Security in Online Transactions

D095 - Gaurav Mehra
D096 - Aryan Moghe
D108 - Aditi Singh
D109 - Arushi Singhi

01

INTRODUCTION

Transaction security, refers to a category of practices, protocols, tools and other security measures used during and after business transactions to protect sensitive information and ensure the safe and secure transfer of customer data.

Transaction Security Threats

Threats to transaction security often intersect or contribute to broader cybersecurity threats. Some of the examples are

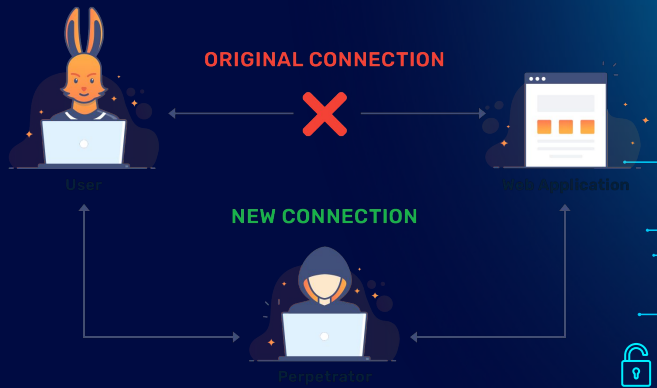
1. **Phishing**
2. **Man-in-the-middle attacks (MITM)**
3. **Card-not-present fraud**
4. **Account takeover fraud**
5. **Synthetic identity fraud (SIF)**
6. **Business email compromise (BEC) scams**

Phishing

- Phishing scams trick people into giving away personal info, like credit card numbers, either to steal money from individuals or to get lots of payment details from companies.
- They can also target businesses in an attempt to steal customer payment information in bulk.

Man-in-the-Middle (MITM)

- A well-known form of cyberattack, during a MITM attack, a hacker will surreptitiously position themselves between two parties who believe they have a private connection. The attacker may attempt to manipulate their transferred data or simply eavesdrop to steal any private payment information that may be shared.



Card-Not-Present-Fraud

- While in-person transactions typically require a physical credit card, transactions made online or over the phone often require only a credit card number.
- This loophole can open up online or telephone-based transactions to card-not-present fraud, in which fraudsters use stolen numbers to make fraudulent transactions.

Account Takeover Fraud

- Make unauthorized purchases.
- Another risk posed by phishing is account takeover fraud. Fraudsters may use phishing or other means to seize unauthorized access to a consumer's banking or online shopping account.

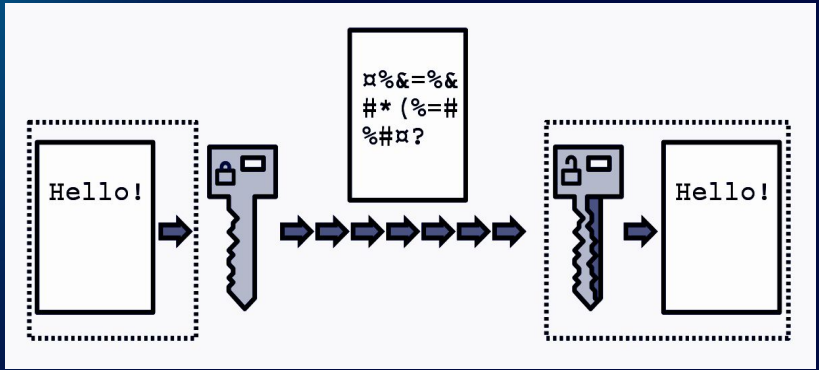
E-Banking Trojans

- E-Banking Trojans are are one of the most significant threat to online banking
- They intercept the victims account information before the system can encrypt it and send it to attackers control center
- Installation of these Trojans take place when the user clicks on some malicious email

Types of Transaction Security

. The following are a few of the most common methods for bolstering transaction security:

1. **Encryption**
2. **Tokenization**
3. **Authentication**
4. **Secure payment gateways**



Encryption

- The backbone of data privacy, businesses and customers rely on data encryption to protect sensitive information during and after transactions.
- Commonly used encryption standards like Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are frequently used during online transactions to prevent unauthorized access, tampering and theft.

Tokenization

- Tokenization is a process that replaces sensitive customer data, like credit card numbers, with unique tokens that can neither be used to make fraudulent transactions nor reverse engineer the original payment information.
- These tokens are then used to reference the original payment information, which is stored in a secure token vault. Tokenization both reduces the risk associated with data breaches and simplifies regulatory compliance since the tokens themselves are useless even if they fall into the wrong hands.

Authentication

- Single-factor authentication (SFA) requires one form of identification, such as a password or a pin; two-factor authentication (2FA) requires additional forms of identification, such as a one-time passcode sent to a registered device or email.
- Other standard authentication methods include requiring a card verification value (CVV) for credit card payments and biometric authentication (such as facial recognition or fingerprint scanning).

Secure Payments Gateway

- Secure payment gateways are a crucial part in establishing strong transaction security and building and maintaining customer trust.
- Secure payment gateways often combine various transaction security techniques, including encryption, tokenization and authentication, to ensure data security.
- By integrating these security techniques, secure payment gateways provide a robust defense against data breaches and fraud, fostering customer trust and compliance with security standards.

02

PROTOCOLS

SSL / TLS

SET

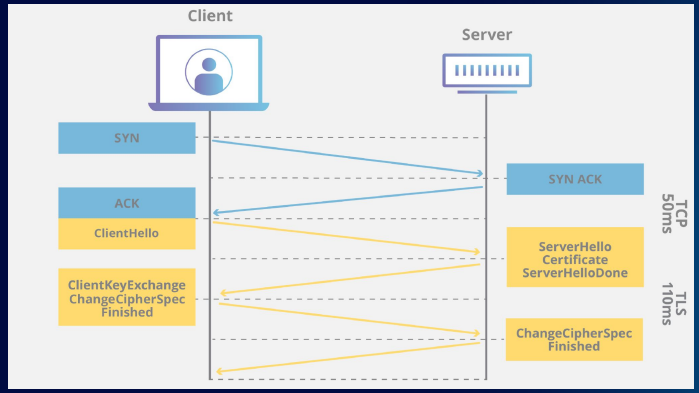
SSL/TLS

Secure Socket Layer is standard technology for securing an internet connection by encrypting data sent between a website and a browser (or between two servers). It prevents hackers from seeing or stealing any sensitive information (like credit card numbers) transferred, including personal or financial data.

TLS, short for “Transport Layer Security,” is a cryptographic protocol that serves the same purpose as SSL. It is essentially an improved version of SSL, addressing security vulnerabilities found in earlier SSL protocols.

The Handshake Process

- **Client Hello**:The client sends a "Client Hello" message to the server.
- **Server Hello**:The server responds with a "Server Hello" message. The server also sends its digital certificate to authenticate its identity. This “Hello”message includes information about the supported TLS versions, cipher suite, and random data.
- **Key exchange**: The client verifies the server’s certificate. The client sends the encrypted pre-master secret to the server.
- **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.



SET : Secure Electronic Transactions

What it is

Participants

Process

Model

- Open encryption and security specification for protecting credit-card transactions on the internet

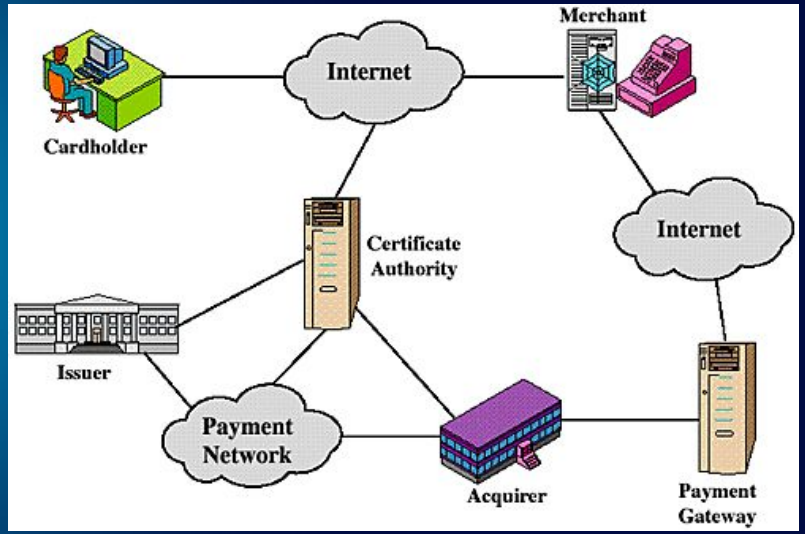
- 1996 by MasterCard and Visa jointly.

- NOT a payment system.
  -> 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.

- Provides:

1. A secure communication channel
2. Authentication
3. Ensures confidentiality

SET Participants



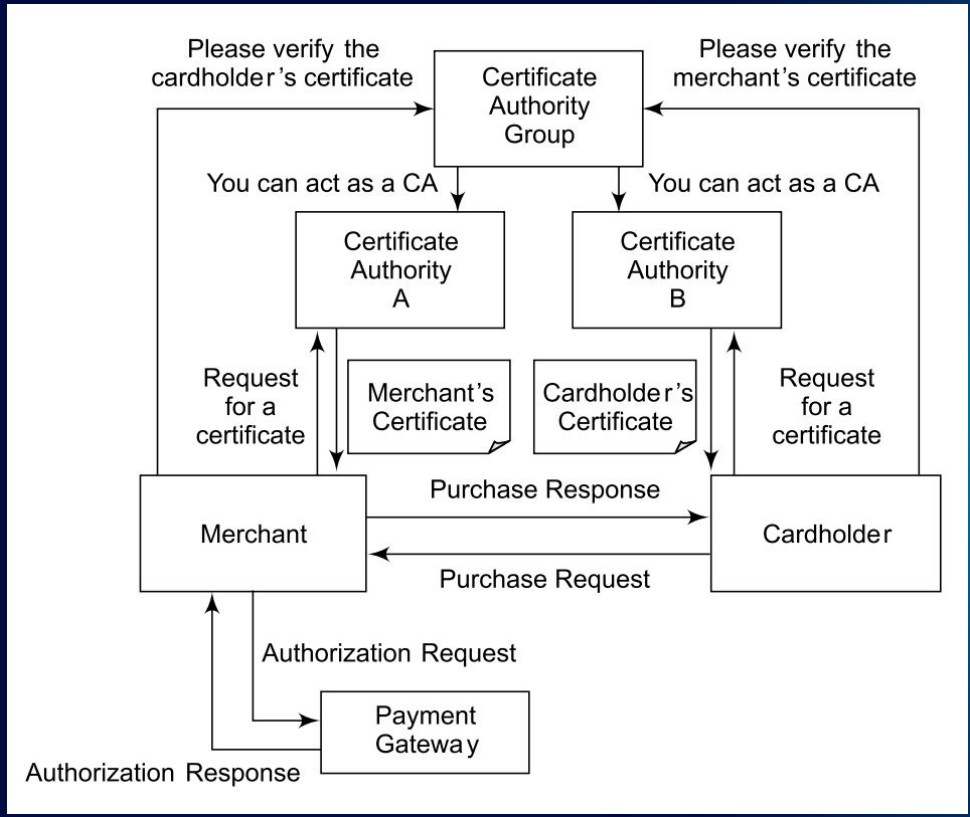
1. **Cardholder :** Authorized holder of a payment card
2. **Merchant :** A person or an organization that wants to sell goods or services to cardholders.
3. **Issuer :** Financial institution that provides a payment card to a cardholder.
4. **Acquirer :** Financial institution that has a relationship with merchants for processing payment-card authorizations and payments.
5. **Payment Gateway :** Task that can be taken up by the acquirer or it can be taken up by an organization as a dedicated function.
6. **Certification Authority :** An authority that is trusted to provide public key certificates to cardholders, merchants and payment gateways.

SET Process:

1. Customer opens an account
2. The customer receives a certificate
3. Merchant receives a certificate
4. The customer places an order
5. The Merchant is Verified
6. The order and payment details are sent
7. Merchant requests payment authorization
8. The Payment Gateway Authorizes the payment
9. The merchant confirms the order
10. The Merchant Provides Goods or Service
11. The Merchant Requests Payment

SET Model

- 3 main parties:
  Customer, Merchant & Payment Gateway
- The merchant and the customer make requests for their respective certificates.
- Customer Certificate - the bank or the credit card company, third party agency.
- Merchants Certificate - Financial Institution (Acquirer).
- Merchant needs to have many certificates as the no. of brands of credit cards.
- Customer <-> Merchant - Purchases
- Merchant <-> Payment Gateway - Authorization of Payment



03

LAWS AND STANDARDS

PCI-DSS

- The **Payment Card Industry Data Security Standard** is a proprietary information security standard for organizations that handle cardholder information.
- PCI DSS applies to all entities involved in payment card processing:
  - Merchants
  - Processors
  - Acquirers
  - Issuers
  - Service Providers
  - Other Entities

PCI-DSS

1. **Build and Maintain a Secure Network**
    a. Maintain a firewall configuration
    b. Default system passwords
2. **Protect Cardholder Data**
    a. Protect stored data
    b. Encrypt transmission of data
3. **Maintain a Vulnerability Management Program**
    a. Anti-virus softwares
    b. Secure systems and apps

PCI-DSS

4. **Implement Strong Access Control Measures**
    a. Need-to-know basis
    b. Use unique IDs
    c. Physical access
5. **Regularly Monitor and Test Networks**
    a. Monitor all resources' access
    b. Regularly test systems
6. **Maintain an Information Security Policy**

04

DEMO: HOW TO ??????????

04

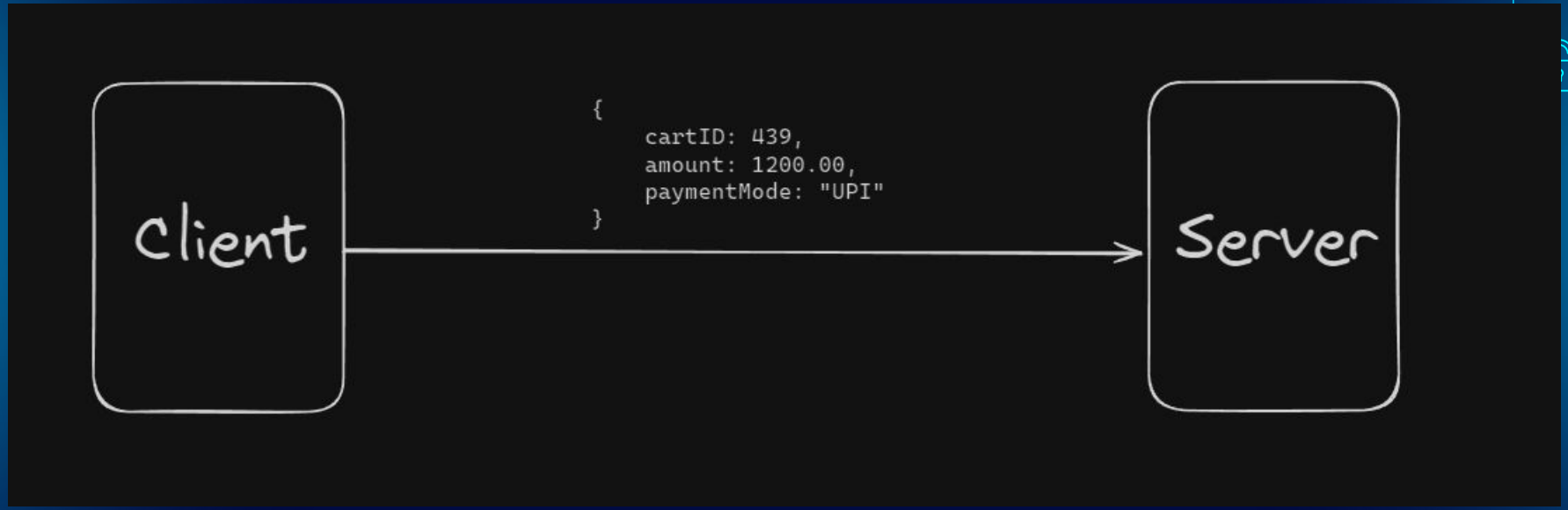
DEMO: HOW TO COMMIT FRAUD

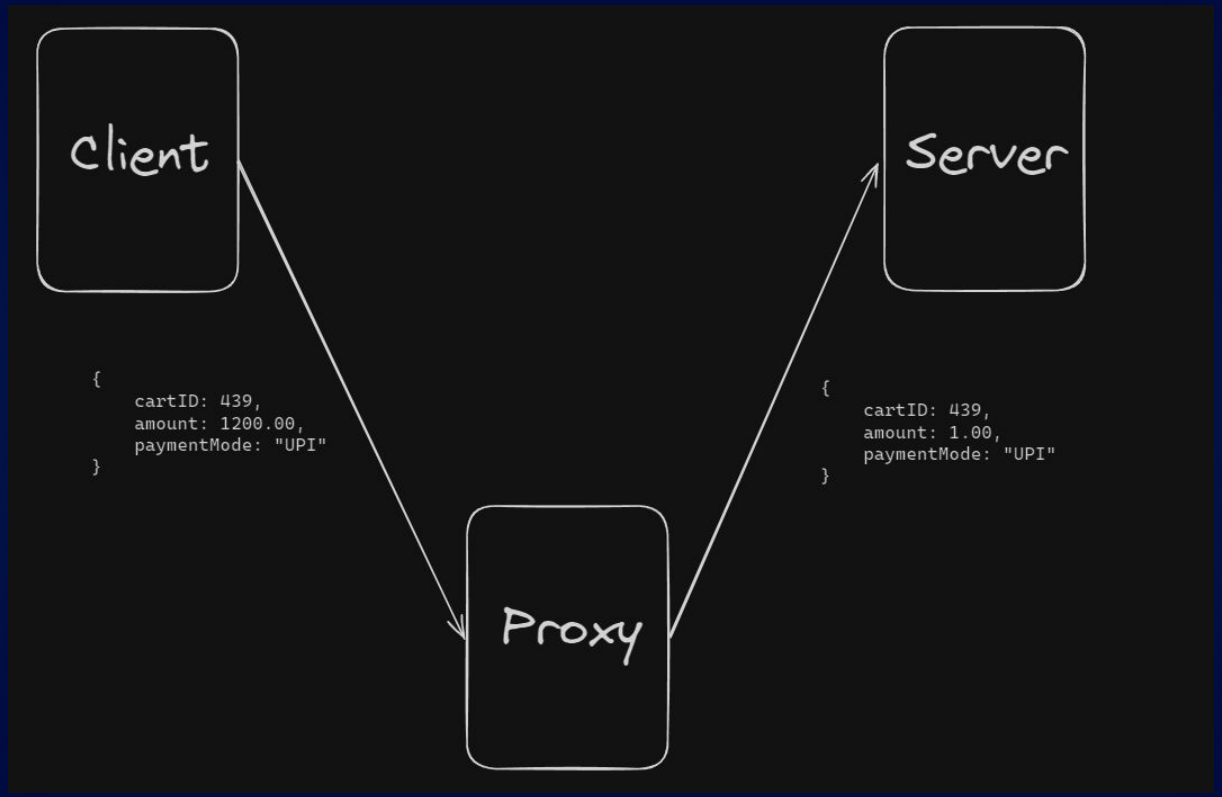
04

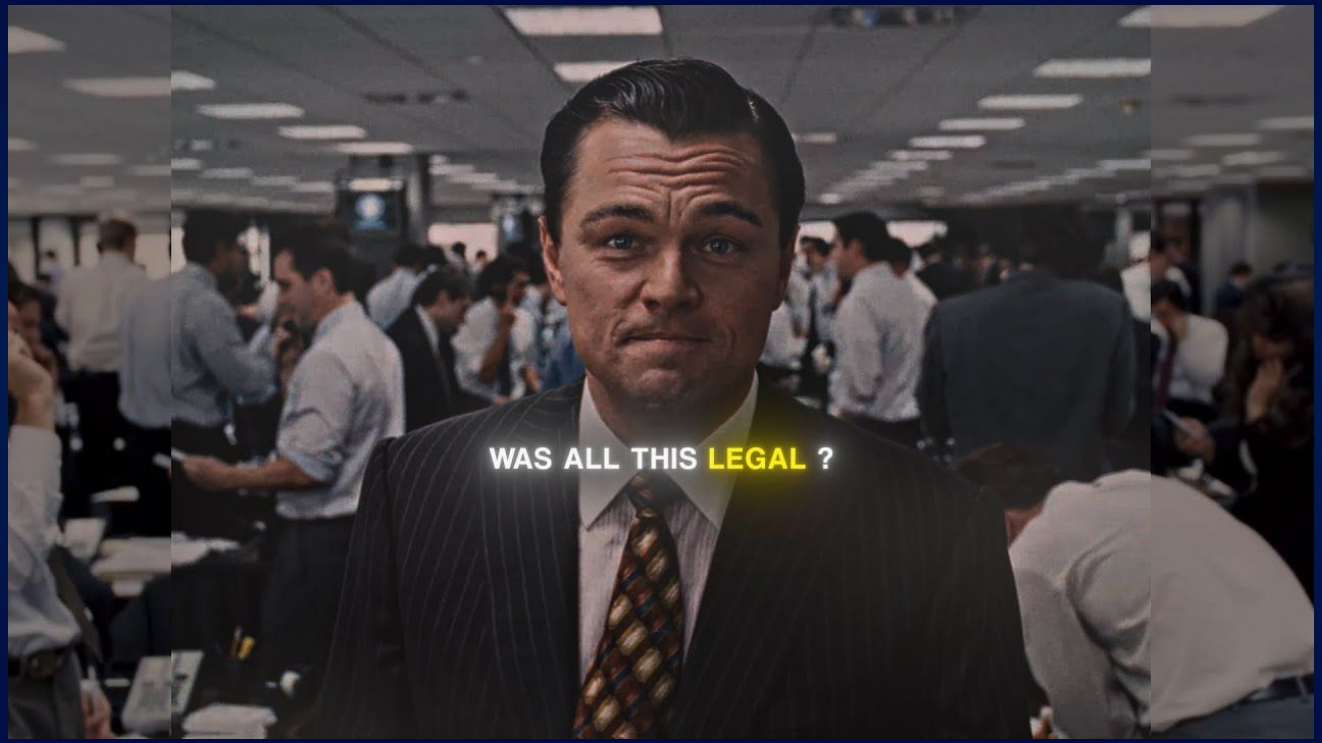
DEMO: HOW TO COMMIT FRAUD

(ONLY FOR EDUCATIONAL PURPOSES)
(and marks)

How to Commit Fraud?




Client
Server
Proxy
{
cartID: 439,
amount: 1200.00,
paymentMode: "UPI"
}
{
cartID: 439,
amount: 1.00,
paymentMode: "UPI"
}


WAS ALL THIS LEGAL ?

Why is it Legal?

Fraud is a crime, but for penalisation it must be committed wilfully.

Why is it Legal?

Fraud is a crime, but for penalisation it must be committed wilfully.

- Not performed with harmful intentions
- Done solely for educational purposes (and Keyur's birthday)
- Will get us marks

Thanks!

Any questions?
Please go through the Q&A
and find the answers yourself