Aryan
Q. **What are some of the threats to transactions**
Ans.
Major Threats to Transaction Security

1. **Man-in-the-Middle (MitM) Attacks**:
   - Attackers intercept and potentially alter communication between a client and a server.

2. **Phishing**:
   - Attackers trick users into providing sensitive information by masquerading as a trustworthy entity.

3. **SQL Injection**:
   - Malicious SQL code is injected into web forms or URL parameters to gain unauthorized database access.

4. **Cross-Site Scripting (XSS)**:
   - Attackers inject malicious scripts into web pages viewed by other users, leading to data theft or session hijacking.

5. **Distributed Denial of Service (DDoS) Attacks**:
   - Attackers overwhelm a service with a flood of traffic, rendering it unavailable to legitimate users.

6. **Malware**:
   - Malicious software designed to steal information, disrupt operations, or gain unauthorized access.

7. **Session Hijacking**:
   - Attackers steal or manipulate a user's session token to gain unauthorized access to their session.

8. **Weak Passwords**:
   - Easily guessable or common passwords make it easier for attackers to gain access.

Q. Give any 5 types of transaction security
Ans.
Encryption:

- **Symmetric Encryption**: Uses a single key for both encryption and decryption (e.g., AES).
- **Asymmetric Encryption**: Uses a pair of keys (public and private) for encryption and decryption (e.g., RSA).

Authentication:

- **Password-based Authentication**: Uses passwords to verify identity.
- **Multi-factor Authentication (MFA)**: Combines two or more verification methods (e.g., password + OTP).
- **Biometric Authentication**: Uses biometric data such as fingerprints or facial recognition.

Digital Signatures:

- Ensures the authenticity and integrity of a message, software, or digital document.

Tokenization:

- Replaces sensitive data with unique identification symbols (tokens) that retain essential information without compromising security.

Aditi

Q. Explain the SSL/TLS Protocol

Ans.

SSL, or Secure Sockets Layer, is a protocol developed to provide secure communication over a computer network. It ensures that data transmitted between a client (e.g., a web browser) and a server (e.g., a website) is encrypted and secure from eavesdropping, tampering, and message forgery.

1. **Encryption**: SSL uses symmetric encryption to encrypt data during transmission. This ensures that even if data is intercepted, it cannot be read without the decryption key.
2. **Authentication**: SSL uses public key infrastructure (PKI) to authenticate the identity of the server. This is usually done using digital certificates issued by trusted Certificate Authorities (CAs).
3. **Integrity:** SSL ensures data integrity through the use of message digests and hashing functions. This ensures that the data has not been altered during transmission.

Issues with SSL:

Security Vulnerabilities: SSL had several security flaws, such as the POODLE and BEAST attacks.

Protocol Complexity: SSL had complex implementations that made it difficult to maintain and secure.

Lack of Standardization: SSL was not standardized, leading to inconsistencies across implementations.

TLS, or Transport Layer Security, is the successor protocol to SSL, designed to address the shortcomings of SSL and provide a more secure communication channel.

Key Improvements in TLS over SSL:

1. **Enhanced Security**: TLS incorporates stronger encryption algorithms and more secure hashing functions.
2. **Improved Handshake Protocol**: The TLS handshake process includes additional security measures to prevent man-in-the-middle attacks.
3. **Forward Secrecy**: TLS supports forward secrecy, ensuring that session keys are not compromised even if the server's private key is.
4. **Standardization**: TLS is an open standard maintained by the Internet Engineering Task Force (IETF), ensuring consistency and interoperability across implementations.
5. **Extensions and Flexibility**: TLS is designed to be extensible, allowing for the addition of new features and improvements without disrupting existing implementations.

Q. Difference between SSL and TLS
Ans.

SSL	TLS
SSL stands for Secure Socket Layer.	TLS stands for Transport Layer Security.
SSL (Secure Socket Layer) supports the Fortezza algorithm.	TLS (Transport Layer Security) does not support the Fortezza algorithm.
SSL (Secure Socket Layer) is the 3.0 version.	TLS (Transport Layer Security) is the 1.0 version.
In SSL(Secure Socket Layer), the Message digest is used to create a master secret.	In TLS(Transport Layer Security), a Pseudo-random function is used to create a master secret.
In SSL(Secure Socket Layer), the Message Authentication Code protocol is used.	In TLS(Transport Layer Security), Hashed Message Authentication Code protocol is used.
SSL (Secure Socket Layer) is more complex than TLS(Transport Layer Security).	TLS (Transport Layer Security) is simple.
SSL (Secure Socket Layer) is less secured as compared to TLS(Transport Layer Security).	TLS (Transport Layer Security) provides high security.
SSL is less reliable and slower.	TLS is highly reliable and upgraded. It provides less latency.
SSL has been depreciated.	TLS is still widely used.

SSL uses port to set up explicit connection.	TLS uses protocol to set up implicit connection.

Q.Explain the Handshaking Process/ Explain the working of SSL/TLS
Ans.
The TLS (Transport Layer Security) or SSL (Secure Sockets Layer) handshake is a process used to establish a secure connection between a client and a server. This involves several steps to ensure both parties authenticate each other and agree on encryption methods:

1. **Client Hello:**
    - The client sends a "Client Hello" message to the server. This message includes information about the client's capabilities, such as supported TLS versions, cipher suites, and random data.
2. **Server Hello:**
    - The server responds with a "Server Hello" message, which includes the chosen TLS version, cipher suite, and random data.
    - The server also sends its digital certificate to authenticate its identity.
3. **Key exchange:**
    - The client verifies the server's certificate. If valid, the client proceeds to generate a pre-master secret and encrypts it with the server's public key (obtained from the certificate).
    - The client sends the encrypted pre-master secret to the server.
4. **Session Key Generation:**
    - Both the client and the server generate session keys from the pre-master secret and the random data exchanged during the hello messages.
    - These session keys will be used to encrypt the data transmitted during the session.

Q. Describe the SET Protocol.

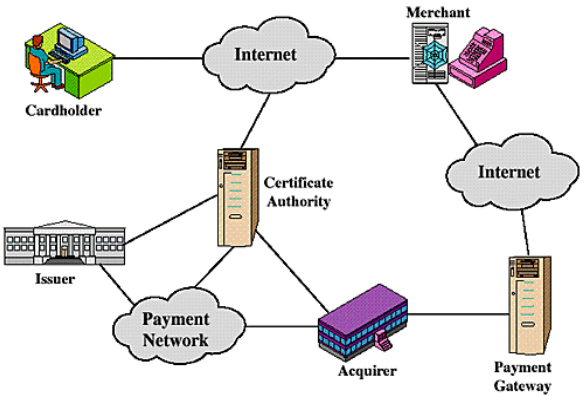
Ans The Secure Electronic Transaction (SET) is an open encryption and security specification that is designed for protecting credit-card transactions on the Internet. The pioneering work in this area was done in 1996 by MasterCard and Visa jointly.

SET is not a payment system. Instead, it is a set of security protocols and formats that enable the users to employ the existing credit-card payment infrastructure on the Internet in a secure manner.

SET services can be summarized as follows:
1. It provides a secure communication channel among all the parties involved in an e-commerce transaction.
2. It provides authentication by the use of digital certificates.
3. It ensures confidentiality, because the information is only available to the parties involved in a transaction, and that too only when and where necessary.

Q. What are the SET Participants ?

1. **Cardholder :** A cardholder is an authorized holder of a payment card such as MasterCard or Visa that has been issued by an issuer.
2. **Merchant :** A merchant is a person or an organization that wants to sell goods or services to cardholders. A merchant must have a relationship with an acquirer for accepting payments on the Internet.
3. **Issuer:** The issuer is a financial institution (such as a bank) that provides a payment card to a cardholder. The most critical point is that the issuer is ultimately responsible for the payment of the cardholder's debt.
4. **Acquirer**: This is a financial institution that has a relationship with merchants for processing payment-card authorizations and payments.
5. **Payment Gateway:** This is a task that can be taken up by the acquirer or it can be taken up by an organization as a dedicated function. Specifically in SET, the payment gateway acts as an interface between SET and the existing card-payment networks for payment authorizations.
6. **Certification authority:** As we know, this is an authority that is trusted to provide public key certificates to cardholders, merchants and payment gateways. In fact, CAs are very crucial to the success of SET.



Q. Describe the SET Process.

Ans

1. **Customer opens an account :** Customer opens a credit card account (MasterCard or Visa) with a bank that supports electronic payment mechanisms and the SET Protocol.

2. **The customer receives a certificate** : After the customer is verified, the customer receives a digital certificate from the CA. The certificate also contains details like the customer's public key and expiration date.

3. **Merchant receives a certificate :** A merchant that wants to accept a certain brand of credit cards must possess a digital certificate

4. **The customer places an order** : This is a typical shopping cart process for the customer. The merchant in turn , sends back details such as the list of items selected, quantities and total price, etc.

5. **The Merchant is Verified** : The merchant also sends its digital certificate to customer to prove its validity.

6. **The order and payment details are sent** : The customer sends both the order and the payment details to the merchant along with the customer's digital certificate. The payment contains the credit card details however the payment information is so encrypted that the merchant cannot read it.

7. **Merchant requests payment authorization** : The merchant forwards this payment detail to the payment gateway via the acquirer and requests the payment gateway to authorize the payment.

8. **The Payment Gateway Authorizes the payment** : Using the credit card information received from the merchant, the payment gateway verifies the customer's payment details and either authorizes or rejects the payment.

9. **The merchant confirms the order** : If the payment gateway authorizes the payment, the merchant sends a confirmation of order to the Customer

10. **The Merchant Provides Goods or Service** : The merchant now ships the goods as per the Customer's order

11. **The Merchant Requests Payment :** The payment gateway receives a request from the merchant for making the payment and after interacting with the issuer and acquirer it sends the payment from the customer's account to the merchant's account.

Q. Describe the SET Model.

Ans.

- The three main parties involved in the actual transaction are, of course, the customer, the merchant and the payment gateway.
- The merchant and the customer make requests for their respective certificates. We have shown two different certification authorities. Of course, it is very much possible that both the merchant and the customer receive certificates from the same certification authority.

- In general, the certificate to a customer is issued by the bank or the credit card company who has issued the card to the customer, or sometimes also by a third-party agency representing the credit-card company.

- On the other hand, a financial institution, also called an acquirer, issues a merchant's certificate.
- A merchant needs to have as many certificates as the number of different brands of credit cards that it accepts (e.g. one for Master-Card, one for Visa, one for Amex, and so on).
- Thus, when a customer receives a merchant certificate, it is also assured that the merchant is authorized to accept payments for that brand of credit card.

- The transactions between a customer and merchant are for purchases, and those between the merchant and the payment authority are for authorization of payment.

Gaurav

Q. Explain a standard related to Transactions.

Ans.

- The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
- This standard offers robust and comprehensive standards and supporting materials to enhance payment card data security.
- These materials include a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information.
- PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data.
- PCI DSS comprises a minimum set of requirements for protecting cardholder data.

Q. Explain the 6 requirements of PCI-DSS.

Ans.

- **Build and Maintain a Secure Network**
    - Install and maintain a firewall configuration to protect cardholder data.
    - Do not use vendor-supplied defaults for system passwords and other security parameters.
- **Protect Cardholder Data**
    - Protect stored data
    - Encrypt transmission of cardholder data across open, public networks.
- **Maintain a Vulnerability Management Program**
    - Use and regularly update anti-virus software or programs.
    - Develop and maintain secure systems and applications.
- **Implement Strong Access Control Measures**
    - Restrict access to cardholder data by businesses on a need-to-know basis.
    - Assign a unique ID to each person with computer access.
    - Restrict physical access to cardholder data.
- **Regularly Monitor and Test Networks**
    - Track and monitor all access to network resources and cardholder data.
    - Regularly test security systems and processes.
- **Maintain an Information Security Policy**
    - Maintain a policy that addresses information security for all personnel.