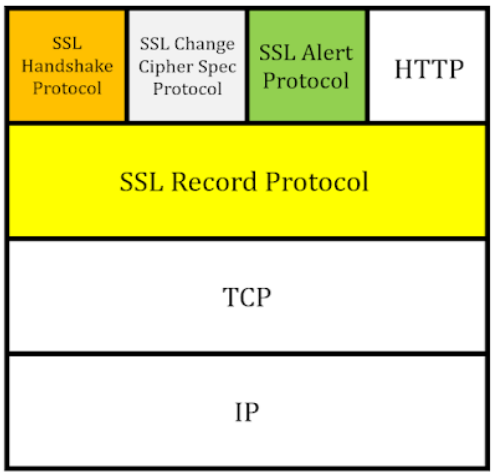
Explain SSL Architecture

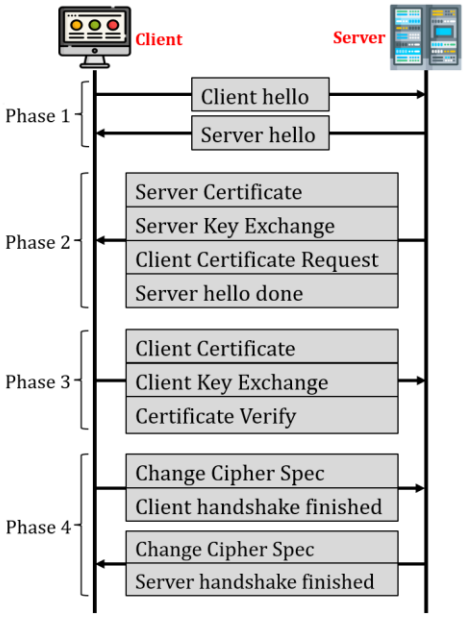
- Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

- SSL is a two layered protocol which was designed to make use of TCP to provide a reliable end-to-end secure service. SSL communicates using the Transport Control Protocol (TCP).
- The term "socket" in SSL refers to the method of sending data via a network between a client and a server.
- A Web server requires an SSL certificate to establish a secure SSL connection while using SSL for safe Internet transactions.
- SSL is works in between application layer and transport layer the reason SSL is also called TLS (Transport Layer Security).



SSL 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.



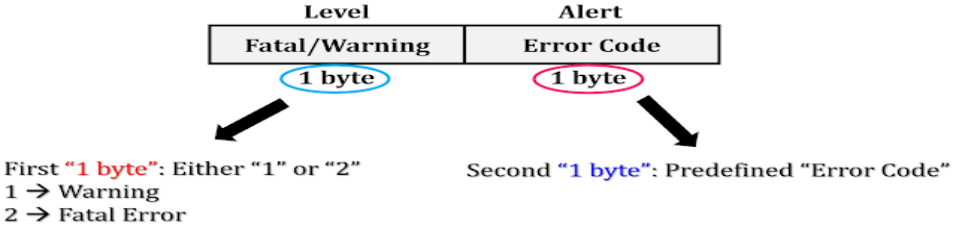
Change-cipher spec Protocol :

- SSL Change Cipher Spec Protocol is upper layer protocol. It is the simplest protocol. This protocol consists of only single byte with value "1", as shown in figure.

- This protocol's purpose is to cause the pending state to be copied into the current state.

SSL Alert Protocol :

- SSL uses the Alert protocol for reporting error that is detected by client or server, the party which detects error sends an alert message to other party.
- If error is serious than both parties terminate the session. Figure Shows Alert Protocol Format :



SSL Record Protocol :

- SSL record protocol is second sub-protocol of SSL also called lower-level protocol.

- SSL Record provides two services to SSL connection.
  1. Confidentiality
  2. Message Integrity
- SSL record protocol is responsible for encrypted data transmission and encapsulation of the data sent by the higher layer protocols also to provide basic security services to higher layer protocols.
- After that encryption of the data is done and in last SSL header is appended to the data.

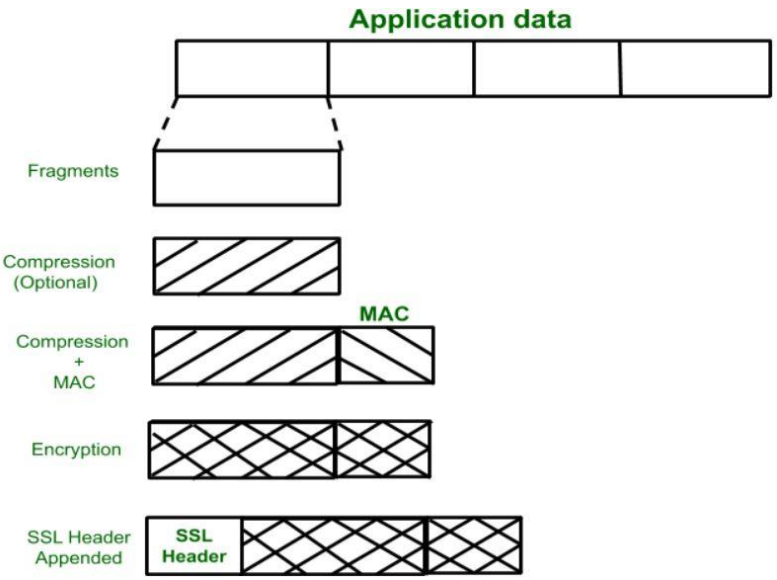


Figure: SSL Reccord Protocol Operation

Explain SSL Record Protocol ?

- 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.

- SSL is a two layered protocol which was designed to make use of TCP to provide a reliable end-to-end secure service. SSL communicates using the Transport Control Protocol (TCP).

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

SSL record protocol :

- SSL record protocol is second sub-protocol of SSL also called lower-level protocol.
- SSL Record provides two services to SSL connection.
    1. **Confidentiality -** This can be achieved by using secret key, which is already defined by handshake protocol.
    2. **Message Integrity** - The handshake protocol defines a shared secret key that is used to assure the message integrity.
- SSL record protocol is responsible for encrypted data transmission and encapsulation of the data sent by the higher layer protocols also to provide basic security services to higher layer protocols.
- 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.

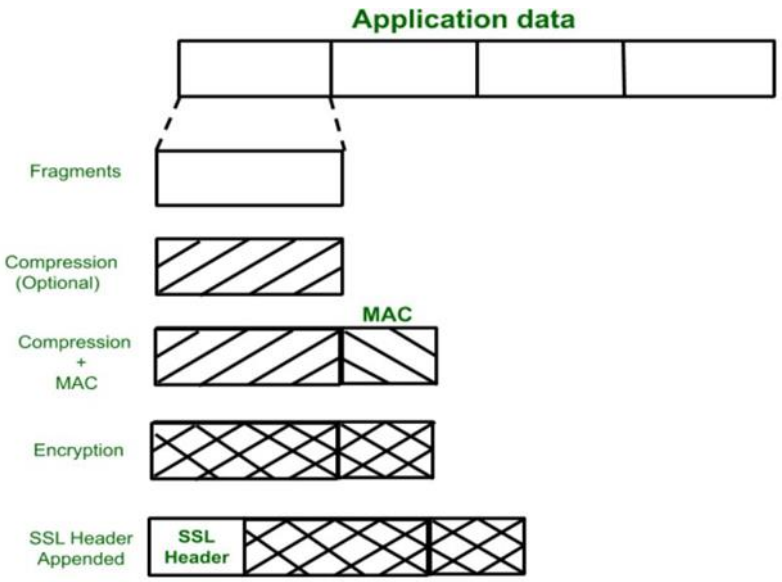
Following are the operation performed in Record protocol after connection is established and authentication is done of both client and server :

Fragmentation: The original message that is to be sent it broken into blocks. The size of each block is less than or equal to 214 bytes.
Compression: The fragmented blocks are compressed which is optional. It should be noted that the compression process must not result into loss of original data.

Addition of MAC: A short piece of information used to authenticate a message for integrity and assurance of message.

Encryption: The overall steps including message is encrypted using symmetric key but the encryption should not increase the overall block size.

Append Header: After all the above operation, header is added in the encrypted block which contains following fields.



Explain SSL Handshake Protocol ?

- 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.

- SSL is a two layered protocol which was designed to make use of TCP to provide a reliable end-to-end secure service. SSL communicates using the Transport Control Protocol (TCP).

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

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.
- Client Hello: The client initiates the handshake by sending a "ClientHello" message to the server. This message includes the SSL/TLS version supported by the client, a list of supported cipher suites (encryption algorithms), and other parameters required for the handshake.
- Server Hello: Upon receiving the ClientHello message, the server responds with a "ServerHello" message. This message contains the SSL/TLS version selected for the connection, the chosen cipher suite from the client's list, and the server's digital certificate (if required).

Phase-2:

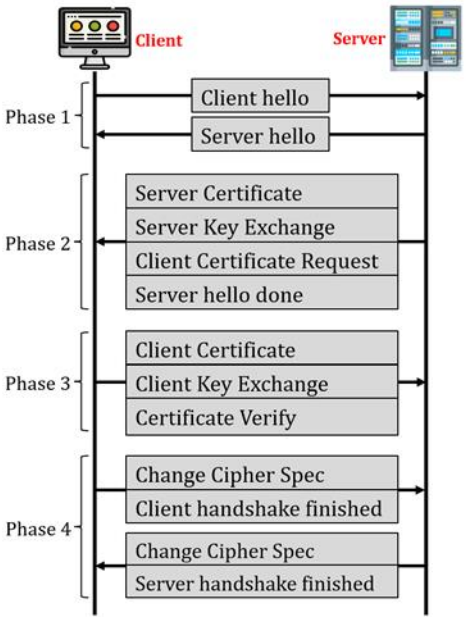
- Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
- Server Certificate: If the server requires client authentication (mutual SSL), it sends its digital certificate to the client. The certificate contains the server's public key, which is used for encryption.
- Server Key Exchange (optional): In some cases, the server may send additional key exchange information, especially if the chosen cipher suite requires it.

Phase-3:

- In this phase, Client replies to the server by sending his certificate and Client-exchange-key.
- ***Client Certificate:*** It is optional, it is only required if the server had requested for the client's digital certificate. If client doesn't have certificate, it can be sending no certificate message. Then it is up to server's decision whether to continue with the session or to abort the session.
- ***Client key exchange:*** The client sends a client key exchange, the contents in this message are based on key exchange algorithms between both the parties.

Phase-4:

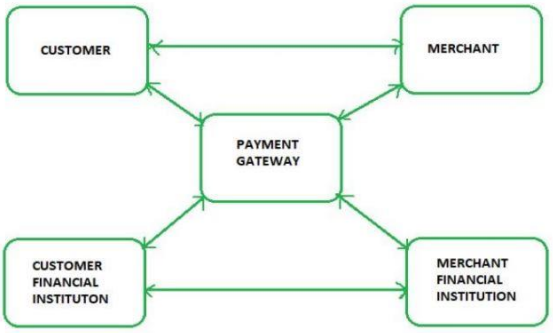
- In Phase-4 Change-cipher suite occurs and after this the Handshake Protocol ends.
- **Secure Connection Established:** At this point, both the client and server have exchanged the necessary information and verified each other's authenticity. They can now begin securely exchanging data using the agreed-upon encryption algorithms and session keys.



What is SET ? Explain SET Participants and Requirements?

- 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. SET protocol was developed to protect consumers' card details and financial information from hackers
- SET protocols use digital certificates to provide electronic access to funds from a bank account or a credit line. Each time a purchase is made electronically, an encrypted digital certificate generates for the merchant, financial institution, or customer.
- SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

The general scenario of electronic transaction is as follows :



In the general scenario of online transaction, SET includes similar participants:

- **Cardholde**r – A cardholder is an authorized holder of a payment card (MasterCard, Visa, and so on) that has been issued by an issuer.
- **Issuer** – This is a financial institution, such as a bank, that provides the cardholder with the payment card. The issuer is responsible for the payment of the debt of the cardholder.
- **Merchant** - A merchant is a person or organization with goods or services to sell to the cardholder. Typically, these goods or services are offered via a web site or by electronic mail.
- **Acquirer** – This is a financial institution that establishes an account with a merchant and processes payment card authorizations and payments.
- **Certificate authority** – Authority that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways.

Secure Electronic Transaction (SET) Protocol functionalities:

Provide Authentication –

- **Merchant Authentication:** SET allows customers to verify previous relationships between merchants and financial institutions. This is achieved using standard X.509V3 certificates for verification.

- **Customer / Cardholder Authentication:** SET verifies if the use of a credit card is authorized by the intended user. This authentication is facilitated through the use of X.509V3 certificates.
- **Message Confidentiality:**
  SET ensures that messages being transferred are kept confidential using encryption techniques. Traditionally, the Data Encryption Standard (DES) is used for encryption purposes to prevent unintended access to message content.
- **Message Integrity**:
  SET ensures the integrity of messages by preventing unauthorized modification through the use of digital signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1

SET in Action

1. **The customer opens an account:** The customer obtains a credit card account, such as MasterCard or Visa, with a bank that supports electronic payment and SET.
2. **The customer receives a certificate:** After suitable verification of identity, the customer receives an X.509v3 digital certificate, which is signed by the bank.
3. **The customer places an order :** This is a process that may involve the customer first browsing through the merchant's web site to select items and determine the price and at last finalize the order by placing it.
4. **The merchant is verified :** In addition to the order form, the merchant sends a copy of its certificate, so that the customer can verify that he or she is dealing with a valid store.
5. **The order and payment are sent.** The customer sends both an order and payment information to the merchant, along with the customer's certificate. The order confirms the purchase of the items in the order form.
6. **The merchant requests payment authorization**: The merchant sends the payment information to the payment gateway, requesting authorization that the customer's available credit is sufficient for this purchase.
7. **The merchant confirms the order :** The merchant sends confirmation of the order to the customer.
8. **The merchant provides the goods or service:** The merchant ships the goods or provides the service to the customer.
9. **The merchant requests payment**: This request is sent to the payment gateway, which handles all of the payment processing.
10. **Transaction is completed :** After merchant requests for the payment the customer pays for the order and completes the transaction successfully.

Explain Different approaches used for Intrusion detection?

- An intruder is an unauthorized person or entity that tries to access a system or network without authorization with the intent of doing harm, stealing data, or interfering with regular operations.
- Intruders are often referred to as hackers and are the most harmful factors contributing to the vulnerability of security. They have immense knowledge and an in-depth understanding of technology and security.
- An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer.
- The IDS is also a listen-only device. The IDS monitors traffic and reports results to an administrator. It cannot automatically take action to prevent a detected exploit from taking over the system.
- It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration.

Approaches to Intrusion Detection and Prevention :

Pre-emptive Blocking :

- It is also called Banishment vigilance. It seeks to prevent intrusion from happening before they occur.
- The above method is done by observing any danger signs of imminent threats and then blocking user or IP address from which these signs originate.
- While this approach aims to enhance security, it comes with complexities, including the potential for blocking legitimate users erroneously.
- Distinguishing between normal and potentially threatening traffic is a challenge, leading to the risk of false positives.

Signature-Based Detection :

- Signature-based detection is one of the most widely used approaches to intrusion detection and prevention. This method uses a database of known attack patterns or "signatures" to detect and prevent intrusions.
- The system compares incoming network traffic or system activity against the signatures in the database. If a match is found, the system will flag the activity as potentially malicious and take appropriate action.
- Since the database is the backbone of a SIDS solution, frequent database updates are essential, as SIDS can only identify attacks it recognizes.
- As a result, if the organization becomes the target of a *never before seen* intrusion technique, no amount of database updates will protect the organisations system.

Anomaly-Based Intrusion Detection :

- Anomaly-based detection is another approach to intrusion detection and prevention. This method uses machine learning algorithms to detect anomalies in network traffic or system activity.
- The system compares the current activity to a baseline of normal activity and flags any activity that seperates from the normal as potentially malicious.
- The strength of anomaly-based detection is that it can detect new or previously unknown threats. Additionally, the system can adapt to changes in the environment and can detect new types of attacks.
- This approach also has several weaknesses. For example, the system can generate false positives, and it can be difficult to accurately define a baseline of normal activity.

Behavior-Based Detection :

- Behavior-based detection is a newer approach to intrusion detection and prevention. This method uses machine learning algorithms to detect abnormal behavior in network traffic or system activity.
- The system observes the behavior of the network or system and compares it to a baseline of normal behavior. If the system detects abnormal behavior, it flags it as potentially malicious.
- The system continuously monitors ongoing activities, comparing them to the baseline. Any deviations or anomalies from the expected behavior trigger alerts or alarms, signaling potential security incidents.

Describe the architecture for distributed intrusion detection system

- A distributed IDS (dIDS) consists of multiple Intrusion Detection Systems (IDS) over a large network, all of which communicate with each other, or with a central server that facilitates advanced network monitoring.
- By having these co-operative agents distributed across a network, network operations, and security personnel are able to get a broader view of what is occurring on their network as a whole.
- A distributed intrusion detection system may need to deal with different audit record formats.
-

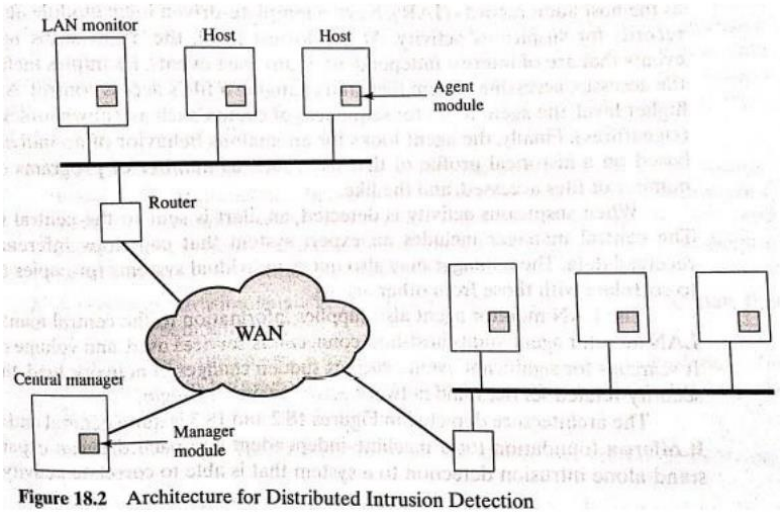


Figure 18.2 Architecture for Distributed Intrusion Detection

- The DIDS architecture combines distributed monitoring and data reduction with centralized data analysis.

  The Central Analysis Server
- The central analysis server is really the heart and soul of the operation. This server would ideally consist of a database and Web server.

The three main components are :

- **Host agent module:** An audit collection module operating as a background process on a monitored system. Its purpose is to collect data on security-related events on the host and transmit these to the central manager.
- **LAN monitor agent module:** Operates in the same fashion as a host agent module except that it analyzes LAN traffic and reports the results to the central manager.
- **Central manager module:** Receives reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion.

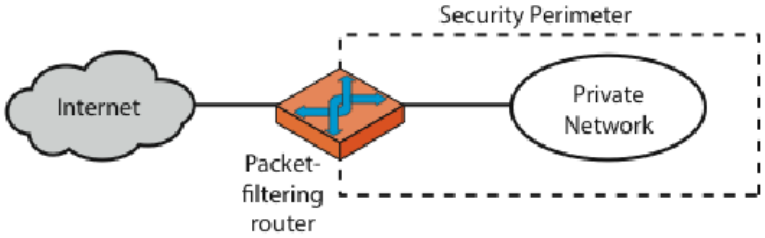
Explain Different Types of firewalls?

- Network Firewalls are the devices that are used to prevent private networks from unauthorized access. A Firewall is a security solution for the computers or devices that are connected to a network, they can be either in form of hardware as well as in form of software.
- By allowing only authorized traffic and blocking unwanted traffic, firewalls protect against unauthorized access, malware and other security threats. Firewalls can also prevent sensitive data from leaving the network.
- The data sent over a computer network is assembled into a packet, which contains the sender and recipient's IP addresses and port numbers. Before a packet is delivered to its destination, it's sent to the firewall for inspection.
- By blocking traffic from untrusted sources, firewalls act as a gatekeeper and prevent external threats like unauthorized access attempts, malware and viruses. In short, a firewall helps keep an organization's data safe and prevent security breaches that can cause significant damage.

Types of Network Firewall :

1. **Packet Filters:**

- Packet filters, often referred to as static firewalls, control network access by examining incoming and outgoing packets.
- They make access decisions based on various factors, including source and destination IP addresses, protocols, and specific ports.



(a) Packet-filtering router

2. **Stateful Inspection Firewalls:**

- Stateful inspection firewalls are a more advanced version of packet filters.
- They not only analyze packets but also keep track of the state of active connections.
- These firewalls permit or deny traffic based on the establishment of a valid session between two endpoints.

3. **Application Layer Firewalls:**

- Application layer firewalls operate at the OSI model's application layer and can examine data such as HTTP requests.
- These firewalls block potentially harmful applications or traffic that could pose risks to the network's security.

4. **Next-generation Firewalls:**

- Next-generation firewalls, often known as intelligent firewalls, combine the functions of the previously mentioned types with additional features.
- These features include application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.

5. **Circuit-level Gateways:**

- Circuit-level gateways provide security for User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connections.
- They function between the OSI model's transport and application layers, offering security at the session layer.

6. **Software Firewalls:**

- Software firewalls are installed on individual computers to protect them from external threats.
- These firewalls notify users about potential security risks, such as opening suspicious emails or visiting unsafe websites.

7. **Hardware Firewalls:**

- Hardware firewalls are physical devices deployed at network boundaries.
- They have the capability to inspect both inbound and outbound network traffic, enforcing access controls and security policies.

8. **Cloud Firewalls:**

- Cloud firewalls are software-based, cloud-deployed network devices.
- They filter data at the cloud level, safeguarding private networks from unauthorized access.

Advantages of Using Firewalls

- Firewalls play an important role in the companies for security management. Below are some of the important advantages of using firewalls.
- It provides enhanced security and privacy from vulnerable services. It prevents unauthorized users from accessing a private network that is connected to the internet.
- Firewalls provide faster response time and can handle more traffic loads.
- A firewall allows you to easily handle and update the security protocols from a single authorized device.
- It safeguards your network from phishing attacks.

Write a short note on trusted systems?

- In network systems, a trusted system is a computer system or network that has been designed, implemented, and tested to meet specific security requirements.
- Trusted systems are used to protect sensitive information, prevent unauthorized access, and ensure the integrity and availability of data and systems.
- A trusted system is typically designed with a set of security features, such as access controls, authentication mechanisms, and encryption algorithms, that are carefully integrated to provide a comprehensive security solution.

Trusted Systems are based on different level of security. They are mentioned as below:

- **Multilevel Security:** This type of Trusted system ensures that security is maintained at different levels of the computer system. It ensures that the information is prevented from being at risk. The different security levels of computer systems are :
    - Top Secret Level
    - Secret Level
    - Confidential Level
    - Unclassified Level

    A multilevel secure system must enforce:
    - **No read up:** A subject can only read an object of less or equal security level. This is referred to as **simple security property.**
    - **No write down:** A subject can only write into an object of greater or equal security level.

Data Access Control

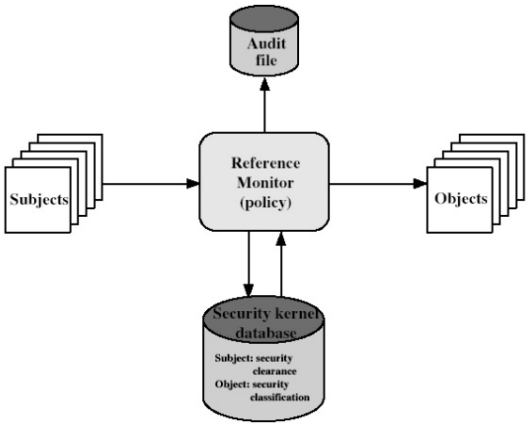
- In every Organization, Employees are given login credentials to make a secure connection. It is a method of identifying whether the right person has logged in to this work, based on the identification of profiles the associated ones with the company are authenticated.
- Then Finally letting the person access the data they want. Data Access control is the process of allowing the employees or the customers to use the data, cloud storage, folder, software, slide, or related information

There are three basic models of Data Access Control:

- **Access Matrix:** They are composed of three parts
    - Subject
    - Object
    - Access right
- **Access Control List:** They are composed of different entries of objects depicting user access and the level of access granted (public or private). Access control list demonstrate column-wise split.
- **Capability List:** They are composed of authorized users and the granted operations for them. Users can have multiple capability tickets. Capability list demonstrate row-wise split.

Reference Monitor:

- This type of trusted system provides hardware level security by limiting the access to objects.
- Reference monitor maintain security rules ensuring that 'Read Up' and 'Write Down' operations are not performed.
- Reference monitor ensure that the entire security maintaining process that is carried out is verified and safe.



Importance of Trusted System:

- **Identity Verification:** Trusted systems ensure that only verified users are given access. The verification process takes place that each user is identified uniquely.
- **Safety Maintained:** Trusted system ensures that safety is maintained by preventing direct access to confidential information.
- **Limiting Access:** Permissions and access that are absolutely necessary are granted for users. Unwanted rules and permissions are avoided.
- **Preventing Malicious Activities:** Trusted systems have a mechanism in place to detect and prevent malicious activities such as hacking attempts and unauthorized access.

Examples of Trusted Systems:

Windows BitLocker: Windows BitLocker is a trusted system that provides encryption for the entire hard drive. It prevents unauthorized access to the data stored on the hard drive by requiring a password or a smart card to unlock the drive.