various applications, including authentication and access control.

Ans :- Smart cards play a significant role in enhancing security across various applications, particularly in authentication and access control. Here's how smart cards contribute to enhancing security in these areas:

1. **Authentication**:
    - **Two-Factor Authentication (2FA)**: Smart cards are often used as part of a two-factor authentication system, where users must present both something they know (e.g., a PIN) and something they have (the smart card) to access a system or service. This adds an extra layer of security beyond just passwords.
    - **Strong Authentication**: Smart cards store cryptographic keys and certificates, enabling strong authentication mechanisms. These keys are used to verify the identity of the cardholder, ensuring that only authorized users can access protected resources.
    - **Mutual Authentication**: Smart cards support mutual authentication, where both the card and the reader authenticate each other. This prevents unauthorized devices from communicating with the smart card and helps mitigate man-in-the-middle attacks.
2. **Access Control**:
    - **Physical Access Control**: Smart cards are widely used for physical access control to buildings, facilities, and secure areas. Employees or users must present their smart cards to access entry points equipped with card readers. This ensures that only authorized individuals can enter restricted areas.
    - **Logical Access Control**: In IT environments, smart cards are used for logical access control to computers, networks, and sensitive data. Users must insert their smart cards into card readers or authenticate wirelessly using contactless smart card technology to access their devices or log into systems. This helps prevent unauthorized access to critical information and systems.
    - **Role-Based Access Control (RBAC)**: Smart cards support RBAC by storing user credentials, permissions, and role information. Access rights can be assigned to specific users based on their roles, and smart cards enforce these permissions when users attempt to access resources or perform actions.
3. **Secure Transactions**:
    - Smart cards enable secure transactions in various applications, including banking, e-commerce, and electronic payments. They securely store payment credentials, such as credit card numbers or digital cash, and facilitate secure transactions using encryption and authentication mechanisms. This protects sensitive financial information and prevents unauthorized access or fraud.
4. **Data Protection**:
    - Smart cards can store sensitive data securely, such as encryption keys, digital certificates, and personal information. The data stored on smart cards is encrypted and protected by access control mechanisms, preventing unauthorized access or tampering.

Overall, smart cards enhance security in various applications by providing strong authentication, access control, secure transactions, and data protection capabilities. Their versatility and cryptographic capabilities make them valuable tools for protecting sensitive information and ensuring secure access to resources in both physical and digital environments.

10. Explain the Security in Wireless Communication and its protocols.

Ans :- Security in wireless communication is essential to protect data transmitted over wireless networks from interception, tampering, and unauthorized access. Several protocols and mechanisms are employed to ensure the security of wireless communication. Here's an overview:

1. **Wi-Fi Protected Access (WPA/WPA2/WPA3)**:
    - WPA and WPA2 are security protocols used to secure Wi-Fi networks. They use encryption (e.g., TKIP or AES) to protect data transmitted over the network and implement authentication mechanisms (e.g., Pre-Shared Key or 802.1X/EAP) to verify the identity of users or devices.
    - WPA3 is the latest version of the Wi-Fi Protected Access protocol, introducing stronger encryption (e.g., forward secrecy) and security enhancements to mitigate common attack vectors.
2. **IEEE 802.11i (WPA2-Enterprise)**:
    - WPA2-Enterprise, based on the IEEE 802.11i standard, provides more robust security for Wi-Fi networks by using the Extensible Authentication Protocol (EAP) framework for authentication. It allows for centralized authentication and dynamic key generation, enhancing security in enterprise environments.
3. **Virtual Private Networks (VPNs)**:
    - VPNs create secure, encrypted tunnels over public networks, such as the Internet, to transmit data securely between remote users and corporate networks. VPN protocols like IPsec (Internet Protocol Security) and SSL/TLS (Secure Sockets Layer/Transport Layer Security) are commonly used to establish secure VPN connections.
4. **Transport Layer Security (TLS) and Secure Sockets Layer (SSL)**:
    - TLS and SSL are cryptographic protocols used to secure communication over the Internet. They provide encryption and authentication between client-server applications, ensuring that data transmitted between them is secure and protected from eavesdropping or tampering.

5. **Bluetooth Security**:
    - Bluetooth devices implement security features such as pairing, encryption, and authentication to ensure secure communication between devices. Bluetooth protocols like Secure Simple Pairing (SSP) and Bluetooth Secure Connections (LESC) enhance security and privacy in Bluetooth communication.

6. **Secure Shell (SSH)**:
    - SSH is a protocol used for secure remote login and command execution over a network. It provides strong encryption and authentication mechanisms to protect data transmitted between client and server systems.
7. **End-to-End Encryption (E2EE)**:
    - E2EE ensures that data is encrypted on the sender's device and decrypted only on the recipient's device, preventing intermediate parties from accessing plaintext data. Messaging apps and communication platforms often implement E2EE to protect user privacy and confidentiality.

These security protocols and mechanisms play a crucial role in safeguarding wireless communication, ensuring the confidentiality, integrity, and authenticity of data transmitted over wireless networks. By implementing robust security measures, organizations and individuals can mitigate the risks associated with wireless communication and protect sensitive information from unauthorized access or interception.

11. Identify and discuss common threats in computer networks, including malware, phishing, and denial-of-service attacks.

Ans :- Common threats in computer networks pose significant risks to data security, system integrity, and user privacy. Here's a discussion on three prevalent threats: malware, phishing, and denial-of-service (DoS) attacks:

1. **Malware**:
    - **Definition**: Malware, short for malicious software, refers to any software designed to infiltrate, damage, or gain unauthorized access to computer systems or networks.
    - **Types**: Malware includes viruses, worms, trojans, ransomware, spyware, adware, and rootkits, each with distinct characteristics and attack vectors.

- **Behavior**: Malware can corrupt or delete files, steal sensitive information, exploit system vulnerabilities, disrupt system operations, or turn infected devices into bots for botnet attacks.
- **Propagation**: Malware spreads through various vectors, including email attachments, malicious websites, infected removable media, software vulnerabilities, and social engineering tactics.
- **Prevention**: Preventive measures against malware include using antivirus software, keeping software and operating systems up to date with security patches, exercising caution when downloading files or clicking on links, and implementing network security measures such as firewalls and intrusion detection systems.

2. **Phishing**:
    - **Definition**: Phishing is a social engineering attack where attackers masquerade as legitimate entities to deceive individuals into disclosing sensitive information, such as usernames, passwords, credit card numbers, or personal details.
    - **Techniques**: Phishing attacks commonly involve fraudulent emails, text messages, or websites that mimic trusted organizations or individuals, tricking users into providing confidential information.
    - **Objectives**: Phishing attacks aim to steal personal information, financial credentials, or login credentials for unauthorized access to accounts or systems.
    - **Indicators**: Phishing emails often contain urgent or enticing messages, grammatical errors, suspicious links, or requests for sensitive information.
    - **Prevention**: Preventive measures against phishing include user education and awareness training, implementing email filtering and anti-phishing tools, verifying the legitimacy of websites and email senders, and enabling multi-factor authentication for account logins.
3. **Denial-of-Service (DoS) Attacks**:
    - **Definition**: DoS attacks aim to disrupt or degrade the availability of network services or resources, rendering them inaccessible to legitimate users.
    - **Types**: DoS attacks include flooding attacks (e.g., SYN flood, UDP flood), resource depletion attacks (e.g., ping of death, buffer overflow), and application layer attacks (e.g., HTTP flood, DNS amplification).
    - **Impact**: DoS attacks can overload network bandwidth, exhaust system resources, crash servers, or disrupt critical services, resulting in downtime, financial losses, and reputational damage.

- **Motivations**: Attackers may launch DoS attacks for various reasons, including extortion, revenge, political activism, competitive advantage, or disruption of services.
- **Prevention**: Preventive measures against DoS attacks include implementing network firewalls, intrusion detection and prevention systems (IDPS), rate limiting, traffic filtering, and employing content delivery networks (CDNs) or DoS protection services.

Overall, mitigating these common threats requires a multi-layered approach, including robust security measures, user education, and proactive monitoring to safeguard computer networks and mitigate potential risks.